University of California, Irvine
School of Law

Selected References: Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression

by UCI Law International Justice Clinic

I. Introduction

This unofficial document is meant to accompany the June 2015 report to the Human Rights Council of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression. The report explores how encryption and anonymity facilitate the exercise of the rights to privacy and freedom of opinion and expression and proposes a legal framework to govern the individual use and government restriction of encryption and anonymity technologies. The report itself provides citations to numerous sources for the report's conclusions. However, because of space requirements attached to a report to the Human Rights Council, we prepared this companion reference document to highlight a limited set of additional technical and legal resources that interested readers may wish to investigate. All of these documents informed, in one way or another, the report itself.

The submissions of States, civil society organizations and individuals, found at the official website of the Office of the High Commissioner for Human Rights, played an important role in the preparation of this report, and they deserve study by all interested persons.

This document was prepared by Emile Ayoub, David Bosner and Citlalli Ochoa, students in the UC Irvine School of Law International Justice Clinic who made significant contributions to the research of the report.

II. Additional References

INTRODUCTION

1. United Nations human rights mechanisms, including the previous Special Rapporteur, have discussed extensively not only the value of the Internet to freedom of expression but also the capacity that contemporary digital technologies offer Governments, corporation, and criminals, among others, to interfere with the rights to freedom of opinion and expression. In particular, reference should be made to Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 30 June 2014 (**A/HRC/27/37)**; UN General Assembly Resolution 68/167, 18 December 2013 (available at **A/RES/68/167)**; Report of the Special Rapporteur, 10 August 2011 (**A/66/290)**; and Report of the Special Rapporteur, 17 April 2013 (**A/HRC/23/40)**.

2. For more information on encryption and anonymity facilitating harassment and criminal activity, see UN Counter-Terrorism Implementation Task Force (CTITF), **Countering the Use of the Internet for Terrorist Purposes**, CTITF Working Group Report (February 2009); CTITF, **Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects**, Working Group Compendium (May 2011); Michael Chertoff and Tobby Simon, ***The Impact of the Dark Web on Internet Governance and Cyber Security***, Global Commission on Internet Governance Paper Series: No. 6 (Chatham House, February 2015); Jonathan Mahler, ***Who Spewed That Abuse? Anonymous Yik Yak App Isn't Telling***, N. Y. Times, March 8, 2015.

3. For examples on encryption and anonymity facilitating communication of sensitive topics such as religion and sexual orientation, sexual abuse, illnesses like HIV/AIDS, or drug addiction see the submission of the Association for Progressive Communication at 3, 6, 7.

SECURE AND PRIVATE COMMUNICATION IN THE DIGITAL AGE

Contemporary encryption and anonymity

1. For a detailed explanation of the history of cryptography, see David Kahn, THE CODE BREAKERS (1996); Simon Singh, THE CODE BOOK (1999).

2. Public key encryption is described in Bruce Schneier, PRACTICAL CRYPTOGRAPHY 207.

3. A full discussion of the U.S. crypto wars in the 1990s may be found in the submission of the Open Technology Institute of the New America Foundation at 4–7.

4. For a more detailed explanation of the need for sophisticated means to protect individual, corporate, and government data – such as official identity numbers, financial and health data, and electronic commerce see the submissions of the Open Technology Institute at 12–14, and Article 19 at 18.

5. A description of how encryption may be used to create digital signatures to ensure that a document and its sender are authentic, certification authorities to authenticate and verify the identity of the server, internet security protocols to protect browsers and servers (such as Transport Layer Security), among others is available in the submission Citizen Lab and Collin Anderson at 2–4.

6. For examples on how the use of encryption may protect data stored on laptops, hard drives, servers, tablets, mobile phones, and other devices, see Bruce Schneier, Data and Goliath 325 (2015). See also Alex Hern, ***Apple Defies FBI and Offers Encryption by Default on New Operating System*** (17 October 2014) explaining that Apple's FileVault and Window's BitLocker encrypt a user's entire hard drive and removable drives.

7. More examples of who uses and who benefits from the use of encryption tools may be found in the submissions of, among others, Human Rights Watch at 11–15, Freedom House at 5-6, PEN America/Access at *passim*, and Reporters Committee for Freedom of the Press/Committee to Protect Journalists at *passim*.

8. For a more detailed explanation of "Off-the-Record" technology, see Nikita Borisov et al., ***Off-the-Record Communication, or, Why Not to Use PGP*** (2004).

9. There is an abundance of sources stating that no special access can be made available only to government authorities. For instance, see Bruce Schneier, ***iPhone Encryption and the Return of the Crypto Wars***, October 6, 2014; Cory Doctorow, ***There's No Backdoor That Only Works for Good Guys***, October 9, 2014.

