Call for Submissions on the Protection of Sources and Whistleblowers by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye

Written Submission of the Center for Constitutional Rights[1]

666 Broadway
7th Floor
New York, NY 10012
(212) 614-6464

June 22, 2015

Table of Contents

1 CCR is dedicated to advancing and protecting the rights guaranteed by the United States Constitution and the Universal Declaration of Human Rights. Founded in 1966 by attorneys who represented civil rights movements in the South, CCR is a non-profit legal and educational organization committed to the creative use of law as a positive force for social change.

INTRODUCTION

1. The Center for Constitutional Rights (CCR)[2] submits this report to help guide the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, in the upcoming report addressing the international standards on whistleblowers.

2. CCR represents the publishing organization WikiLeaks and its editor-in-chief Julian Assange, which have been subject to an unprecedented US investigation and attempts at prosecution following WikiLeaks' publication of classified materials in 2010.

3. In 2012, CCR brought a suit challenging the lack of transparency around the court-martial of alleged WikiLeaks source Pfc. Chelsea Manning on behalf of itself and a diverse group of media figures: Glenn Greenwald, Amy Goodman of *Democracy Now!*, *The Nation* and its national security correspondent Jeremy Scahill, and Wikileaks and Mr. Assange. Also included were Kevin Gosztola, co-author of *Truth and Consequences: The U.S. vs. Bradley Manning* and a civil liberties blogger covering the Manning court martial, and Chase Madar, author of *The Passion of Bradley Manning* and a contributing editor to *The American Conservative*. Jonathan Hafetz of Seton Hall Law School was co-counsel with CCR in that case, along with Bill Murphy and John J. Connolly of Zuckerman Spaeder LLP's Baltimore office.

4. The right of access to information is a fundamental right applying to all state institutions and officials, and grounded in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and universally in regional instruments and special procedures.[3] The right arises from the fact that the state holds public information necessary for a properly informed citizenry. That information belongs to the public; it is produced, collected and processed using public resources.

5. There is a rich body of existing analysis surrounding access to information, freedom of expression, and whistleblowing.[4] The purpose of this Submission, using the experiences of CCR's clients, is to emphasize two important principles:

---

2 Prepared by Carey Shenkman, Attorney working for Michael Ratner, President Emeritus of CCR. I have been involved for several years with CCR's work in the defense and advocacy on behalf of whistleblowers. I worked on CCR's appellate litigation in Chelsea Manning's court-martial. Presently, I work with Michael Ratner representing whistleblowers and publishers, including WikiLeaks and Julian Assange. I frequently write and lecture on legal issues surrounding whistleblowers. I would like to sincerely thank Michael Ratner, Baher Azmy, Melinda Taylor, and Christophe Marchand for their valuable feedback during the preparation of this Submission.

3 *See, e.g.*, International Covenant on Civil and Political Rights (ICCPR), 999 U.N.T.S. 171 (Dec. 16, 1966), Art. 19; UN Human Rights Committee, General Comment No. 34 on Article 19, UN Doc. CCPR/C/GC/34 (Sept. 12, 2011); *see also Grigoriades v. Greece*, no. 24348/94, ECHR 1997; *Palamara-Iribarne v. Chile*, Inter-American Commission on Human Rights (IACHR), Case 11.571, Report No. 77/01, OEA/Ser./L/V/II.114 Doc. 5 rev. at 128 (2001).

4 For instance, former CCR attorney Emi MacLean submitted a brief to the Inter-American Commission on Human Rights, robustly articulating many international and regional standards surrounding whistleblowers. *See* Emi MacLean, *Written Submission to Thematic Hearing on Freedom of Expression and Communications Surveillance by the United States*, OPEN SOCIETY JUSTICE INITIATIVE (Oct. 28, 2013), *available at* http://www.opensocietyfoundations.org/sites/default/files/IACHR%20hearing%20on%20US%20surveillance%20-%2010%2028%202013.pdf.

6. **First, States have an obligation to protect whistleblowers, a vulnerable group that faces systematic stigmatization as a result of exercising fundamental rights to access and obtain information.** International and regional legal standards, case law, and State practice (through national laws and asylum practice) widely support that whistleblowers are a vulnerable group triggering State obligations to protect them. This protection is not limited to whistleblowers, but also applies to individuals generally exposing abuses in the public interest. These can include members of civil society on fact-finding missions, UN monitors, publishers, and their sources.

7. Human rights fact-finding source protection and whistleblowing are related; in essence, both protect individuals accessing and obtaining information from retaliation. That retaliation may take several forms, whether it be compelled disclosure, legal sanctions, or extralegal harassment. There exists a paramount public interest in the work of these individuals that cannot be effectively achieved without special protection.

8. **Second, States have a positive obligation to promote freedom of expression through cyber laws, and must not use technical violations to punish whistleblowers.** There is a serious risk that cyber laws will displace secrecy laws as a tool to prosecute whistleblowers on basis of their activities accessing and obtaining information. In the United States, the cases of Chelsea Manning, NSA whistleblower Thomas Drake, and WikiLeaks reveal the application of "unauthorized access" computer laws to punish whistleblowers and publishers.

9. Indeed, today significant amounts of access to information, particularly by whistleblowers, is enabled by computers. Whistleblowers must not be punished for using a computer to blow the whistle. Cyber laws sanctioning whistleblowers or sources who already have access to computers, purely based on their intent to blow the whistle, raise serious problems for freedom of expression.

10. Restrictions on freedom of expression must be 'established in law' and necessary to achieve an important purpose. In addition to risking misuse for illegitimate purposes (as an alternative to state secret laws punishing access to information), cyber laws punishing "unauthorized access" may not actually define what is or is not 'authorized.' The term may be defined after the fact by terms-of-use agreements or employer discretion. This raises serious concerns under principles of legal certainty; indeed, many States and representatives of civil society already recognize that such access laws can be, and are used to prosecute individuals who already have clearance for systems, purely based on their intent to disseminate information to the public.

