State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace

Gabor Rona* & Lauren Aarons**

Introduction: Translating Rights

Debate over whether or not international human rights law applies to cyberspace and cyber-related activities[1] has more or less been settled. It does apply, as it would to any other context. Yet, debate continues about the content and scope of application of international human rights law to cyberspace. It is one thing to say that cyber communications, for example, hold the same civil and political protection as their offline predecessors, but it's entirely another thing to say exactly what these protections are, where their limits may lie and the exact nature of the State's obligations to protect human rights vis-a-vis cyberspace.

Indeed, there are a number of areas of controversy or confusion in the application of human rights law to cyberspace. Some reflect ongoing debates within the human rights legal field that pre-exist the emergence of cyber. These include questions concerning the relationship between human rights law and other international legal constructs such as the law of armed conflict, the territorial scope of application of human rights law obligations, and how to balance competing rights. But crucially, there are also a number of unique features of cyberspace that exacerbate these persistent tensions, or that call for the specific engagement/adaptation of human rights law to address new circumstances. Aspects of cyberspace that to some extent present new challenges include the mobility of data online, the amount of personal detail individuals render vulnerable through cyberspace, and the potential of acts emanating from or involving cyberspace to cause grave disruption and harm to others. Indeed, some legal scholars argue that there comes a point in which analogies and adaptations from the offline world are no longer feasible or helpful, and that international human rights law is not equipped to regulate cyber.[2]

This article considers the content and scope of application of international human rights law applicable to cyberspace. Instead of addressing head-on whether international human rights law is well-equipped to regulate the online

---

* Gabor Rona, formerly the International Legal Director of Human Rights First, is a Visiting Professor of Law at Cardozo Law School, where he teaches Human Rights Law and International Humanitarian Law.

** Lauren Aarons has an LLM from Columbia University and a MPhil from the University of Oxford. The authors thank Leigh Rome for her invaluable assistance.

1. While the term "cyberspace" and "online" are narrower than "cyber-related activities" or "cyber," these terms will be used interchangeably in this paper.

2. *See, e.g.*, Ashley Deeks, *An International Legal Framework for Surveillance*, 55 Va. J. Int'l L. 2 (2015).

world, it identifies how human rights law does apply to cyber, and where the application of human rights law remains unclear or, in some cases, ill-suited.

Following this introduction, Section one affirms the application of human rights law to cyberspace, and also considers its scope of application, including with regard to mobile data. Section two reflects on the content of a State's obligation to respect human rights law in cyberspace. Section three addresses a State's obligation to *ensure* respect for human rights (protect and fulfill rights) in cyberspace by protecting against third party abuse and by providing a remedy for violations. It also addresses State obligations to promote human rights in cyberspace and whether there is a right to access the Internet, or certain online content. Section four considers the limitations of human rights obligations and permissible restrictions in cyberspace. A conclusion follows.

I. APPLICATION OF HUMAN RIGHTS LAW TO CYBERSPACE

A. The Duty to Respect, Protect (Ensure Respect) and Fulfill Human Rights in Cyberspace

The UN Human Rights Council, the UN General Assembly and States, acting both individually and collectively, regularly assert that individuals enjoy the same rights online that they enjoy offline.[3] The United States has, for example, taken the position that "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace."[4] France has stated that "in international forums and through its cooperation, France is committed to promoting and protecting freedom of opinion and

3. *See, e.g.*, Human Rights Council, The Promotion, Prot. and Enjoyment of Human Rights on the Internet, ¶ 1, U.N. Doc. A/HRC/20/L.13 (June 29, 2012) ("[T]he same rights that people have offline must also be protected online"); Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 22, U.N. Doc. A/HRC/29/32 (May 22, 2015); G.A. Res. 68/167 (Jan. 21, 2014); Human Rights Council Res. 26/13 U.N. Doc. A/HRC/RES/26/13 (June 20 2014); Human Rights Council Res. 26/13 U.N. Doc. A/HRC/RES/26/13 (June 20 2014); *Guide To Human Rights For Internet Users*, CM/Rec (2014)6 (Council of Eur.); Barack Obama, U.S President, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; Budapest Convention on Cybercrime, art. 15.1, Jan. 7, 2004, C.E.T.S. 185; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 21, U.N. Doc. A/68/98 (June 24, 2013) (findings of 15 governmental experts adopted unanimously by the General Assembly: "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments."); Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/RES/68/243 (Jan. 9, 2014) ("Noting the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies"); Deauville Declaration of the G8 Countries, art. 10, (2011).

4. Barack Obama, U.S. President, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, (2011), *supra* note 3.

expression, as well as the freedom of assembly and association online and in the real world, so long as they respect the other fundamental rights."[5] It has likewise noted that more than 180 governments have reaffirmed the full applicability of the Universal Declaration of Human Rights online during the World Summit on the Information Society (WSIS).[6]

Indeed, there is no reason why human rights protection should be limited by the advent of cyberspace. At the emergence of international human rights, it was anticipated that its principles would extend to all media, regardless of new technological advancements. This is particularly evident in connection with the right to freedom of expression. The Universal Declaration of Human Rights, for example, proclaims that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers*" (emphasis added).[7] Article 27 of the Universal Declaration of Human Rights, echoed in the International Covenant of Economic, Social and Cultural Rights, is similarly forward looking, noting that 'Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.'[8] Other rights,

5. France Diplomatie, *Freedom and fundamental rights on the Internet*, last updated November 2013, http://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/digital-technology-and/article/freedom-and-fundamental-rights-on.

6. World Summit on the Information Society, Declaration of Principles, ¶ 1, WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003), http://www.itu.int/wsis/docs/geneva/official/dop.html ("We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights"); *see also* U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Recommendations on Norms, Rules, and Principles of Responsible Behavior by States*, ¶ 21, U.N. Doc. A/68/98 (June 24, 2013) ("State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.").

7. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 19 (Dec. 10, 1948) [hereinafter UDHR] ("Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.); *see also* International Covenant on Civil and Political Rights, art. 19.2, 999 U.N.T.S. 171 (Mar. 23, 1976) [hereinafter ICCPR] ("[r]egardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice"); European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10.1, 213 U.N.T.S. 221 (Nov. 4, 1950) [hereinafter ECHR] ("[r]egardless of frontiers"); American Convention on Human Rights, art 13.1, 1144 U.N.T.S. 123 (Nov. 22, 1969) [hereinafter ACHR] ("[r]egardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.").

8. UDHR, art. 27; *see also* the International Covenant on Social, Economic and Cultural Rights, U.N.T.S. 3 (Jan. 03, 1976, 993) [hereinafter ICESCR], which recognizes in Article 15 (1)(b) "the right of everyone . . . [t]o enjoy the benefits of scientific progress and its applications."

such as the right to privacy, do not limit the application of the right to any particular forum or media.

There is thus no reason to see cyber as outside of international human rights law. States are required to respect human rights on the Internet; they may not violate human rights that an individual is exercising in cyberspace, and, likewise, may not use cyberspace as a location/technology from which to violate rights of individuals.. States' obligations also extend beyond the duty to respect to include positive measures. The law of human rights, which extends to cyber, requires States to respect, protect and fulfill human rights.[9] States are required to take "judicial, administrative, educative and other appropriate measures in order to fulfill their legal obligations,"[10] including to protect individual rights from arbitrary interference by third parties through legislation, and to take measures to ensure that individuals can realize their rights, including through availability of remedies, for violations. States that are party to the International Convention on Economic, Social and Cultural Rights also have an obligation to "progressively realize" the rights contained in that Covenant to the best of their available resources.[11]

B. Scope of Application of International Human Rights Law to Cyberspace

Most actions in cyberspace are not limited by borders.[12] Questions about the extra-territorial application of international human rights law, and how the law developing in this area applies to cyberspace, thus become significant issues. The last couple of decades have seen the question of the extra-territorial application of human rights law slowly crystalize around several key concepts, but the manner in which these concepts apply to cyberspace, and particularly issues of surveillance, are yet to be fully determined.

The International Covenant on Civil and Political Rights (ICCPR) obligates each State party to respect and to ensure all individuals within its territory and subject to its jurisdiction, the rights recognized in the Covenant.[13] For sure, this

---

9. *See generally* Human Rights Comm., General Comment No. 31: "The Nature of the General Legal Obligations Imposed on States Parties to the Covenant", ¶ 6, UN Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004) ("The legal obligation under article 2, paragraph 1 [of the ICCPR], is both negative and positive in nature."); ICESCR, art. 2. This is discussed further under Section 3.

10. Human Rights Committee, *supra* note 9, at ¶ 7 ("Article 2 requires that States Parties adopt legislative, judicial, administrative, educative and other appropriate measures in order to fulfill their legal obligations.").