10. For a discussion of how metadata analysis can help identify users, see Ronald Deibert, BLACK CODE 43-45 (2013).

11. The Tor network allows not only encrypted and anonymous communication, but also the hosting of "hidden services" that disguise websites' locations. *See* Tor Project, **Tor: Hidden Service Protocol**.

Uses of the technologies

1. A discussion of groups that are most at risk when their communications are intercepted may be found in the submissions of Freedom House (discussing case studies in Iran, Angola, and Vietnam); the Human Rights Foundation & Wickr Inc. at 8–17; and the Joint Submission of World Wide Web Foundation/Centre for Internet and Human Rights at European University Viadrina/Oficina Antivigilância at the Institute for Technology and Society - ITS Rio/Derechos Digitales at *passim.*

2. A table listing civil society requirements for security and availability in digital communications may be found as an appendix in the submission of the Citizen Lab and Collin Anderson at Appendices p.1–4.

3. For information on the economic threats to the Internet see CSIS/McAfee, *Net Losses: Estimating the Global Cost of Cybercrime* (June 2014).

4. Encryption and anonymity can shield an opinion from outside scrutiny. *See, e.g.,* Helmi Noman, ***Arab Religious Skeptics Online: Anonymity, Autonomy, and Discourse in a Hostile Environment***, Feb. 5, 2015.

5. Encryption and anonymity empower individuals to circumvent barriers and access information that is in the public interest. Expression in the public interest is at the "core of the concept of democratic society." European Court of Human Rights, Lingens v Austria (1986) 8 EHRR 103 para 42. *See also* Human Rights Comm., Rep. of the Human Rights Comm., Aug. 1, 2008-Jul. 31, 2009, P 85(26) U.N. Doc. A/64/40 (Vol. 1) (focusing on traditional methods of political expression, including canvassing and written materials); *id.* P 86(19) (human rights defenders in report on Nicaragua).

6. For more information on how journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves from surveillance and harassment see Human Rights Watch & ACLU, **With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy** (2014); PEN America, **Chilling Effect: NSA Surveillance Drives U.S. Writers to Self-Censor** (2013).

7. For a discussion of how encryption and anonymity facilitate the exploration of gender, religious, ethnic, and sexual identity see submission of Association for Progressive Communication at 3–7.

THE RIGHTS TO FREEDOM OF OPINION AND EXPRESSION AND PRIVACY

For a more detailed discussion on the need for exceptional vigilance when protecting rights to freedom of opinion and expression online, see General Assembly Resolution 68/167, para 3; Human Rights Council Res A/HRC/RES/20/8, para 1.

Privacy as a gateway for freedom of opinion and expression

1. For a discussion on the right to privacy in the digital age and how it relates to freedom of expression see especially Report of the Office of the High Commissioner for Human Rights, ***The Right to Privacy in the Digital Age*** (2014); Submission of Privacy International at *passim*; Submission of Human Rights Foundation & Wickr Inc. at 3–7.

2. When discussing how the rights to privacy and freedom of expression are interlinked, the previous mandate-holder, Mr. Frank LaRue, stated "[i]n order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous." A/HRC/23/40.

3. “Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships.” A/HRC/13/37 at 13; *see also Privacy in a Digital Age* at 5; A/HRC/23/40 at ¶ 24.

Right to hold opinions without interference

1. For a more detailed discussion on how targeted digital interference harasses individuals and civil society organizations for the opinions they hold, see Citizen Lab, **Communities @ Risk: Targeted Digital Threats Against Civil Society**, November 2014.

Right to freedom of expression

1. In addition to the rights to privacy, opinion, and expression, other provisions of human rights law clarify the scope of rights. In particular, a fundamental and pervasive tenet of human rights law obligates States to respect and ensure respect for the rights guaranteed by the law “without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.” *See* Article 2(1), ICCPR; Article 2, UDHR. *See also* Article 2(2), International Covenant on Economic, Social and Cultural Rights; General Comment 31, para.10. In environments where discrimination exists, the ability of users to exercise the right to freedom of expression securely may depend on the use of tools such as encryption and anonymity. *See* Article 2(1), ICCPR; Article 2, UDHR. See also Article 2(2), International Covenant on Economic, Social and Cultural Rights; General Comment 31, para. 10.

2. The use of encryption and anonymity empowers individuals to gain access to the benefits of scientific progress that might be curtailed by Governments. ICESCR, art. 15(1)(b). See Sarah McKune, ***Encryption, Anonymity and the “Right to Science”***, Just Security, April 28, 2015.

3. An example of international mechanisms acknowledging that the protections of freedom of expression apply to activities on the internet is the **Joint Declaration of the Special Rapporteurs on freedom of expression and the internet** (2011).