11. Emerging regional instruments already problematically call for States to use cyber laws to prosecute the disclosure of official secrets[5] or declare as a threat using "information infrastructure to disseminate information harmful to the . . . spiritual, moral and cultural

5 League of Arab States, Arab Convention on Combating Information Technology Offenses, Art. 6 (Dec. 21, 2010), *available at* https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd [Arab League Cyber Crime Convention] (punishment for illicit access to a computer "shall be increased" if it leads to "the acquirement of secret government information").

environment of other States [through] mass media [or] on the Internet."[6] States must ensure that measures prosecuting cyber crime properly take into account their obligations to respect and promote freedom of expression.

I. States must protect as a category of vulnerable persons individuals who, in the public interest, access and collect information exposing abuses.

A. Whistleblowers are a vulnerable group under international law

> . . . Hence,
> Horrible villain! or I'll spurn thine eyes
> Like balls before me; I'll unhair thy head:
> Thou shalt be whipp'd with wire and stew'd in brine...
> . . . let ill tidings tell
> Themselves when they be felt.[7]

1. International standards support the vulnerability of whistleblowers

12. The concept of "vulnerable persons" is an emerging concept in international law that is rapidly gaining traction in the decisions of the European Court of Human Rights (ECtHR).[8] In *Chapman v. United Kingdom*, the ECtHR presented the notion of a protected category of persons in regard to the Roma people:

> [T]he vulnerable position of Gypsies as a minority means that some special consideration should be given to their needs and their different lifestyle both in the relevant regulatory planning framework and in reaching decisions in particular cases.[9]

13. The standard articulated by the Court in *MSS v. Belgium and Greece* in recognizing asylum seekers as a vulnerable category is "the existence of a broad consensus at the international and European level concerning this need for special protection, as evidenced by the Geneva Convention, the remit and the activities of the UNHCR and the standards set out in the Reception Directive."[10]

---

6 Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Annex 2, para. 5 (June 16, 2009), *available at* http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf [Shanghai Cooperation Organization Cyber Crime Treaty]. Signed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan in 2008, the agreement lists as a major international information security threat the "[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environments of other States."

7 William Shakespeare, *Anthony and Cleopatra* Act II: Sc. 5 (Cleopatra responding to her messenger telling her Antony married Octavia).

8 Alexandra Timmer, *A Quiet Revolution: Vulnerability in the European Court of Human Rights*, *in* VULNERABILITY: REFLECTIONS ON A NEW ETHICAL FOUNDATION FOR LAW AND POLITICS 147-170 (Martha Fineman & Anna Grear eds. 2013) ("[T]he European Court of Human Rights is increasingly relying on vulnerability reasoning.").

9 *Chapman v. United Kingdom* (GC), no. 27238/95, ECHR 2001, para. 96.

10 *M.S.S. v. Belgium and Greece*, no. 30696/09, ECHR 2011, para. 251.

14. The concept of vulnerable groups is non-exhaustive, and the ECtHR has continued to recognize vulnerable groups of HIV-afflicted individuals,[11] the mentally disabled,[12] and asylum-seekers.[13] In each of these cases, a retaliation against each of these groups was considered disproportionate. The Court in *Kiss* also suggested that vulnerable groups include those discriminated against on basis of gender, race, or sexual orientation,[14] and acknowledged one factor in the determination being "broad consensus at the international and European level concerning the need for special protection." The European Committee of Social Rights now applies the concept of vulnerable groups in its own decisions, recognizing categories closely tracking those of the ECtHR.[15] Outside of the European system, the same premise behind vulnerable groups underlies the major instruments protecting women,[16] children,[17] and the disabled.[18] While the Universal Declaration of Human Rights makes clear that human rights are to be enjoyed by all, human rights law also contemplates that some groups may require special attention in order to enjoy their rights.[19]

15. The concept of "vulnerable persons" bears resemblance to protected categories under the crime of persecution in international criminal jurisprudence,[20] which include for example ethnic and religious categories such as Bosnian Muslims of Srebrenica or Eastern Bosnia.[21] The

11 *Kiyutin v. Russia*, no. 2700/10, ECHR 2011, para. 64.
12 *Kiss v. Hungary,* no. 38832/06, ECHR 2010, para. 42.
13 *M.S.S. v. Belgium and Greece*, no. 30696/09, ECHR 2011, para. 251.
14 *Kiss v. Hungary,* no. 38832/06, ECHR 2010, para. 42 (citing *Abdulaziz, Cabales and Balkandali v. the United Kingdom*, nos. 9214/80, 9473/81, 9474/81, ECHR 1985, para. 78 (gender); *D.H. and Others v. the Czech Republic* [GC], no. 57325/00, ECHR 2007, para. 182 (race); *E.B. v. France*[GC], no. 43546/02, ECHR 2008, para. 94 (sexual orientation)).
15 *See, e.g.*, *Centre on Housing Rights and Evictions (COHRE) v. Italy*, Complaint No. 58/2009, Merits (June 25, 2010), para. 76 (concerning Roma and Sinti); *Centre on Housing Rights and Evictions (COHRE) v. Croatia*, Complaint No. 52/2008, Merits (June 22, 2010), para. 88 (displaced families of Serb ethnicity); I*nternational Association Autism Europe v. France*, Complaint No. 13/2002, Merits (Nov. 4, 2003), para. 53 (concerning persons with autism).
16 UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)*, 1249 U.N.T.S. 13 (Dec. 18, 1979).
17 UN General Assembly, *Convention on the Rights of the Child*, 1577 U.N.T.S. 3 (Nov. 20, 1989).
18 UN General Assembly, *Convention on the Rights of Persons with Disabilities*, U.N. Doc. A/RES/61/106, Annex I (Dec. 13, 2006).
19 Elisabeth Reichart, UNDERSTANDING HUMAN RIGHTS, CHAPTER 5: VULNERABLE GROUPS 77 (2006) ("[D]espite the importance of viewing human rights within a universal context and not simply as something for the disadvantaged, instances arise when particular groups often require more attention to ensure human rights of those groups.").
20 *See* Rome Statute of the International Criminal Court, U.N. Doc. A/CONF. 183/9, 2187 U.N.T.S. 90 (July 17, 1998), Art. 7(g) (defining persecution as "the intentional and severe deprivation of fundamental rights contrary to international law by reason of the identity of the group or collectivity"); *see also id.* Art. 7(h) (granting the ICC prosecutorial power over crimes against humanity involving "[p]ersecution against any identifiable group" on "grounds that are universally recognized as impermissible under international law"); Updated Statute of the International Criminal Tribunal for the Former Yugoslavia, Adopted 25 May 1993 by Resolution 827, As Amended 7 July 2009 by Resolution 1877 (Sept. 2009), Art. 5(h) (granting the ICTY prosecutorial power over crimes against humanity involving "persecutions on political, racial and religious grounds); Statute of the International Criminal Tribunal for Rwanda (ICTR), U.N. Doc. S/Res/955 (1994), Art. 3(h) (same).
21 *Prosecutor v. Krstic*, ICTY, Judgement, No. IT-98-33-T (Aug. 2, 2001), para. 554 ("The Chamber concludes that the protected group, within the meaning of Article 4 of the Statute, must be defined, in the present case, as the Bosnian Muslims. The Bosnian Muslims of Srebrenica or the Bosnian Muslims of Eastern Bosnia constitute a part of the protected group under Article 4."). In addition to genocide Krstic was also charged and convicted for persecution on basis of actions against this group.