11. ICESCR, art. 2.

12. *See, e.g.*, Jennifer Daskal, *The Un-Territoriality Of Data*, 125 YALE L. J. 2 (2015).

13. ICCPR, art. 2.1 ("Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction"); *cf.* ECHR, art. 1 ("The High Contracting Parties shall secure to everyone within their jurisdiction"); ACHR, art. 1.1 ("The States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction."); The African Charter on Human and Peoples" Rights, art. 1, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) provides that States shall "recognize the rights, duties and freedoms" and "shall undertake to adopt legislative or other measures to give effect to them."

means a State is duty-bound to respect, protect and fulfill human rights of all individuals within in its territory and also under its jurisdiction, and it must do so without discrimination. Moreover, increasingly, the terms "within its territory and subject to its jurisdiction" are being interpreted in their disjunctive, rather than conjunctive sense, at least as concerns the State's negative obligation to refrain from violating rights.[14] Thus, the State is bound by international human rights law in relation to individuals outside of its territory but otherwise under its jurisdiction. While the United States and Israel maintain that, for the most part, human rights obligations do not apply extra-territorially,[15] this categorical position is rejected by the weight of international jurisprudence.

With regard to what is known as the "spatial model" of jurisdiction, the Human Rights Committee has held that "a State party must respect and ensure the rights laid down in the Covenant to anyone *within the power or effective control* of that State party, even if not situated within the territory of that State party" (emphasis added).[16] Decisions from the European Court of Human Rights and the Inter-American Commission on Human Rights, have confirmed the extra-territorial application of human rights and have established the test of "effective control,"[17] and "authority and control,"[18] respectively, for when a state exercises jurisdiction outside its territory for the purposes of triggering human rights law obligations. As confirmed by the International Court of Justice, it is now widely recognized that international human rights law obligations apply extra-territorially where a State is occupying territory of another State.[19] Moreover, extra-territorial human rights obligations are also increasingly recognized where a State's forces have effective control over another State's territory as a result of military operations, even where the area is not understood as "occupied territory."[20] In addition to the spatial model, States have also been found to have jurisdiction, and therefore, human rights obligations, under the "personal model," when and where the State has physical control of an individual outside of a territory over which it exercises effective

14. *See* Human Rights Comm., *supra* note 9, at ¶ 10.

15. For U.S. position, *see*, *e.g.*, U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Third Periodic Reports of States Parties, United States of America, ¶ 3, U.N. Doc. CCPR/C/USA/3, Annex I (Nov. 28, 2005) ("[T]he United States respectfully reiterates its firmly held legal view on the territorial scope of application of the Covenant."). For Israeli position, *see, e.g.*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2005 I.C.J. Reports 142, ¶¶ 109-111 (July 9, 2004).

16. Human Rights Comm., General Comment No. 31: "The Nature of the General Legal Obligations Imposed on States Parties to the Covenant", *supra* note 9, ¶ 10.

17. *See, e.g.*, Loizidou v. Turkey (Preliminary Objections), 1995-Eur. Ct. H.R. 1, ¶¶ 61-62 (1995).

18. *See, e.g.*, Alexandre v. Cuba, Case 11.589, Inter-Am. Comm'n H.R. Report No. 109/99, ¶ 23 (1999).

19. *See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2005 I.C.J. Reports at ¶ 109; Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005 I.C.J. Reports (Dec. 19, 2005).

20. *See, e.g., Loizidou*, 1995-Eur. Ct. H.R. at ¶ 61-62; Alexandre, Inter-Am. Comm'n H.R. Report No. 109/99 at ¶ 23 (1999); Issa And Others v. Turkey, 2004-II, Eur. Ct. H.R., 1 (2004).

control. The personal model has been applied in situations where State forces have captured, arrested or detained individuals in foreign jurisdictions.[21] The European Court of Human Rights has also determined that a State exercised jurisdiction where its forces were physically beating an individual, finding that the act of beating brought the individual under the State's authority and control.[22]

In their simplest sense, these models suggest that a State would be bound to respect the human rights of individuals in cyberspace where these individuals are within its territory, in territory under its control, or when the individual is in the hands of a State agent.

However, as currently defined, the spatial and personal models of extra-territorial jurisdiction and application of human rights law remain unsatisfying for application to cyberspace. Indeed, for the most part, the debate in this area has revolved around a questionably analogous situation: the State's security forces' exercise of physical force. It remains unclear if a State's control over a territory or a person through cyber means can also trigger the application of human rights law, even if, as Marco Milanovic points out, "virtual methods can accomplish the exact same thing as physical ones, [and thus] there seems to be no reason to treat them differently and insist on some kind of direct corporeal intervention."[23] Crucially, could a cyber operation or an act of foreign cyber-surveillance bring an area, or an individual outside the territory of the State (and the control of its security forces), under that State's jurisdiction?

The answer is unclear. However, human rights law may yet develop around an understanding that cyber operations (in addition to physical acts) may also trigger the extra-territorial application of international human rights law, or at least some elements of it, in some circumstances. The Human Rights Committee has already indicated its position in this regard, suggesting that extra-territorial surveillance does implicate the ICCPR, by raising concerns "about the surveillance of communications in the interest of protecting national security, conducted by the National Security Agency (NSA) both within *and outside the United States*" (emphasis added).[24]

An argument can also be made that human rights law applies where a State intercepts data on its own territory that belongs to an individual outside its territory. In its 2008 judgment in the case of *Liberty and Others v. United Kingdom*, the European Court of Human Rights held that the UK violated the European Convention right to privacy through legislation that provided wide

21. *See, e.g.,* U.N. Human Rights Comm., Lopez Burgos v. Uruguay, ¶¶ 12.1-12.2 (July 12, 1981); Ocalan v. Turkey, 2005-Grand Chamber, Eur. Ct. H.R. 1, ¶ 91 (2005).

22. Isaak and Others v. Turkey, 2006-IV, Eur. Ct. H.R. 1, 21 (2006).

23. Marko Milanovic, *Foreign Surveillance and Human Rights, Part 4: Do Human Rights Treaties Apply to Extraterritorial Interferences with Privacy?* EJIL:TALK, (Nov. 2013), http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-4-do-human-rights-treaties-apply-to-extraterritorial-interferences-with-privacy/.

24. Human Rights Comm., *Concluding Observations on the Fourth Periodic Rep. of the United States*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014).

scope for executive authorities to undertake extraterritorial surveillance.[25] The case related to communications between the claimant NGOs in Ireland and the UK that ran through a cable in the UK. Legislation gave the UK authorities extensive power to capture and read emails originating from outside the UK in order to protect national security or economic interests. The extra-territorial location of the Irish claimants was not identified as a barrier to the finding of an Article 8 violation of the European Convention on Human Rights. The United Nations Office of the High Commissioner for Human Rights (OHCHR), has also suggested human rights law would apply where a State exercises its power or effective control in relation to digital communications infrastructure wherever located, for example through direct tapping or penetration of communication infrastructure located outside that State's territory.[26]

Finally, it is also important to note that human rights law applies to cyber operations in the context of armed conflict, subject to the operation of international humanitarian law (IHL, or the law of armed conflict) as *lex specialis.*[27] Cyberattacks that neither trigger application of IHL nor occur in the context of armed conflict are subject to human rights law and not to IHL.

II. THE DUTY TO RESPECT HUMAN RIGHTS IN CYBERSPACE

A. A Fertile Field for the Violation, and Exercise, of Rights

David Kaye, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (since August 2014), notes that contemporary digital technologies, including cyber technologies, offer "unprecedented capacity" for States to interfere with a range of human rights.[28] It is certainly the case that the arrival of cyberspace enables

25. Liberty and Others v. the United Kingdom, 2008-IV Eur. Ct. H.R. 1 (2008). OHCHR has also argued in the cyber context that a State's human rights obligations are triggered where the State exercises regulatory jurisdiction over a third party that physically controls individuals' data, or if a State asserts jurisdiction over the data of private companies as a result of the incorporation of those companies in that country. In such circumstances, the human rights obligations of the State are arguably triggered in connection with all those affected, wherever they are located.

26. Rep. of the Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, ¶ 34, U.N. Doc. A/HRC/27/37 (June 14, 2014); Report of the United Nations High Commissioner for Human Rights on the Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Human Rights Council, ¶ 41, U.N. Doc. A/HRC/13/36 (Jan. 22, 2010).

27. United Nations Human Rights Comm., General Comment No. 31, ¶ 11, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004). Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Reports 226, ¶ 25 (July 8, 1996); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2005 I.C.J. Reports 142, ¶ 106 (July 9, 2004); *see also* Report of the International Commission of Inquiry to Investigate All Alleged Violations of International Human Rights Law in the Libyan Arab Jamahiriya, 5, 41, U.N. Doc. A/HRC/17/44 (June 1, 2011); Third Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, 45, U.N. Doc. A/HRC/21/50, (August 14, 2012).

28. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 1.

States to surveil, harass and undermine the rights of individuals in invidious new ways. At the same time, cyberspace is also becoming an increasingly important forum for individuals to enjoy and express their human rights. Harold Hongju Koh, then Legal Advisor to the U.S. Department of State, recognized this when he stated that "[Cyber communication] is increasingly becoming a dominant mode of expression in the 21st century. More and more people express their views not by speaking on a soap box at a Speakers' Corner, but by blogging, tweeting, commenting, or posting videos and commentaries."[29] Cyber is indeed becoming an increasingly central forum for the exercise of a host of other rights as people increasingly look to the Internet to access information, form connections with others, and organize social life. In this context, it is crucial that States refrain from using cyber technology to violate human rights and must likewise refrain from interfering with or curtailing the enjoyment of human rights in cyberspace.

B. Interfering with Access to Online Content and Websites

International human rights law protects the right to hold and express opinions, to seek, receive and impart information, as well as to peacefully assemble and associate[30] Restricting or blocking specific online content[31] may interfere with these rights. As a general rule, these rights require that there should be as little interference as possible by States to freedom of expression and the flow of information, and this holds true also for cyberspace. Limitations, which should conform to criteria established under international human rights law, must be the exception.[32] Typical forms of expression that should not ordinarily be subject to restrictions, either offline or online, include discussion of government policies and political debate; reporting on human rights, government activities and corruption in government; engaging in election campaigns, peaceful demon-

---

29. Harold Hongju Koh, Legal Advisor to the U.S. Dep't of State, Prepared Remarks before the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm. However, members of the Shanghai Cooperation Organization have taken a restrictive position of rights on the Internet. *See* СОГЛАШЕНИЕ МЕЖДУ ПРАВИТЕЛЬСТВАМИ ГОСУДАРСТВ – ЧЛЕНОВ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [Agreement between the Gov'ts of the Member States of the Shanghai Cooperation Org. on Cooperation in the Field of Int'l Info. Sec.], Annexes 1–2 (2009).

30. Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 82, U.N. Doc. A/HRC/17/27 (May 16, 2011).

31. Blocking refers to measures taken to prevent certain content from reaching an end user. This includes preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions, the taking down of websites from the web server where they are hosted, or using filtering technologies to exclude pages containing keywords or other specific content from appearing. *Id.* at ¶ 29.

32. Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 12, U.N. Doc. A/HRC/66/290 (Aug. 10, 2011); Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 30 at ¶ 68.

strations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups.[33]

As in the offline world, States must refrain from creating "insurmountable barriers" to the right to access information in cyberspace by "criminalizing online expression, intimidating political opposition and dissenters and applying defamation and lese-majesty laws to silence journalists, defenders and activists."[34] When attributable to the State, cyberattacks against websites hosting legitimate expression also constitute an interference with the right to respect freedom of opinion and expression.[35] In this regard, Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (between August 2008 and July 2014) has noted his deep concern "that websites of human rights organizations, critical bloggers, and other individuals or organizations that disseminate information that is embarrassing to the State or the powerful have increasingly become targets of cyber-attacks."[36]

The prohibition under human rights law against restricting certain forms of expression or blocking sites that facilitate individuals' ability to access their economic, social and cultural rights, such as valid health information or services,[37] also serve to prohibit the State from taking such action on the Internet.[38] At the very least, this can be seen as an interference with these rights, which may only be permitted in certain limited circumstances in line with human rights law.

C. Conducting Surveillance

The right to privacy, among other rights, will also be implicated in cyber operations undertaken by States, including operations that involve surveillance, the interception of digital communications of individuals, or the collection of personal data. It is clear, for example, that the right to privacy includes the right

---

33. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (May 16, 2011), *supra* note 30 at ¶ 37 (citing Human Rights Council Res. 12/16, U.N. Doc. A/HRC/RES/12/16 at ¶ 5 (p)(i) (Oct. 12, 2009)). Similarly, the Human Rights Committee has asserted that article 19, paragraph 3, of the International Covenant on limitations "may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights." Human Rights Comm., Gen. Comment No. 34 on Art. 19: Freedoms of Opinion and Expression, ¶ 23, U.N. Doc. CCPR/C/GC/34 (Nov. 2, 1999).

34. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 23.

35. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 30, at ¶ 81.

36. *Id.* at ¶ 80.

37. *See, e.g.*, Comm. On Econ., Soc. And Cultural Rights, Gen. Comment No. 14 on Substantive Issues Arising in the Implementation of the Int'l Covenant on Econ., Soc., and Cultural Rights: The Right to the Highest Attainable Standard of Health, ¶ 3, U.N. Doc. E/C.12/2000/4 (Aug. 11, 2000).

38. *See also* David P. Fidler, *Cyberspace and Human Rights*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 106 (Nicholas Tsagourias & Russell Buchan eds., 2015).

to respect for digital communications.[39]

The reading and retention of the *content* of online communications intended to be confidential certainly interferes with the right to privacy. The right to privacy in human rights law requires that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*. "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read."[40] That "correspondence" includes cyber communications is affirmed in a number of cases.[41] Thus, the European Court of Human Rights has reiterated that the mere existence of legislation which allows for the secret monitoring of communications amounts to an interference with the right to privacy, irrespective of any measures actually taken against individuals.[42]

International human rights law also suggests that the capture and retention of *communications data* (metadata) also constitutes an interference with the right to privacy where linked to the individual. This is the case even if the content of the communication is not read, because it is possible to obtain a large amount of information about a person from their communications data.[43] In 2014 the European Court of Justice determined that a requirement that providers of publicly available electronic communications services or of public communications networks retain, for a certain period, data relating to a person's private life and to his communications, for the purpose of possible access to them by the competent national authorities, directly and specifically affects private life and consequently, violates relevant articles of the EU Charter of Fundamental Rights.[44] In doing so, it also held that the collection and retention of both communications content and metadata amounts to an interference with privacy whether or not the data is sensitive, and whether or not the persons concerned

39. *See* G.A. Res. 68/167 (Dec. 18, 2013); Rep. of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, ¶¶ 16-18, U.N. Doc. A/69/397 (Sept. 23, 2014); *see also* Copland v. United Kingdom, 45 Eur. Ct. H.R. 37 (2007); Weber and Saravia v. Germany, 46 Eur. Ct. H.R. 47, ¶ 77 (2006).

40. Human Rights Comm., Gen. Comment No. 16 on Art. 17 (Right to Privacy), ¶ 8, U.N. Doc. HRI/GEN/1/Rev.9 at 192 (1988).

41. *See e.g., Copland*, 45 Eur. Ct. H.R. 37; *see also* G.A. Res. 68/167 (Dec. 18, 2013); U.N. Secretary-General, *supra* note 39 at ¶¶ 16–18.

42. *See Weber and Saravia*, 46 Eur. Ct. H.R. at ¶ 78.

43. By combining and aggregating information derived from communications data, it is possible to identify an individual's location, associations, and activities. *See* Rep. of the Office of the U. N. High Comm'r for Human Rights, *supra* note 26, at ¶19 ("In the absence of special safeguards, there is virtually no secret dimensions of a persons' personal life that would withstand close metadata analysis."); *see also* Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Nat. Res., ECLI:EU:C:2014:238, ¶¶ 26-29, 37 (Apr. 8, 2014) ("[communications metadata] taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained . . . it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed" and "the retention of data for the purpose of possible access to them by the competent national authorities [as provided for by the EU directive in question] directly and specifically affects private life.").

44. *See* Case C-293/12, *Digital Rights Ireland*, *supra* note 43, at ¶¶ 29-34.

have been inconvenienced in any way.[45]

Human rights law is less clear about State interference with cyber-specific technologies designed to protect privacy, such as encryption. This is yet to be addressed by any international judicial body, and there is little in the way of a clear offline analog. Arguably, however, actions to compel the identification of users will at least constitute an interference with the right to privacy that would need to be lawfully justified, as would measures to prohibit, restrict or undermine access to devices that support encryption and anonymity. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, asserted this claim, stating that "Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys."[46] Likewise, his successor David Kaye also added in 2015 that encryption alone might be insufficient to enable individuals to protect their privacy, given the power of metadata analysis. In such cases, only by engaging online anonymously will individuals be able to protect their right to privacy, and any interference with a person's ability to engage on the Internet anonymously is likewise an interference with their right to privacy.[47]

It is widely recognized that privacy is also critical to the protection and promotion of other human rights,[48] including freedom of opinion and expression,[49] and freedom of peaceful assembly and association – "rights all linked closely with the right to privacy and, increasingly, exercised through digital

45. *See id*. at ¶ 33. *See also* Rep. of the Office of the U. N. High Comm'r for Human Rights, *supra* note 26, at ¶ 20.

46. Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 89, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).

47. Encryption alone may be insufficient to enable an individual to protect their privacy, given the power of metadata analysis "to specify an individual's behaviour, social relationships, private preferences and identity." *See* Rep. of the Office of the U. N. High Comm'r for Human Rights, *supra* note 26, at ¶ 19; Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 17.

48. The U.N. General Assembly has recognized privacy as a "gateway" to other rights. G.A. Res. 68/167 U.N. Doc. A/RES/68/167 (Jan. 21, 2014); *see also* Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 46; Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 47.

49. Rep. of the Special rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 46 at ¶ 79; *see also id*. at ¶ 11 ("an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today."); Council of Europe, Comm. Of Ministers, Declaration on Freedom of Communication on the Internet, Principle 7 (May 28, 2003), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dfbd5 ("Anonymity may be essential to the exercise of freedom of opinion and freedom of expression on the Internet and online context."); *see also* R v. Spencer, [2014] 2 S.C.R. 212, 234 at ¶ 43 (Can.); *Totalise PLC v. The Motley Fool Ltd. & Anor*, [2001] 29 E.M.L.R. 750 (QB); *Sheffield Wednesday Football Club Ltd. v. Hargreaves*, [2007] EWHC 2375 (QB); Oberlandesgericht [OLG] [Higher Regional Court of Hamm], Oct. 3, 2011, Case I-3 U 196/10 (Ger.), http://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I_3_U_196_10beschluss20110803.html.

media."[50] In this context, actions by States that interfere with the ability of individuals to communicate securely or anonymously in cyberspace may thus also interfere with a range of other rights, the enjoyment of which is dependent on the right to privacy, such as rights related to freedom of expression, association, peaceful assembly, etc. This will also be the case where the fear of unwilling disclosure of online activity, such as search and browsing, deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes, or where individuals and groups face unlawful restrictions on content, or where they risk arbitrary and unlawful interference or attacks when expressing themselves in a manner protected under human rights law.[51]

Arguably, economic, social and cultural rights, such as the right to health, may also be interfered with by cyber surveillance practices, including where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised.[52] Again, where rights are interfered with, the onus would be on the State to demonstrate that such interference complies with permissible restrictions to these rights as set out in human rights law.

Interestingly, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (David Kaye) has asserted that the right *to hold an opinion* may also be implicated by surveillance, and by interference with the use of anonymity and encryption software. This argument is an important one because, unlike the rights to freedom of expression and privacy, the right to freedom of opinion is absolute and cannot be restricted.[53] The Special Rapporteur notes that in offline circumstances, physical harassment, detention or subtler efforts to punish individuals for their opinion may be recognized as interference with the right to hold an opinion and that such protection thus must be recognized as extending to the cyber domain, as individuals regularly hold opinions digitally.[54] According to his analogy, "(i)nterference [with the right to hold opinions] may also include such efforts as targeted surveillance, distributed denial of service (DDoS) attacks,[55] and online and offline intimidation, criminalization and harassment of people engaged in cyber activities. Restrictions on encryption and anonymity must also be as-

50. Rep. of the Office of the U. N. High Comm'r for Human Rights, *supra* note 43, at ¶14.

51. *See* Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 47, at ¶¶ 16, 21.

52. *See* Rep. of the Office of the U. N. High Comm'r for Human Rights, *supra* note 26, at ¶ 14.

53. *See* Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3 at ¶ 19; ICCPR, *supra* note 7, at art. 19.1.

54. *See* Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 20 (stating "individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives.").

55. A DDoS attack involves flooding the target site with Internet traffic, so that it slows or is temporarily knocked offline.

sessed to determine whether they would amount to an impermissible interference with the right to hold opinions."[56]

D. Restricting Protest

Protest is also increasingly going digital. The Internet is now used to organize offline acts of protest, and is also a forum for acts of protest. Online forums including popular social networking sites are being used as a platform for civil and political action. Human rights law developed in the offline world also protects online protest. Certain forms of non-violent direct action are contemplated under the right to freedom of expression and so, by extension, analogous forms of protest (and disruption) online may well be permissible.

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, has also noted that freedom of association and assembly "often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors."[57] These may be threatened by surveillance and/or restrictions to the use of anonymity or encryption technology. The UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, likewise asserted, following a visit to the UK, that "(t)he practice of surveillance and intelligence databases undeniably has a chilling effect on protestors who fear to hold further protests."[58] Much of this surveillance and holding of intelligence databases occurs online.

Again, there is less clarity regarding how human rights law would apply to certain forms of direct action unique to cyber, and whether certain online actions are indeed analogous to offline actions protected under human rights law. Debate has emerged, for example, concerning the right to non-violent online protest that seeks to cause disruption, including where activist groups are able to target online infrastructure and temporarily shut it down. For example, in 2010 the "hacktivist" group Anonymous launched a DDoS attack on a number of online institutions, including PayPal, in retaliation for their freezing the assets of, and donations to, Wikileaks. Anonymous used the same tactic in a 2013 protest against the detention of one of its programmers. Arguably, such forms of non-violent disruption online should in some circumstances be protected as a cyber-corollary of certain forms of protest and disruption tradition-

56. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 24.

57. Human Rights Council, Rep. of the Special Rapporteur promotion and protection of human rights and fundamental freedoms while countering terrorism, ¶ 36, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009).

58. Human Rights Council, Rep. of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Addendum, Mission to the United Kingdom of Great Britain and Northern Ireland, ¶32, U.N. Doc. A/HRC/23/39/Add.1 (May 29, 2013).

ally protected offline under the right to freedom of expression.[59] The Executive Director of the Freedom of Expression NGO, Article 19, for example asserts that actions such as DDoS attacks and site redirects are the equivalent of a sit-in or act of peaceful civil disobedience and that "disruptive tactics do not negate the legitimacy of protest: this is as true online as offline."[60] This position remains contested. Others have argued that DDoS attacks cannot be treated in the same way as offline non-violent but disruptive protests, as a small number of activists engaged in DDoS attacks could have a hugely disruptive effect online.[61] A German court has been reported to have recognized a "call for action" by a German online activist calling for DDoS attacks as a protected form of protest.[62] The court decision was said to pivot on the point that these actions were oriented to influence the public, and through that avenue, influence the actions of the Lufthansa corporation, rather than an act of force intended to compel an action from Lufthansa. This is not, however, widely accepted. Members of Anonymous have for example been tried and harshly sentenced under the USA's Computer Fraud and Abuse Act, for non-violent, temporarily disruptive protest action online.

III. THE DUTY TO ENSURE RESPECT (PROTECT AND FULFILL) FOR HUMAN RIGHTS IN CYBERSPACE

A. The Duty of States to Ensure Respect by Third Parties for Rights in Cyberspace

Human rights law requires States to not only respect, but to also take positive action to protect the enjoyment of rights. Thus, States must take a number of actions online and offline in relation to third parties, in order to ensure that individuals can realize their rights online, and, at the same time, that cyberspace is not used to attack the human rights of others.[63] Since regulation intended or designed to protect the exercise of human rights in cyberspace from the actions

59. Thomas Hughes, *Hacktivism to Balaclava Punk: Protest Must Be Protected in All Its Forms*, HUFFINGTON POST (June 22, 2015), http://www.huffingtonpost.co.uk/thomas-hughes/right-to-protest_b_7620410.html.

60. *Id.*

61. German precedent upholds online civil disobedience, COURAGE (Oct. 22, 2014), https://couragefound.org/2014/10/german-precedent-upholds-online-civil-disobedience/.

62. *Id.*

63. ICCPR, art. 2.1 ("Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind."); *see also* Human Rights Comm., General Comment No. 3: Implementation at the National Level, ¶1, U.N. Doc. HRI/GEN/R/Rev.1 (July 29, 1981) ("[T]he obligation . . . is not confined to the respect of human rights, but that States parties have also undertaken to ensure the enjoyment of these rights to all individuals under their jurisdiction."); Human Rights Comm., General Comment No. 31: The Nature of the General Legal Obligations Imposed on States Parties to the Covenant, ¶ 7, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004) ("Article 2 [of the ICCPR] requires that States Parties adopt legislative, judicial, administrative, educative and other appropriate measures in order to fulfill their legal obligations.").

of third parties may also constitute interference with their human rights, these restrictions must also comply with international human rights standards relating to restrictions/limitations of human rights.