Roles of corporate actors

1. For discussions of the obligations of corporate actors, see the submissions of Global Network Initiative at 1–2; Freedom House at 7; Center for Democracy & Technology at 8–10.

2. For a discussion on the right to freedom of expression and the role of intermediaries, see Rebecca Mackinnon et al, **Fostering Freedom Online: The Role of Internet Intermediaries** (UNESCO/Internet Society, 2014); the **Manila Principles on Intermediary Liability** (2015); and the submission of the Center for Democracy & Technology at 3–4, 8–10.

EVALUATING RESTRICTIONS ON ENCRYPTION AND ANONYMITY

Legal framework

1. Article 2(3)(b), ICCPR guarantees that individuals enjoy a right to a remedy for a violation of the Covenant that would be "determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State." The Concluding Observations, Poland highlights the same concern. The Concluding observations, found at U.N. Doc. CCPR/C/79/Add.110 (1999), ¶ 22. Principle 1.1)(b) of the **Johannesburg Principles** on National Security, Freedom of Expression and Access to Information (Oct. 1995), state that, "[t]he law should provide for adequate safeguards against abuse, including prompt, full and effective judicial scrutiny of the validity of the restriction by an independent court or tribunal."

2. Proportionality has been widely recognized as an essential element of the necessity standard. For a more detailed discussion of the principle of proportionality, see Case of Escher et al v. Brazil, Judgment of 6 July 2009, **http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf**; see also Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism, Advisory Opinion OC-5/85, Inter-Am. Ct. H.R. (Ser. A) No. 5 (1985) at P46.

3. References to General Comments and Resolutions of the Human Rights Committee discussing proportionality and arbitrary interference may be found in Human Rights Foundation & Wickr Inc. at 1–7.

4. A useful review of anonymity in the context of the ongoing Delfi case before the European Court of Human Rights may be found in Nicolo Zingales, ***Virtues and Perils of Anonymity*** (2014) JIPITEC 155.

STATE PRACTICE: EXAMPLES AND CONCERNS

Encryption

1. For discussions of various state practices that threaten anonymous and encrypted communication worldwide see the Article 19 submission 8–11 (on anonymity), 18–22 (on encryption); the joint submissions of the World Wide Web Foundation et al at 5–25; Citizen Lab and Collin Anderson at 6–9; Human Rights Foundation & Wickr Inc. at 8–16; the Freedom House submission at 4–7; Human Rights Watch submission at 13–15; Electronic Frontier Foundation at 40–46; and the submission of the Association for Progressive Communication at 9–10. Further focus on state practice in Colombia may be found in the submission of Fundacion Karisma at *passim*; and on state practice in Australia in the submission of Australian Privacy Foundation at *passim.*

2. For a more detailed discussion about backdoors and how they undermine the security of all online users see PACE, Committee on Legal Affairs and Human Rights, **Report on Mass Surveillance** (2015); Bruce Schneier, Data and Goliath 147–48.

3. For a discussion of key escrows and their vulnerabilities see Abelson et al., **The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption** (1997).

Anonymity

1. For examples of States that have attempted to ban or intercept anonymous communications in time of protests and of activists using encryption and anonymity for protests see the submission of the Human Rights Foundation & Wickr Inc. at 8–16; the submission of the World Wide Web Foundation et al at 8, 11.
2. A discussion of policies that undermine the use of anonymity tools in Brazil, South Korea, Vietnam, Russia, Europe, and the United States, in a addition to a discussion of harmful effects of mass copyright litigation and mass surveillance may be found in the submission of the Electronic Frontier Foundation at 28–35.
3. For examples of State practices in the United States, Canada, South Korea, and Mexico that are positive policies for the protection of anonymity see the submission of the Electronic Frontier Foundation at 23–28.
4. For a discussion of anonymity in a video-mediated world see the submission of WITNESS Cameras Everywhere (addressing issues such as facial recognition and anonymity, video censorship and freedom of expression).
5. For additional information regarding China's announced regulations requiring internet users to register real names for certain websites to avoid spreading content that challenges national interests see Josh Chin, ***China is Requiring People to Register Real Names for Some Internet Services***, *Wall Street Journal*, February 4, 2015.
6. As of February 2014, data compiled from various sources, including research conducted by MobileActive (an advocacy group), Steve Song of Village Telco, Jentzsch's (2012) work on the economic implications of mandatory SIM registration, and the authors' own data collection efforts indicated that only Cape Verde, Lesotho, Mauritania, Namibia, Somalia and Swaziland had not introduced a policy for SIM registration. Kevin P. Donovan & Aaron K. Martin, ***The Rise of African SIM Registration***, Feb. 3, 2014.