International Criminal Tribunal for the Former Yugoslavia (ICTY) appeals chamber has explicitly held that the crime of persecution can include "the denial of employment, and the denial of the right to judicial process" and rejected the argument that these forms of treatment do not amount to serious violations of international law.[22]

16. In studying vulnerable groups, Peroni and Timmer observe that while the ECtHR has yet to apply a clear test in establishing such a group, the overarching factors include a vulnerability that is "partly constructed by broader societal, political, and institutional circumstances," with common traits including stigmatization and social exclusion.[23] In *Kiyutin v. Russia* recognizing the HIV-afflicted as a protected class, the ECtHR held that "people living with HIV are a vulnerable group with a history of prejudice and stigmatization."[24] In *M.S.S. v. Belgium and Greece*, extending the protection to asylum seekers, the Court found it necessary to consider vulnerability caused by the difficult circumstances faced by the applicants, particularly with regard to their past traumatic persecution and detention.[25] The key element for finding a vulnerable group is a pattern of persecution of a group, and the ECtHR looks to treaty bodies, UN reports, and civil society fact-finding in making such determinations.[26]

17. The benefits of recognizing a group as "protected" means that States are not only afforded less deference in restricting the rights of persons belonging to the group, but also have a positive obligation to protect them. In terms of the jurisprudence of the ECtHR, the benefit to belonging to a vulnerable category is a "substantially narrower" margin of appreciation afforded to States, which must have "very weighty reasons for the restrictions in question."[27] In terms of international analyzing restrictions under legal instruments such as the International Covenant on Civil and Political Rights (ICCPR), this would mean that "legitimate aims" articulated by States in restricting rights must be subject to more robust scrutiny.

18. **Whistleblowers are a vulnerable group because they face systematic stigmatization as a result of their exercise of their right to access and obtain information.** "[I]t has been shown time and again," according to the Committee of Ministers of the Council of Europe, "that whistleblowers often face indifference, hostility, or worse, retaliation" in forms that are varied

22 *Prosecutor v. Mićo Stanišić*, ICTY, Judgement, No. IT-08-91-T (Mar. 27, 2013), para. 92; *Prosecutor v. Radoslav Brđanin*, ICTY, Appeal Judgement, No. IT-99-36-A (Apr. 3, 2007), paras. 295, 297 (calling "misplaced" the argument that "denial of the rights to employment, freedom of movement, proper judicial process, and proper medical care all fall outside the jurisdiction of the Tribunal" as persecution).

23 Lourdes Peroni & Alexandra Timmer, *Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law*, 11 INT'L J. CONST. L. 1056, 1063, 1070 (2013) .

24 *Kiyutin v. Russia*, no. 2700/10, ECHR 2011, para. 64.

25 *M.S.S. v. Belgium and Greece*, no. 30696/09, ECHR 2011, para. 232 ("In the present case the Court must take into account that the applicant, being an asylum seeker, was particularly vulnerable because of everything he had been through during his migration and the traumatic experiences he was likely to have endured previously.").

26 *See El Haski v. Belgium*, no. 649/08, ECHR 2012, para. 98 (citing the Human Rights Committee, Committee Against Torture, Human Rights Watch, and FIDH, in recognizing the particular vulnerability faced by Moroccans suspected of terrorism).

27 *Kiss v. Hungary*, no. 38832/06, ECHR 2010, para. 42.

and numerous.[28] Significant scholarship from anthropologists,[29] psychologists,[30] and civil society experts[31] support recurring factors faced by whistleblowers as a class of individuals, including phases of isolation and retaliation. Indeed, punishing a person bearing bad news, or "shooting the messenger" is as old as civilization and is referenced in Plutarch's *Lives*[32] and Shakespeare; in sixteenth-century England it was even considered treasonous to harm town criers—the local newsmen.[33]

19. The Parliamentary Assembly of the Council of Europe's (PACE) report on whistleblowing identifies some of the roots of this victimization in "deeply engrained cultural attitudes,"[34] and the UN Secretariat itself acknowledges the risk of retaliation faced by whistleblowers in order to provide internal UN protections.[35] Indeed, the UN Dispute Tribunal, in a decision commended by the French government, found that the dismissal of an official for disclosing an internal UN report on the alleged sexual abuse of children by French troops in Central African Republic to French prosecutors was "prima facie unlawful."[36]

---

28 Committee of Ministers of the Council of Europe, Protection of Whistleblowers, Recommendation CM/Rec(2014)7 adopted by the Committee of Ministers of the Council of Europe on 30 April 2014 and explanatory memorandum [Committee of Ministers Recommendation], para. 4.