The vast amount of personal information that is made available online, including through social networking sites, poses serious concerns regarding the rights of Internet users vis-a-vis third parties, and gives rise to questions such as who may gain access to specific personal information, how the information may be used, and whether, and for how long, the information may be stored. States are therefore obligated to "provide such safety in law and policy that will allow individuals to secure themselves online."[64]

A high-profile European Court of Justice (ECJ) decision highlights the intersection of the duty to respect and the duty to ensure respect. The European Union's Data Protection Directive[65] provides that transfer of personal data to another country may, in principle, take place only if that third country ensures an adequate level of protection of the data.[66] Data provided by EU residents to Facebook is transferred from Facebook's Irish subsidiary to servers located in the United States, where it is processed.[67] Upon learning of the 2013 revelations by U.S. National Security Agency contractor Edward Snowden, Maximillian Schrems, an Austrian citizen and Facebook user, complained to the Irish supervisory authority (the Data Protection Commissioner) that the United States does not offer sufficient protection against surveillance by the public authorities of the data it receives from other countries.[68] The Irish authority rejected the complaint, on the ground, in particular, that in a decision of 26 July 2000 the Commission considered that, under its 'safe harbor' scheme, the United States ensures an adequate level of protection of the personal data transferred.[69] The ECJ felt otherwise. It determined that the Irish authority's reliance on the U.S. safe harbor provisions, which are merely voluntary and subject to caveats, was misplaced. In so deciding, the ECJ confirmed the obligation of European authorities to respect Schrems' right to private life and his right to effective

64. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra note* 28, at ¶ 11; Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶¶ 53-59 U.N. Doc. A/HRC/17/27 (May 16, 2011) ("In a digital age, protecting . . . rights demands exceptional vigilance."); Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra note* 28, at ¶ 18 ("States are obliged to protect privacy against unlawful and arbitrary interference and attacks."). Relating specifically to enacting legislation, *see also id.* (States must ensure "the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors."); Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 46, at ¶ 84 ("States should criminalize illegal surveillance by public or private actors.").

65. Council Directive 95/46/EC, ¶ 31, 1995 O.J. (L 281).

66. Court of Justice of the European Union Press Release 117/15, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid (Oct. 6, 2015).

67. *Id.*

68. *Id.*

69. *Id.*

judicial protection of his rights guaranteed by the European Charter. The decision also served to protect against the violation of Schrem's rights by the United States.[70]

States are also required to put in place effective measures to protect against attacks aimed at silencing those exercising their rights, such as freedom of expression, on as well as offline. This includes measures to protect journalists against threats, intimidation and attacks because of their activities.[71] It also includes measures to protect persons who engage in gathering and analysis of information on human rights conditions and who publish human rights-related reports, including judges and lawyers.[72] All such attacks should be subject to accountability mechanisms, including remedies, discussed below.

B. The Duty to Protect Individuals from Rights Violations Emanating from Cyberspace

Obviously, "the Internet [may] be abused to interfere with the rights of others, national security, or public order."[73] Thus, in addition to taking action to ensure that individuals are protected and can exercise their rights online, the State must ensure that individuals are protected from human rights abuses including those that are initiated in cyberspace by third parties.

In this regard, the State is required to criminalize exceptional types of action/expression, including online. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank Le Rue) has suggested that these include: direct and public incitement to genocide,[74]

---

70. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015). *Schrems*, and other decided and pending cases concerning data protection before the ICJ, the European Court of Human Rights and national courts of EU member states have been collected and summarized in a publication of the European Data Protection Supervisor. *Case Law Overview 1 December 2014–31 December 2015* (Eur. Data Prot. Supervisor, Working Paper), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/MembersMission/Members/Documents/16-03-15_Case_Law_Overview_2015_EN.pdf.

71. *See, e.g., Concluding Observations of the Human Rights Committee: Algeria*, U.N. Doc. CCPR/C/DZA/CO/3 (Nov. 1, 2007); *Concluding Observations of the Human Rights Committee: Costa Rica*, U.N. Doc. CCPR/C/CRI/CO/5 (Nov. 16, 2007); *Concluding Observations of the Human Rights Committee: Sudan*, U.N. Doc. CCPR/C/SDN/CO/3 (July 26, 2007).

72. *See* Njaru v Cameroon, Communication No. 1353/2005, U.N. Doc CCPR/C/89/D/1353/2005 (March 19, 2007); *Concluding Observations of the Human Rights Committee: Nicaragua*, U.N. Doc. CCPR/C/NIC/CO/3 (June 10, 2009); *Concluding Observations of the Human Rights Committee: Tunisia*, U.N. Doc. CCPR/C/TUN/CO/5 (Apr. 23, 2008); *Concluding Observations of the Human Rights Committee: Syrian Arab Republic*, U.N. Doc. CCPR/CO/84/SYR (Aug. 9, 2005); *Concluding Observations of the Human Rights Committee: Colombia*, U.N. Doc. CCPR/CO/80/COL (May 26, 2004).

73. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra note* 3, at ¶ 2.

74. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra note* 32, at ¶ 23 (International criminal law prohibits direct and public incitement to commit genocide under article 3 of the Convention on the Prevention and Punishment of the Crime of Genocide, article 25, 3 (e), of the Rome Statute of the International Criminal Court, article

child pornography,[75] and incitement to national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[76] As regulation in each of these areas will constitute restrictions to the right of freedom of expression, again, such regulation must also comply with international human rights standards relating to restrictions/limitations.[77] Likewise, the Internet may be used for terrorist purposes.[78] "States have both a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights," although clearly "[c]ounterterrorism initiatives relating to Internet use may have an impact on the enjoyment of a range of human rights, including the rights to freedom of speech, freedom of association, privacy and a fair trial."[79]

4, 3 (c), of the statute of the International Tribunal for the Former Yugoslavia, and article 2, 3 (c), of the statute of the International Criminal Tribunal for Rwanda).

75. *Id.* at ¶¶ 20-22 (The dissemination of child pornography is explicitly prohibited under international law, notably in the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. The Optional Protocol requires States parties to ensure that, at a minimum, producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography (for purposes set out in article 3) are fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis (article 3, para. 1 (c)).). As noted by the Special Rapporteur on the sale of children, child prostitution and child pornography in her report to the Human Rights Council, the relevant legislation should be clear and comprehensive and should treat child pornography on the Internet as a grave violation of the rights of the child and as a criminal act. Human Rights Council, Rep. of the Special Rapporteur on the sale of children and child pornography, at 2, U.N. Doc. A/HRC/12/23 (July 13, 2009). *See also*, Convention on Cybercrime Treaty art. 9, Jan 7, 2004, C.E.T.S. No. 185.

76. G.A. Res. 260/3, art. 3, U.N.T.S. No. 1021 (Dec. 9, 1948); ICCPR art. 20; *see also* International Convention on the Elimination of All Forms of Racial Discrimination, art. 4, Dec. 21, 1965, 660 U.N.T.S. 195 (States parties shall declare all dissemination of ideas based on racial superiority or hatred and incitement to racial discrimination an offence punishable by law); Committee on the Elimination of Racial Discrimination general recommendation, U.N. Doc. A/48/18 at 114 ("in the opinion of the Committee, the prohibition of the dissemination of all ideas based upon racial superiority or hatred is compatible with the right to freedom of opinion and expression"); Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra note* 32 at ¶¶ 23-25.

77. The Special Rapporteur for freedom of expression has identified a distinction between three types of expression:

> (a) expression that constitutes an offence under international law and can be prosecuted criminally; (b) expression that is not criminally punishable but may justify a restriction and a civil suit; and (c) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others. These different categories of content pose different issues of principle and call for different legal and technological responses.

Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 66th Sess., U.N. Doc. A/66/290, ¶ 18 (Aug. 10, 2011). The European Court of Human Rights has likewise emphasized that the authorities should display restraint in resorting to criminal proceedings in the case of *Feret v. Belgium*. Press Release, European Court of Human Rights, Chamber Judgment, Feret v. Belgium (July 16, 2009).

78. *See* United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, ¶¶ 1-37 (2012).

79. *Id.* at ¶ 33. For an extensive analysis of cybercrime laws related to terrorism in the human rights context, see *id.*, at ¶¶ 80-88.

In this regard, the possible measures that States may take to counter terrorism online are obviously not unlimited.

In addition to types of actions/expression that they are required to criminalize, States are also under an obligation to take steps short of criminalization to protect a range of rights from abuse, including in cyberspace. The State is required, for example, to take steps to protect people from harassment and violence, including sexual harassment, and to protect children from violence and bullying.[80] In the case of *K.U. v. Finland*, interpreting the right to privacy under the ECHR, the European Court of Human Rights (ECtHR) confirmed that States have positive obligations that apply to cyberspace. The case concerned an advertisement placed on an Internet dating site in the name of a 12-year-old boy without his knowledge, suggesting he was looking for an intimate relationship. The courts in Finland dismissed a petition by the boy's family to oblige the service provider to divulge the identity of the IP address of the individual who placed the advertisement. In finding a violation of the right to privacy, the ECtHR asserted that the object of the Article 8 right to privacy "does not merely compel the State to abstain from [. . .] interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life."[81] These include "a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person . . . and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution."[82] Thus, the Court found that it was a violation of petitioner's rights for the State not to compel the internet service provider to divulge to police the identity of the individual who placed the advertisement. Again, the Court affirmed that "(a)lthough 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" and it is "the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.'[83]

C. The Duty to Provide a Remedy

Victims of human rights violations have a right to an effective remedy,[84] and this applies to violations online. Effective remedies for violations in or through

80. *See, e.g.*, K.U. v. Finland, 2008-V Eur. Ct. H.R. 125 (2008).

81. *Id.*, at ¶ 42 (citing Airey v. Ireland, 32 Eur. Ct. H.R. (ser. A) 32 (1979)).

82. *Id.*, at ¶ 46.

83. *Id.*, at ¶ 49.

84. Article 2(3)(a) of the ICCPR requires that States, "[E]nsure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;" article 2(3)(b) further specifies that States parties to the Covenant undertake, "To ensure that any person claiming such a remedy shall

cyberspace can come in a variety of judicial, legislative or administrative forms. For a remedy to be effective, it must be known and accessible to anyone who claims that his or her rights have been violated.

There is little doubt that the right to remedy also applies online (see, for example*, K.U. v Finland*, as set out above). However, the implementation of the right to an effective remedy becomes particularly contested in the context of cyber-surveillance regimes. One concern especially relevant in this context is that individuals are often unaware of interference with their rights. Indeed, it would be hard to see how the right to remedy for unlawful surveillance may be effective where individuals are not aware that they are being surveilled. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (David Kaye) has argued in this regard that, "individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data."[85] Of course, such rights are subject to limitation as discussed above and obviously in certain cases of targeted surveillance, at least, giving affected persons advance or concurrent notification might jeopardize the effectiveness of the surveillance.

The European Court of Human Rights has responded to this problem by noting the importance of procedures (independent monitoring mechanisms) "to provide adequate and equivalent guarantees safeguarding (a person's) rights"[86] during the period in which surveillance is initiated and carried out. At the same time, it has required additionally that after the surveillance has been terminated, the individual concerned must be advised of the measures taken without his or her knowledge in order to challenge their legality retrospectively[87] or, in the alternative, that any person who suspects that his or her communications are being or have been intercepted must be able to apply to courts, "so that the courts' jurisdiction does not depend on notification to the interception subject

---

have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy." International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), art. 2(3) (Dec. 16, 1966). States must also ensure that the competent authorities enforce such remedies when granted. *Id.* The Human Rights Committee has emphasized in its General Comment No. 31, failure by a State party to investigate allegations of violations could in and of itself give rise to a separate breach of the Covenant. Human Rights Comm., General Comment No. 31, Nature of the General Legal Obligation on States Parties to the Covenant, 80th Sess. U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004); *see also* Human Rights Comm., General Comment 16, Right to Privacy, 23rd Sess., U.N. Doc. HRI/Gen/1/Rev.9 (Apr. 8, 1988); Human Rights Comm., Bulgakov v. Ukraine, Communication No. 1803/2008, 106th Sess., U.N. Doc. CCPR/C/106/D/1803/2008 (Nov. 29, 2012).

85. Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29th Sess., U.N. Doc. A/HRC/29/32, ¶ 18 (May 22, 2015).

86. Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R., ¶ 233 (Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324.

87. *Id.* at ¶ 234; Weber and Saravia v. Germany, 2006-XI Eur. Ct. H.R. 309, ¶ 135 (2006); *see also* Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 23rd Sess., U.N. Doc. A/HRC/23/40, ¶ 82 (Apr. 17, 2013).

that there has been an interception of his communications."[88]

D. Is There a Positive Duty to Facilitate Access to Cyberspace or to Certain Online Content?

The Internet has become an essential venue for enjoyment of civil and political and social, economic, and cultural rights. Indeed, cyberspace has become a medium to advance realization of human rights. A State's "positive obligations" to exercise its commitments under human rights treaties, including progressive realization of social, economic and cultural rights,[89] may require the State to take certain actions with regard to cyberspace.

To fulfill the right to freedom of expression, States have a duty to facilitate access to cyberspace. The free flow of information across borders remains essential to realization of the human rights of freedom of opinion and expression regardless of the medium,[90] including in cyberspace.[91] The Human Rights Council has stated that "[a]ccess to and use of information technologies and the media of one's choice, including . . . the Internet, should be promoted and facilitated at the national level . . . as an integral part of the enjoyment of the fundamental rights to freedom of opinion and expression."[92] Likewise, access to the Internet is increasingly central to the exercise of other civil and political rights, such as the right to freedom of association and assembly, which States are also obliged to promote/fulfill.[93] States' efforts to facilitate access to the

88. *Zakharov*, *supra* note 86, at ¶ 234; *see also* Kennedy v. United Kingdom, App. No. 26839/05, Eur. Ct. H.R., ¶ 167 (May 18, 2010), http://hudoc.echr.coe.int/eng?i=001-98473.

89. International Covenant on Economic, Social and Cultural Rights, art. 2(1), G.A. Res. 2200A (XXI) (Dec. 16, 1966). *See also* Human Rights Council, General Comment 3, The Nature of States Parties' Obligations, 5th Sess., U.N. Doc. E/1991/23, ¶ 1 (Dec. 14, 1990); G.A. Res. 24/21, ¶ 1, U.N. Doc. A/HRC/24/L.24 (Oct. 9, 2013) (States have an obligation to "respect and fully protect the civil, political, economic, social and cultural rights of all individuals . . . online as well as offline . . .").

90. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, ¶ 19, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

91. G.A. Res. 36/103, ¶ 2(I)(c), U.N. Doc. A/RES/36/103 (Dec. 9, 1981) (noting the right of peoples to use information systems and mass media to promote their "political, social, economic and cultural interests and aspirations . . .").

92. Human Rights Council Res. 22/6, ¶ 7, U.N. Doc. A/HRC/22/L.13 (Apr. 12, 2013). The Human Rights Committee, in its general comment No. 34 on the right to freedom of opinion and expression, also underscored that States parties should take all necessary steps to foster the independence of new media, such as the Internet, and to ensure access of all individuals thereto. Human Rights Comm., General Comment No. 34, *supra* note 33; *see also,* Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 30, at ¶ 61 ("[T]he Special Rapporteur would like to reiterate that States have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, which includes the Internet."); *id.* at ¶¶ 67, 85 ("[E]nsuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy . . . to make the Internet widely available, accessible and affordable to all segments of the population."); Org. for Security and Cooperation in Eur. [OSCE], *Joint Declaration on Freedom of Expression and Access to Information* (June 1, 2011), http://www.osce.org/fom/78309 (stating that there is "an obligation on States to promote universal access to the Internet.").

93. "The Internet has been essential to accessing civil and political rights, as a 'political platform' and tool for mobilization." U.N. Human Rights Office of the High Commissioner, Realizing the Right

Internet may also contribute to meeting their obligation to progressively implement a number of economic, social and cultural rights, such as the right to education, to health, to work, and to full participation in political, cultural, social and economic life. The facilitation of access to the Internet and promotion of digital literacy may be an increasingly important/required step in meeting some of these obligations.[94]

That is not to say, however, that there is a right to the Internet, and States certainly have discretion as to how they will implement their positive cyber-related obligations under human rights law. Still, arguably, States may not cut off Internet access to their populations once it has been instated. For example, a joint Declaration on Freedom of Expression and responses to conflict situations – issued by the United Nations (UN) Special Rapporteur on freedom of opinion and expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on freedom of the media, the Organization of American States (OAS) Special Rapporteur on freedom of expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on freedom of expression and access to information, affirmed that "using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law."[95] At the same time, States are also encouraged to promote digital literacy among individuals under their jurisdiction. "In addition to the availability of relevant online content free of censorship, the Special Rapporteur [on the promotion and protection of the right to

---

to Development, U.N. Doc. HR/PUB/12/4, Sales No. E.12.XIV.1, at p.107, 126 fn. 25 (2013); *see also* Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Human Rights Council ¶¶ 32, 84(k), U.N. Doc. A/HRC/20/27 (May 21, 2012) ("The Special Rapporteur notes the increased use of the Internet . . . as [a] basic tool[] which enable[s] individuals to organize peaceful assemblies.").

94. Indeed, given that the Internet has become an indispensable tool for full participation in political, cultural,

> social and economic life, States should adopt effective and concrete policies and strategies, developed in consultation with individuals from all segments of society, including the private sector as well as relevant Government ministries, to make the Internet widely available, accessible and affordable to all.

Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 32, at ¶ 69. "The Special Rapporteur believes that access to the Internet will progressively be a key element of the right to education." *Id.* at ¶ 70. Note that the UN Committee on Economic, Social and Cultural Rights requires States to report on Article 15 of ICESCR, right to cultural life to "indicate the measures taken to promote broad participation in, and access to, cultural goods, institutions and activities, including measures taken [. . .] (b) To enhance access to the cultural heritage of mankind, including through new information technologies such as the Internet." Comm. on Economic, Social and Cultural Rights, Guidelines on Treaty-Specific Documents to be Submitted by States Parties under Articles 16 and 17 of the International Covenant on Economic, Social and Cultural Rights, E/C.12/2008/2 ¶ 67 (Mar 24, 2009).

95. Org. for Security and Cooperation in Eur. [OSCE], *Joint Declaration on Freedom of Expression and Access to Information* (June 1, 2011), *supra* note 92; *see also* Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 30, at ¶¶ 78–79.

freedom of opinion and expression, Frank La Rue] also notes the importance of ensuring that individuals possess the necessary skills to make full use of the Internet, or what is often referred to as 'digital literacy.'"[96]

States that have ratified the Convention on the Rights of Persons with Disabilities are under a specific obligation to "promote the availability and use of new technologies, including information and communications technologies . . . suitable for persons with disabilities, giving priority to technologies at an affordable cost,"[97] and "promote access for persons with disabilities to new information and communications technologies and systems, including the Internet."[98]

IV. LEGITIMATE RESTRICTIONS/LIMITATIONS ON THE EXERCISE OF HUMAN RIGHTS

Human rights law allows States to limit the enjoyment of certain rights in order to protect other rights and to maintain national security and public order, including in cyberspace. Indeed, wrongdoing takes place online as well as off and under certain circumstances, States have a right and duty to take restrictive measures on the Internet.[99]

Any restriction on human rights in cyberspace must be "provided" or "prescribed by law"[100] which meets "certain minimum qualitative requirements of clarity, accessibility, and predictability."[101] No interference can take place ex-

96. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, *supra* note 32, at ¶ 45 ("The Special Rapporteur encourages States to provide support for training in information and communications technology (ICT) skills, which can range from basic computer skills to creating web pages. In terms of the right to freedom of expression, course modules should not only clarify the benefits of accessing information online, but also of responsibly contributing information.").

97. Convention on the Rights of Persons with Disabilities, art. 4, ¶ 1(g), Dec. 13, 2006, 2515 U.N.T.S 3.

98. *Id.* at art. 9, ¶ 2(g).

99. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 13.

100. *See, e.g.*, ICCPR, *supra* note 7, at arts. 9.1, 12.3, 1.17; ECHR, *supra* note 7, at arts. 8-11; UN Comm'n on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, U.N. Doc. E/CN.4/1985/4, ¶¶ 15–18 (Sept. 28, 1984) (interpreting principles relating to the "Prescribed by Law" limitations clause of the ICCPR); Human Rights Comm., General Comment No. 16, *supra* note 40, at ¶ 4 (Arbitrary interference extends to "interference provided for under the law. The concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances"); Human Rights Comm., Toonen v. Australia, ¶ 8.3, U.N. Doc. CCPR/C/50/D/488/1992 (1994); Human Rights Comm.,Van Hulst v. Netherlands, ¶ 7.6, U.N. Doc. CCPR/C/82/D/903/1999 (2004); Copland, *supra* note 39; Yildirim v. Turkey, 2012-VI Eur. Ct. H.R. 505.

101. Human Rights Comm., General Comment No. 34, *supra* note 33, at ¶ 25 ("[A] 'law,' must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made available to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expressions are properly restricted and what sorts are not."); *see also* Sunday Times v. United Kingdom, App. No. 6538/74, Eur. Ct. H.R., ¶ 49 (Apr. 26, 1979) ("Firstly, the law must be adequately accessible: the citizen

cept in cases envisaged by the law and relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted.[102] Limitations or restrictions on human rights may only be lawful if they serve a legitimate purpose, which includes protection of the rights or reputations of others; national security, public order, public health or morals.[103] Where restrictions are justified, any interference must be limited to what is necessary[104] and proportionate to achieve a legitimate aim or objective.[105] Restrictions must be applied narrowly to avoid a legitimate objective being used as a pretext for an illegitimate restriction on human rights.[106]

The European Court of Human Rights affirmed, for example, in the 2012 case of *Yildirim v. Turkey* that permissible restrictions generally should be content-specific and that generic bans on the operation of certain sites and systems are not compatible with the right to receive and impart information. Given the importance of the Internet for freedom of expression, such prior restraint must be subject to most careful scrutiny and follow a particularly strict legal framework.[107] Ahmet Yildirim owned and managed a website hosted by Googlesites, which was among a number of sites blocked when the Turkish courts accepted that in order to block another site hosted on Googlesites (for violating Turkish law prohibiting insults to the memory of Ataturk), the government would, for technical reasons, need to block all sites hosted by that platform. The European Court found that the blocking order amounted to a

---

must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.").

102. Human Rights Comm., General Comment No. 16, *supra* note 40, at ¶¶ 3, 8.

103. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 33.

104. According to the European Court of Human Rights, "necessary" is more than "useful," "reasonable" or "desirable." *Sunday Times*, *supra* note 101, ¶ 49; *see also* Chaparro Alvarez v. Ecuador, 2007 Inter-Am. Ct. H.R. (Ser. C) No. 170, at ¶ 93 (Nov. 21, 2007) (stating that intrusions into privacy must be "necessary, in the sense that they are absolutely essential to achieve the purpose sought and that, among all possible measures, there is no less burdensome one in relation to the right involved, that would be as suitable to achieve the proposed objective.").

105. Human Rights Comm., General Comment No. 34, *supra* note 33, at ¶ 2; Human Rights Comm., Comm. No. 2156/2012: Views adopted by the committee at its 112th session, ¶¶ 9.3–9.4, U.N. Doc. CCPR/C/112/D/2156/2012 (Nov. 18, 2014); ECHR, *supra* note 7, at arts. 8 (right to privacy); ICCPR, *supra* note 7, at art. 19 (freedom of opinion and expression); ACHR, *supra* note 7, at art. 14 (freedom of expression). While Article 17 ICCPR does not explicitly stipulate that any restriction on the right to privacy must be necessary for a specified purpose, both the UN Special Rapporteur on counter-terrorism and the UN Special Rapporteur on freedom of expression have held that the "permissible limitations" test under Article 19 among other articles of the ICCPR, was equally applicable to Article 17 ICCPR.

106. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 33; Human Rights Comm., General Comment No. 31: "The Nature of the General Legal Obligations Imposed on States Parties to the Covenant," U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004).

107. *Yildirim*, 2012-VI Eur. Ct. H.R. 505.

violation of Yildirim's right to freedom of expression in part because it was not prescribed by law, as relevant Turkish legislation did not authorize the wholesale blocking of an entire online platform, as occurred here.

The Human Rights Council has also insisted that when a State invokes a legitimate ground for restriction of the right to freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, the necessity and the proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.[108] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue) has noted that limitations of freedom of expression on the Internet provided by law must be transparent and precise enough for the individual to understand the rules applicable to the case and the consequences that may result from an action.[109] States should provide full details regarding the necessity and justification for blocking a particular website; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue) has also argued that determination of what content is to be blocked should be undertaken by a competent judicial authority or a body that is independent of any political, commercial, or other unwarranted influences to ensure that blocking is not used as a means of censorship.[110] It is obviously inconsistent with human rights law "to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."[111]

Likewise, the ECtHR has raised concerns with domestic legislation containing sweeping grounds for intercepting communications, including broad national, military, economic security purposes, absent any indication of the particular circumstances under which an individual's communications may be intercepted. Most recently, in *Roman Zakharov v. Russia*, the Court affirmed that such broadly worded statutes confer an "almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance,"[112] noting that the

---

108. Human Rights Comm., General Comment No. 34, *supra* note 33; *see also* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 32, at ¶ 16.

109. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 30, at ¶ 24, 40, 42, 69.

110. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 32; Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 30, at ¶ 69.

111. *See* Human Rights Comm., General Comment No. 34, *supra* note 33, at ¶ 43; *see also* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 32, at ¶ 38.