29 Gabriela Coleman, Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous (2014) (documenting the fragmentation and persecution of journalists, activists, and whistleblowers associated with the Anonymous movement); Dr. Wim Vandekerckhove, Whistleblowing and Organizational Social Responsibility: A Global Assessment (2012) (studying organizational whistleblowing policies).

30 C. Fred Alford, WHISTLEBLOWERS: BROKEN LIVES AND ORGANIZATIONAL POWER 126 (2001) ("To be a whistleblower is to be without colleagues and friends."); Jean Lennane, *What Happens to Whistleblowers, and Why*, 6 SOC. MED. 4 (2012) (documenting the "predictable set of responses to whistleblowers" and analyzing psychological responses such as groupthink); Joan E. Sieber, *The Psychology of Whistleblowing*, 4 SCI. & ENG. ETHICS 7-23 (1998); *see also* Sherrie Gossett, *NSA Accused of Psychologically Abusing Whistleblowers*, CYBERCAST NEWS SERVICE (Jan. 25, 2006), *available at* http://www.bmartin.cc/dissent/documents/Gossett06.html (documenting testimony by former NSA whistleblowers alleging psychological abuse); SIGMUND FREUD, ON METAPSYCHOLOGY (PFL 11), p. 454-55 (calling 'shooting the messenger' a "marginal case of this kind of defense . . . of fending off what is distressing or unbearable").

31 Shelley Walden, *Is the Experience of 'The Whistleblower' Typical? Yes*., GOVERNMENT ACCOUNTABILITY PROJECT (Sept. 13, 2011), *available at* http://whistleblower.org/blog/120013-experience-%E2%80%9C-whistleblower%E2%80%9D-typical-yes.

32 PLUTARCH'S LIFE OF LUCULLUS (Dryden transl.), para. 25 ("The first messenger, that gave notice of Lucullus' coming was so far from pleasing Tigranes that, he had his head cut off for his pains; and no man dared to bring further information. Without any intelligence at all, Tigranes sat while war was already blazing around him, giving ear only to those who flattered him.")

33 *Top Town Crier to Be Crowned as Hebden Bridge Hits 500*, BBC UK (Aug. 20, 2010), *available at* http://news.bbc.co.uk/local/bradford/hi/people_and_places/arts_and_culture/newsid_8931000/8931369.stm ("Town criers were protected by law and "don't shoot the messenger" was a very real command. Anything that was done to a town crier was deemed to be done to the King and was seen as treason.").

34 Report of the Committee on Legal Affairs and Human Rights, Protection of Whistle-Blowers, Doc. 12006 (Sept. 14, 2009), para. 1 (noting that in some countries there are "deeply engrained cultural attitudes which date back to social and political circumstances, such as dictatorship and/or foreign domination, under which distrust towards 'informers' of the despised authorities was only normal").

35 Bulletin on protection against retaliation for reporting misconduct and for cooperating with duly authorized audits or investigations, U.N. Doc. ST/SGB/2005/21 (Dec. 19, 2005) ("Retaliation against individuals who have reported misconduct or who have cooperated with audits or investigations violates the fundamental obligation of all staff members to uphold the highest standards of efficiency, competence and integrity and to discharge their functions and regulate their conduct with the best interests of the Organization in view.").

36 Sandra Laville, *UN Suspension of Sexual Abuse Report Whistleblower Is Unlawful, Tribunal Rules*, THE GUARDIAN

20. Regional instruments and special procedures recognize a positive obligation by States to protect whistleblowers as a category of individuals. The OAS[37] and African Union[38] both actively undertake to protect whistleblowers exposing corruption from reprisal, while PACE in its Resolution 1729 (2010) calls on States to pass legislation protecting whistleblowers from "any form of retaliation (unfair dismissal, harassment or any other punitive or discriminatory treatment)."[39] The ECtHR held in the *Guja* case that disclosure of "illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection."[40] The OAS similarly stipulates in its Model Law that whistleblowers are entitled to protective measures, defining a "protected person" as one granted such measures "in order to guarantee the exercise of his/her personal and labor rights and the administrative or judicial proceeding of the acts of corruption."[41]

21. The European Parliament in response to the revelations of Edward Snowden stressed the "need to provide [whistleblowers] with the necessary protection, including at [the] international level";[42] the Committee of Ministers similarly recognizes a positive obligation on States to ensure "retaliation or victimisation of whistleblowers will not be tolerated in a democratic society."[43] Finally, former UN Special Rapporteur on freedom of opinion and expression rapporteur Frank LaRue, expressed serious concern about surveillance laws being used to

(May 6, 2015), *available at* http://www.theguardian.com/world/2015/may/06/un-suspension-of-sexual-abuse-report-whistleblower-is-unlawful-tribunal-rules?CMP=share_btn_fb.

37 Organization of American States, Text of the Draft Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistleblowers and Witnesses, OEA/Ser.L,SG/MESICIC/doc.345/12 rev. 2 (Mar. 22, 2013) [OAS Model Law], Art. 16 ("The authorities are obliged to protect the rights of those public employees and private citizens who report acts of corruption and, if necessary, to grant the additional protective measures indicated in this law."); Art. 17 (guaranteeing all whistleblowers legal assistance, and "permanent" protection from removal for public officials).

38 African Union Convention on Preventing and Combating Corruption, Adopted by the 2nd Ordinary Session of the Assembly of the Union (July 11, 2003), Arts. 5.5-.6 ("State Parties undertake to . . . Adopt legislative and other measures to protect informants and witnesses in corruption and related offences, including protection of their identities [and] Adopt measures that ensure citizens report instances of corruption without fear of consequent reprisals.").

39 Assembly Debate on 29 April 2010 (17th Sitting) (see Doc. 12006, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Omtzigt). Text adopted by the Assembly on 29 April 2010 (17th Sitting), Arts. 6.2.3, 6.2.4. The Parliamentary Assembly also defended disclosures to the media made in good faith.

40 *Guja v. Moldova* (GC), no. 14277/04, ECHR 2008, para 72. The applicant was head of the press office in the Moldovan Prosecutor General's Office, and came across a letter from a senior politician seeking to pressure the prosecutor to terminate prosecutions against particular police officers. The Grand Chamber unanimously found a violation of Article 10 of the European Convention where a government employee was dismissed after providing information to the press. The Grand Chamber noted that civil servants may as a part of their work become aware of information corresponding to a "strong public interest." The factors evaluated by the ECtHR included: 1) whether there were alternative channels for disclosure; 2) the public interest in disclosure; 3) the authenticity of the disclosed information; 4) the detriment to the employer in disclosure; 5) the source's good faith behind the disclosure; and the 6) severity of the sanction. *Guja*, paras. 73-77; *Bucur v. Romania*, no. 40238/02, ECHR 2013 , paras. 95-119 (applying the test articulated in *Guja* to a "top secret" disclosure of information).

41 OAS Model Law, Art. 25.

42 European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)), para. 13.

43 Committee of Ministers Recommendation, para. 6.

"target whistleblowers or other individuals seeking to expose human rights violations."[44]

22. The retaliations toward whistleblowers, can result in many effects, both direct (violent retaliation, dismissal, harassment, punitive measures, or other discrimination) and indirect (social pressure, chilling of expression). These implicate not only rights of life and liberty, but plainly implicate rights to seek and impart information, as well as economic and social rights such as the right to seek employment. Denial of employment and access to judicial process may theoretically meet the standard of the crime of persecution articulated by the ICTY appeals chamber in *Brđanin*.

23. **CCR witnessed firsthand the vulnerability of whistleblowers during its litigation involving Pfc. Chelsea Manning's court-martial.** Since 2012 CCR maintained an active presence monitoring the court-martial of Manning, whistleblower and alleged WikiLeaks source.

24. CCR represented a coalition of various media members seeking access to the proceedings. CCR observed that the proceedings were conducted in unprecedented secrecy, with members of the media and public regularly denied access to key trial documents, and significant hearings taking place completely behind closed doors. CCR motioned to intervene in the court-martial and was denied. CCR subsequently filed *CCR v. United States*,[45] a petition for extraordinary relief asking the Army Court of Criminal Appeals to grant public and media access to the court-martial. The petition was denied in a one-sentence order,[46] which CCR appealed to the Court of Appeals for the Armed Forces (CAAF). The CAAF held that it lacked jurisdiction over press or public access claims.[47] CCR then brought the case in federal court,[48] which denied CCR's request for relief.[49] As a result of the continued pressure from the litigation the prosecution finally agreed to begin disclosing court records to the public and media.[50]

25. The UN Special Rapporteur on Torture Juan Méndez found that Manning was subject to cruel, inhuman and degrading treatment while detained in pretrial custody.[51] Judge Denise Lind, who presided over Manning's court-martial, granted Manning 112 days sentencing credit as a result. Manning, who writes for *The Guardian* from prison, recently recounted her extreme and dehumanizing isolation:

---

44 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013), para. 84.

45 *CCR v. United States*, Petition for Extraordinary Relief in the Nature of Writs of Mandamus and Prohibition and Supporting Memorandum of Law, Army Misc 20120514 (May 23, 2012).

46 *CCR v. United States*, Order, Army Misc 20120514 (June 21, 2012).

47 *CCR v. United States*, 72 M.J. 126 (C.A.A.F. 2013).

48 *CCR v. Col. Denise Lind*, Complaint, No. 1:13-cv-01504-ELH (D. Md. May 22, 2013).

49 *CCR v. Col. Denise Lind*, Memorandum Opinion, No. 1:13-cv-01504-ELH (D. Md. June 19, 2013).

50 *Government Agrees to Provide Ongoing Access to Court Documents in Bradley Manning Trial*, CCR (June 20, 2013), *available at* http://ccrjustice.org/home/press-center/press-releases/government-agrees-provide-ongoing-access-court-documents-bradley.

51 Report of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez, U.N. Doc. A/HRC/19/61/Add.4 (Feb. 29, 2012) ("The Special Rapporteur concludes that imposing seriously punitive conditions of detention on someone who has not been found guilty of any crime is a violation of his right to physical and psychological integrity as well as of his presumption of innocence.").

> At the very lowest point, I contemplated castrating myself, and even – in what seemed a pointless and tragicomic exercise, given the physical impossibility of having nothing stable to hang from – contemplated suicide with a tattered blanket, which I tried to choke myself with.[52]

26. In the view of CCR, the experiences of Manning are representative of the treatment faced by whistleblowers in the United States. The vulnerability faced by whistleblowers is faced and shared by publishers and individuals associated with them.[53]

27. The key factor in finding a vulnerable group is stigmatization and persecution on account of participation in that group. The categories of the ECtHR are not exhaustive. In the case of Roma and similar protected ethnic categories of individuals, the protection arises because the subcategory of persons has a broader right to protection against persecution on ethnic grounds. Similarly, protection for whistleblowers grows from their systematic reprisal from State actors as result of exercising rights to seek and impart information. Special, positive protections are required for whistleblowers to exercise their fundamental rights under international law.

2. National laws and asylum practices reflect a consensus on the vulnerability of whistleblowers

28. State practice in offering whistleblower protections (even where inadequate), as well as providing "public interest" defenses to secrecy laws,[54] further bolsters the claim that whistleblowers face particular vulnerability in the exercise of their rights of free expression.

29. **Perhaps the most persuasive evidence for accepting the vulnerability of whistleblowers is the fact that they States so often grant whistleblowers political asylum.** Indeed, Canada,[55]

52 Chelsea Manning, *The Years Since I Was Jailed for Releasing the 'War Diaries' Have Been a Roller Coaster*, THE GUARDIAN (May 27, 2015), *available at* http://www.theguardian.com/commentisfree/2015/may/27/anniversary-chelsea-manning-arrest-war-diaries.

53 *See infra* Part I.B.ii.