112. *Zakharov*, *supra* note 86, at ¶ 248. See also *Liberty v. United Kingdom*, 2008-IV Eur. Ct. H.R. 1, where the Court held that the U.K. violated its European Convention obligations against arbitrary interference in an individual's "private and family life, his home and his correspondence" as governing legislation conferred almost unfettered power to capture and read emails originating from outside the

provision of such unfettered power to the discretion of the executive would be contrary to the rule of law, and requiring the provision of a number of safeguards.[113]

To conduct communications surveillance, including in cyberspace, States must "clearly demonstrate" that the surveillance is designed to achieve a legitimate aim or objective and is the "least intrusive means" that can be used to obtain information that is necessary to achieve that aim or objective.[114] The sensitivity of the information accessed must be balanced with the severity of the infringement on human rights. As mass surveillance, including mass cyber surveillance, by its nature involves indiscriminate collection and retention without targeting or reasonable suspicion,[115] the State's burden to justify the restriction is heightened.[116] Moreover, surveillance measures that may be neces-

---

UK in order to protect national security or economic interest, and *Szabo v. Hungary*, App. No. 37138/14, Eur. Ct. H.R. (Jan. 12, 2016), http://hudoc.echr.coe.int/eng?i=001-160020, in which the European Court of Human Rights upheld petitioners' challenge of sweeping legislation authorizing police to search houses, postal mail, and electronic communications and devices without judicial approval when seeking to prevent terrorism or otherwise protect national security.

113. *Zakharov*, *supra* note 86, at ¶ 247.

114. *See* Conference Report, Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance, 11 (May 2015), https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6i yi2u.pdf.

115. *See* Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 21 ("In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated."). In *S. v. United Kingdom*, 2008-V Eur. Ct. H.R. 167, 200, the U.K. government admitted that retention of DNA data was "neither warranted by any degree of suspicion of the applicants involvement in a crime or propensity to crime nor directed at retaining records in respect of investigated alleged offences in the past." The Court noted that the material was "retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected." *Id.* at 207.

116. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, *supra* note 3, at 35; *S.*, 2008-V Eur. Ct. H.R. at 201-202, 206 ("[It is] essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness . . . The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests."); Case C-293/12, *Digital Rights Ireland*, *supra* note 43 (holding that although retention of communications data was for a legitimate aim of combatting "serious crime" the nature of the directive, "requir[ing] retention of all traffic data [including] Internet access, Internet e-mail, and Internet telephony" was a blanket obligation, and entailed "an interference with the fundamental rights of practically the entire European population," including "persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."). The Right to Privacy in the Digital Age, *supra* note 26, at ¶ 26 ("Mass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate."). Rep. of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra* note 39, at 59 ("[b]ulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by [ICCPR] article 17.").

sary and proportionate for one legitimate aim may not be so for the purposes of another.[117]

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (David Kaye) has argued that blanket actions by the State that undermine the ability of individuals to engage in the Internet in a private or anonymous manner are also unlikely to be proportionate, as they undermine the ability of individuals to enjoy a number of their rights, including the right to privacy, and, through this right, the enjoyment of other rights.[118] This includes actions by States that establish any absolute prohibitions of anonymity or encryption software, State regulation of software that results in weakness that undermines its effectiveness, and requirements that individuals provide the government with access to their encrypted communications through backdoor mechanisms or key escrows.[119]

CONCLUSION

A. Persistent Questions

While it is now settled that international law, and specifically, international human rights law, applies to cyberspace, the contours of its application remain unsettled. Some issues are specific to cyber, while others are not. For example, well before cyberspace was a word, debates were underway about the scope of application of human rights law. Does it apply to the conduct of a State beyond its borders? Does it apply in situations of armed conflict given the primacy of international humanitarian law in such situations? Does it apply to non-State actors, such as businesses and armed groups? To varying degrees, but increasingly, the answer to all three of these questions is "yes." The weight of international jurisprudence and legal scholarship recognizes that States carry their human rights obligations with them where they exercise effective control in their extraterritorial operations, and that human rights law applies at all times, although some of its provisions may be pre-empted by the *lex specialis* of humanitarian law in situations of armed conflict. The direct application of human rights law to non-State actors remains doubtful, but there is no doubt that States have an obligation not only to respect, but to ensure respect for, human rights by regulating the conduct of non-State actors. As such, States are required to implement legal measures that prevent third parties from engaging in conduct that would be a human rights violation if committed by the State.

117. "[. . .] sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another." The Right to Privacy in the Digital Age, *supra* note 26, at ¶ 109.

118. Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 3, at ¶ 40.

119. *Id.* at 42, 44.

These measures should provide for accountability for perpetrators, and enforceable remedies for victims.

How these obligations will play out in matters of cyber remains speculative. As concerns extraterritoriality, it is not always clear what is domestic and what is extraterritorial in the cyber realm. Where a State's cyber operations are extraterritorial, it is not always clear that the State is exercising a degree of control that would trigger human rights law obligations.

What does it mean for human rights law to apply to cyber operations in armed conflict? While international humanitarian law will govern matters that it addresses, such as rules for targeting and for treatment and trial of detainees, it does not address all matters related to armed conflict. For example, IHL presumes that persons will be detained in non-international armed conflict (wars between a State and a non-State armed group, or between two or more non-State armed groups), but unlike the case of international armed conflict (wars between States) it does not address grounds and procedures for detention. That topic, therefore, remains the province of domestic law as tempered by the State's human rights law obligations. To the extent cyber means are used in connection with non-international armed conflict detention practices, for example, in the procurement and presentation of evidence, they will be governed by human rights law. IHL may also fail to address other matters related to the armed conflict that are addressed by human rights law, such as surveillance, censorship, the situation of refugees, the phenomenon of enforced disappearance, crimes against humanity and genocide (which would also likely be war crimes, but with different elements). To the extent cyber means are used in connection with these matters, and regardless of whether the armed conflict is international or non-international, human rights law may apply. And of course, even when a State is party to armed conflict, human rights law will continue to apply to matters unrelated to the conflict. For example, the fact that a State is "at war" will not therefore excuse it from compliance with human rights prohibitions against discrimination. Therefore, the fact of "war" will not *ipso facto* permit a State to take measures against a group, for example, surveillance, censorship or denial of Internet access, on the basis of race, religion, ethnicity, nationality or sex.

B. And Newer Ones . . .

How will human rights law impact the behavior of non-State actors in cyberspace, be they hackers, scam artists, child pornographers, consumers, journalists, businesses (including Internet providers), religious institutions and those who criticize them, human rights defenders and other civil society organizations, politicians and political activists, fomenters of hatred and discrimination, or merely people posting or seeking information on the best recipe for chocolate chip cookies? It may be tempting to say that State obligations to respect and ensure respect for human rights in connection with these and other activities and entities in cyberspace will work the same as they would in

pre-cyber contexts. To some extent this may be true. But to some extent, the reach, the speed of operation and the extraordinary power of the individual to focus with precision in cyberspace may alter how States, tribunals, academics, private industry and civil society negotiate the balance between security and liberty that is a well-established process in the application of human rights.

The Internet is also fast becoming indispensable to various human activities in both the public and private sphere. One may be getting a passport, filling a prescription, shopping for groceries (especially if one has a physical disability) or reading and contributing to a journalistic outlet that exists only online. As other platforms for these activities recede in use, the claim of a "right to the Internet" becomes more compelling. As the Internet becomes increasingly essential to the achievement and enjoyment of human rights, what does it mean to keep the Internet "free"? What can and will States do to promote access? Likewise, the lack of alternatives to the Internet may strengthen claims of consumers who object to conditions for use of the Internet that require them to waive various rights, such as those related to privacy and redress.

The future of human rights in cyberspace will also, to a great extent, develop in accordance with which of two competing ethics in international relations prevail. Will States be led more by a drive to seek and maintain competitive advantage, even if it means embracing conduct they criticize when others engage in it (such as surveillance, censorship, hacking, cyberattacks and restriction of Internet access)? Or will they be able to arrive at a "Golden Rule" approach that favors a level playing field? No doubt, it will be some combination of the two, but the rapidly changing nature of the technology makes it impossible to predict with any precision. Edward Snowden has opined that powerful countries like the United States should be more interested in developing defensive measures to ensure a secure Internet than offensive ones, since they have so much more to lose from attacks than to gain by attacking. Thus, the U.S. Administration was right to recently conclude that measures to defeat encryption, as sought by the FBI Director, are ultimately counterproductive because if the government can defeat encryption to fight crime and protect national security, then so can criminals and terrorists for their purposes. This is just one, welcome, but microcosmic example of a long-term vision of human security and human rights prevailing over a short-term attempt to gain a security advantage that could backfire, as well as impede the exercise of human rights. Of course, examples to the contrary also abound.

This is the ultimate question about the exercise of human rights in cyberspace: can and will regulation be able to keep pace with changes in technology in a way that prevents the use of cyberspace as a platform for criminality, all the while without unwarranted interference with human rights? The answer will affect not only cyber operations, but given the increasing prominence of the Internet in daily life, will no doubt affect the enjoyment of all human rights elsewhere.