54 *See, e.g.*, Canadian Security of Information Act (R.S.C., 1985, ch. O-5), Art. 15; Criminal Code (Denmark), Section 152(e) (2010). In Albania, Chile, Colombia, the Czech Republic, Germany, Italy, Mexico, Moldova, the Netherlands, Norway, Paraguay, Romania, Spain, and Sweden, the burden is on the prosecution to show that an unauthorized disclosure resulted in "damage" or "harm" to national security for any penalty to be imposed. At least seven European countries (Albania, France, Germany, the Netherlands, Romania, Serbia and the United Kingdom) provide as a defense or mitigating circumstance the attempted or actual use of internal channels prior to public disclosure. Amanda L. Jacobsen, NATIONAL SECURITY AND THE RIGHT TO INFORMATION IN EUROPE (Apr. 2013), p. 49.

55 David P. Ball, *Mexican Journalist Karla Ramirez Wins Battle Against Deportation*, VANCOUVER OBSERVER (Apr. 9, 2012), *available at* http://www.vancouverobserver.com/politics/2012/04/09/mexican-journalist-karla-ram%C3%83%C2%Adrez-wins-battle-against-deportation-others-face.

Russia,[56] Ecuador,[57] Venezuela,[58] Nicaragua,[59] Norway,[60] Bolivia,[61] and the United States recognize that whistleblowers or those exposing corruption are entitled to asylum protection. Moreover, the PACE Committee on Legal Affairs and Human Rights called on all Council of Europe member and observer states and the European Union to:

> grant asylum as far as possible under national law, to whistleblowers threatened by retaliation in their home countries provided their disclosures qualify for protection under the principles advocated by the Assembly. [62]

30. Asylum for whistleblowers is contemplated in several prominent, ongoing cases. The UN Special Rapporteur on Torture, Manfred Novak, called on Austria to grant asylum to Srebrenica whistleblower Jovan Mirilo.[63] And Star Ugandan distance runner, Moses Kipsiro, who blew the whistle on a sex abuse scandal in Uganda and regularly receives death threats, reportedly received six offers to change his nationality.[64]

31. The United States is possibly the most prolific country in acknowledging whistleblowers—from other States—as a vulnerable category on account of their political opinion. US immigration courts have expressly contemplated and/or granted asylum to whistleblowers from Albania,[65]

56 Russia granted asylum to whistleblower Edward Snowden.

57 *See* Girish Gupta, *A Whistleblower in Ecuador: The Belarusian Dissident Who Found Asylum in Quito*, TIME (June 26, 2013), *available at* http://world.time.com/2013/06/26/a-whistleblower-in-ecuador-the-belarusian-dissident-who-found-asylum-in-quito/ (Belarusian dissident, Alexander Barankov). The Republic of Ecuador granted asylum on both diplomatic and 1951 Refugee Convention grounds to WikiLeaks editor-in-chief Julian Assange owing to the well-founded risk of political persecution he faces in the United States due to his perceived association with whistleblowers. Ecuador also offered asylum to whistleblower Edward Snowden.

58 Venezuela offered asylum to whistleblower Edward Snowden. Jonathan Watts, *Venezeuala, Nicaragua and Bolivia Offer Asylum to Edward Snowden*, THE GUARDIAN (July 6, 2013), *available at* http://www.theguardian.com/world/2013/jul/06/venezuela-nicaragua-offer-asylum-edward-snowden.

59 Nicaragua offered asylum to Edward Snowden.

60 Norway said it would "consider" granting asylum to Israel nuclear whistleblower Mordechai Vanunu. Eileen Fleming, *Free Vanunu to Norway: International Intervention Required*, ARAB DAILY NEWS (June 6, 2015), *available at* http://thearabdailynews.com/2015/06/06/free-vanunu-to-norway-international-intervention-required/.

61 Bolivia offered asylum to Edward Snowden.

62 PACE, Committee on Legal Affairs and Human Rights, Improving the Protection of Whistleblowers, AS/JUR (2015) 06 (2015), para. 9.1.2.

63 *Srebrenica Whistleblower Denied Asylum*, B92.NET (Feb. 3, 2010), *available at* http://www.b92.net/eng/news/crimes.php?yyyy=2010&mm=02&dd=03&nav_id=64957.

64 Onder Erdogan, *Renowned Uganda Runner Pays for Revealing Sex Scandal*, VIDEONEWS.US (May 18, 2015), available at http://news.videonews.us/renowned-uganda-runner-pays-revealing-sex-scandal-1816649.html.

65 *Haxhiu v. Mukasey*, 519 F.3d 685 (7th Cir. 2008).

Armenia,[66] Azerbaijan,[67] Bangladesh,[68] Cameroon,[69] China,[70] Honduras,[71] India,[72] Italy,[73] Philippines,[74] Russia,[75] South Korea,[76] Switzerland,[77] Ukraine,[78] and Uzbekistan.[79] The United States grants asylum where an individual has a "well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion." Indeed, the U.S. Ninth Circuit Court of Appeals held that "official retaliation against those who expose and prosecute governmental corruption may, in appropriate circumstances, amount to persecution on account of political opinion"[80] and that "[w]histle-blowing against government corruption is an expression of political opinion."[81]

32. While beyond the scope of this Submission, an in-depth global survey of State asylum practice will likely reveal even more prevalent State practice protecting whistleblowers and recognizing them as a protected category on account of their political opinion and exercise of free expression.

66 *Antonyan v. Holder*, 642 F.3d 1250 (9th Cir. 2011); *Gyumushyan v. Holder*, 327 Fed. Appx. 37 (9th Cir. 2009); *Hayrapetyan v. Mukasey*, 534 F.3d 1330 (10th Cir. 2008); *Aleksanyan v. Gonzales*, 246 Fed. Appx. 471 (9th Cir. 2007); *Aroyan v. Gonzales*, 183 Fed. Appx. 634 (9th Cir. 2006); *Pashalyan v. Gonzases*, 185 Fed. Appx. 603 (9th Cir. 2006); *Harutyunyan v. Ashcroft*, 104 Fed. Appx. 86 (9th Cir. 2004); *Mamouzian v. Ashcroft*, 390 F.3d 1129 (9th Cir. 2004). Note that most US immigration decisions are unpublished.

67 *See Asylum through Immigration Court for Whistleblower from Azerbaijan*, IS LAW FIRM (May 15, 2012), *available at* http://islawfirm.com/asylum-through-immigration-court-for-whistleblower-from-azerbaijan/.

68 *Hasan v. Ashcroft*, 380 F.3d 1114 (9th Cir. 2004).

69 *Cameroonian Whistleblower and Political Activist Granted Asylum*, JONES DAY (July 2012), *available at* http://www.jonesdayprobono.com/experience/ExperienceDetail.aspx?exp=30879.

70 *Zhu v. Mukasey*, 537 F.3d 1034 (9th Cir. 2008); *Wang v. Mukasey*, 259 Fed. Appx. 763 (6th Cir. 2008); *Bu v. Gonzales*, 490 F.3d 424 (6th Cir. 2007); *Wang v. Gonzales*, 163 Fed. Appx. 489 (9th Cir. 2006); *Cao v. Attorney General*, 407 F.3d 146 (3rd Cir. 2005); *Xiao v. Ashcroft*, 98 Fed. Appx. 632 (9th Cir. 2004).

71 *Maldonado-Castro; Mejia-Almendarez v. Ashcroft*, 103 Fed. Appx. 113 (9th Cir. 2004).

72 *Nandha v. Gonzales*, 207 Fed. Appx. 875 (9th Cir. 2006); *Singh v. Gonzales*, 180 Fed. Appx. 747 (9th Cir. 2006).

73 *Massetti v. Gonzales*, 151 Fed. Appx. 519 (9th Cir. 2005).

74 *Grava v. Immigration and Naturalization Service*, 205 F.3d 1177 (9th Cir. 2000).

75 *Glistina v. Mukasey*, 284 Fed. Appx. 429 (9th Cir. 2008).

76 Jason Dzubow, *South Korean Spy Blows the Whistle, Gets Asylum*, ILW.COM (Feb. 9, 2012), *available at* http://blogs.ilw.com/entry.php?6172-South-Korean-Spy-Blows-the-Whistle-Gets-Asylum.

77 *Christoph Meili Returns – As Hero or Villain?*, SWISSINFO.CH (Apr. 9, 2009), *available at* http://www.swissinfo.ch/eng/christoph-meili-returns---as-hero-or-villain-/7330344.

78 *Morozov v. Mukasey*, 258 Fed. Appx. 138 (9th Cir. 2007); *Fedunyak v. Gonzales*, 477 F.3d 1126 (9th Cir. 2007); *Sagaydak v. Gonzales*, 405 F.3d 1035 (9th Cir. 2005).

79 *Mansurjonov v. Gonzales*, 241 Fed Appx. 443 (9th Cir. 2007).

80 *Grava v. Immigration and Naturalization Service*, 205 F.3d 1177, 1181 (9th Cir. 2000) ("When the alleged corruption is inextricably intertwined with governmental operation, the exposure and prosecution of such an abuse of public trust is necessarily political.").

81 *Baghdasaryan v. Holder*, 592 F.3d 1018, 1023 (9th Cir. 2010).

B. The vulnerability experienced by whistleblowers is shared by human rights fact-finding sources and publishers

1. Whistleblowers belong to a broader class of individuals, including UN monitors and human rights fact-finders, accessing and obtaining information in the public interest

33. While international human rights law and national practice acknowledges whistleblowers as a particularly vulnerable group, it is important to situate the role of whistleblowers with similarly-minded individuals who access and obtain information in the public interest. Whistleblowers, human rights sources and investigators, and the publishers and civil society members that reveal human rights violations all belong to a class of individuals facing particular vulnerability in the exercise of their rights under universal and regional instruments guaranteeing free expression. The concepts of source protection and whistleblowing are distinct but related; in essence, both categories concern the need for individuals to access and obtain information without a fear of retaliation. That retaliation may take several forms, whether it be compelled disclosure or other legal sanction.

34. International judicial bodies afford special testimonial protections to UN human rights defenders, sources, and humanitarians, as a necessary component of their work. For instance, members of the International Committee for the Red Cross enjoy a special status as protected persons under international law and an absolute privilege not to testify in international criminal proceedings, upheld by the ICTY in the *Simic* case.[82] The Trial Chamber acknowledged that "the disclosure of information gathered by its employees while performing official duties would destroy the relationship of trust on which it relies to carry out its mandate."[83] The ICRC must be allowed to gather information about detention conditions and status of detainees without being compelled to testify (for fear of retaliation); there is a public interest in their work that cannot be effectively achieved without protection.

35. The UN Special Court for Sierra Leone has recognized that the same principles establishing a qualified journalists' privilege apply to human rights fact-finders. In the *Brima* case, the prosecution called a UN staff member and human rights monitor as a witness, and the witness was only willing to give evidence if the Trial Chamber could guarantee that it would not compel him to identify sources. The Trial Chamber refused, in a decision subsequently overturned by the Appeals Chamber, finding that the lower chamber struck the wrong balance in weighing the "privileged relationship between a human rights officer and his informants" against the rights of the accused.[84]

36. In her amicus brief before the Appeals Chamber, the UN High Commissioner for Human Rights Navi Pillay underscored the importance of confidentiality in the work of human rights monitors,

82 *Prosecutor v. Blagoje Simic et al.,* ICTY, Trial Chamber, Decision on the Prosecution Motion Under Rule 73 for a Ruling Concerning the Testimony of a Witness, No. IT-95-9-PT (July 27, 1999), para 13.

83 *Id.* para. 65

84 *Prosecutor v. Alex Tamba Brima et al.*, SCSL, Decision on Prosecution Appeal Against Decision on Application for Witness TF1-150 to Testify Without Being Compelled to Answer Questions on Grounds of Confidentiality, SCSL, No. SCSL-2004-16-AR73 (May 26, 2006), para. 33.

stating that:

> confidentiality is an essential element of the working methods of UN human rights officers, and that their work is of fundamental importance to the restoration and maintenance of international peace and security, the rule of law, and the administration of justice.[85]

37. The High Commissioner further warned that source compulsion could "undermine the credibility of guarantees of confidentiality" which would lead to communities "being unwilling to cooperate with, and provide reliable information to, UN human rights officers, thereby making it impossible for the human rights officers to carry out their functions effectively."[86]

38. Similarly, Justice Teresa Anne Doherty, in dissenting from the Trial Chamber opinion, stressed the importance of protecting UN sources:

> It is on such information that international organisations and governments take political actions. ...[they] rely heavily on such reports and there is a public interest in the work and the information of Human Rights Officers as there is in media reports.[87]

39. Justice Geoffrey Robertson QC devoted his whole concurring opinion in the appeal decision to the issue, observing that the principles of source protection set forth by the ECtHR in its *Goodwin* case[88] was "equally applicable to human rights monitors giving evidence in war crimes courts." The whole passage is important and is thus reproduced in its entirety:

> The reasoning behind the protection of journalistic sources can, it seems to me, be applied in principle to human rights reporters, or at least to those "monitors" who are in effect tasked with collecting information for public purposes – to inform the reports of the UN Secretary General (which may well lead to Security Council action) or to research for reports issued to the public by NGOs like Amnesty and Human Rights Watch. There is in my judgement little meaningful difference in this respect between an investigative journalist tracking a story in a war-torn country, a war correspondent reporting on the ebb and flow of the conflict, and a researcher for a human rights organisation filing information for an "in depth" report or for filtered use in an annual report, or for a UN monitor gathering information for a Secretary General's report to the Security Council. All are exercising a right to freedom of expression, (and, more importantly, assisting their source's right of free speech) by extracting information for publication from people who would not give it without an assurance that their names will remain anonymous. The reprisal they often face in such circumstances, unlike the risk run by Mr. Goodwin's source of being sacked or sued for breach of confidence, is of being killed as an "informer" – a traitor to the organisation or the community on whom they are silently squealing. To identify them in court would betray a promise and open them to such reprisals: more importantly, if courts routinely ordered witnesses to name their sources, then information about human rights abuses would diminish because reporters could not in good conscience elicit it by promises to protect their sources. For these reasons, I consider that "human rights monitors", like journalists, have a privilege to refuse to name those sources to whom they have promised anonymity and who are in danger of reprisal if that promise is broken. In practical terms, that means they must not be compelled to do so by threats to invoke the court's power to

85 Amicus Curiae Brief of the United Nations High Commissioner for Human Rights, *Prosecutor v. Alex Tamba Brima et al.*, SCSL, No. SCSL-2004-16-AR73 (Dec. 16, 2005), paras. 32–34.

86 *Id.* para. 37.

87 *Prosecutor v. Alex Tamba Brima et al.*, Dissenting Opinion of Justice Doherty on the Prosecution's Oral Application for Leave to be Granted to Witness TF1-150 to Testify without being Compelled to Answer any Questions in Cross-Examination that the Witness Declines to Answer on Grounds of Confidentiality Pursuant to Rule 70(B) and (D) of the Rules, SCSL, No. SCSL-04-16-T (Sept. 22, 2005), para. 16.

88 *Goodwin v. United Kingdom*, no. 28957/95, ECHR 2002.

hold them in contempt and to fine or imprison them.[89]

40. Sources within the UN individual mandates are consistent with the *Brima* court's acknowledgment of the categorical risks faced by human rights monitors and their sources. For instance, the UN Special Rapporteur on the Situation of Human Rights Defenders is dedicated to protecting what the Human Rights Council identifies as "serious risks faced by human rights defenders due to threats, attacks, reprisals and acts of intimidation against them."

41. Philip Alston, UN Special Rapporteur on Extreme Poverty and Human Rights and former Rapporteur on extrajudicial, summary or arbitrary executions, found that safety and security for witnesses and sources were a grave concern over his fact-finding in six years of his position.[90] In particular, he notes how several high-level inquiries raise the stakes "for reprisals against those who testify, whether they be victims, serving or former security force members, or civil society representatives."[91]

42. The reality of risks faced by human rights fact-finders and sources closely track the challenges faced by whistleblowers, particularly in stigmatization, reprisal, and a recognized necessity for protection. Ultimately, whether whistleblowers are considered to be a form of human rights source, or a parallel category, the risks faced and international responses are the same in kind.

2. Those publishing the work of whistleblowers face persecution – case study of WikiLeaks

43. Article 22 of the ICCPR guarantees that "Everyone shall have the right to freedom of association with others." The permissible restrictions on this right are the same as those of Article 19: they must satisfy a tri-partite test. Restrictions must be provided for by law, pursue a legitimate aim, and be necessary and proportionate.

44. National laws sanctioning association of individuals with sources, such as conspiracy statutes, raise serious concerns under both Articles 19 and 22.

45. The ECtHR, for instance has held that journalists deserve special protection based on their association with sources, even where official secrets are involved. In *Damann v. Switzerland*,[92] a journalist was prosecuted and fined for inciting a source to disclose an official secret. The journalist, in the process of investigating a robbery, obtained information from an administrative assistant in a prosecutor's office regarding the criminal records of several individuals.

46. Finding a violation of Article 10, the ECtHR held that conviction and any penalty at all based on a journalist's association with a source, when there is no trickery, threat, or pressure, has a

89 *Prosecutor v. Alex Tamba Brima et al.*, SCSL, Concurring Opinion of Justice Robertson on Decision on Prosecution Appeal Against Decision on Oral Application for Witness TF1-150 to Testify Without Being Compelled to Answer Questions on Grounds of Confidentiality, No. SCSL-2004-16-AR73 (May 26, 2006), para. 28.

90 Philip Alston, *Safety Concerns for Human Rights Defender Witnesses to UN Fact Finders – UN Must Support – Women*, WUNRN (Sept. 16, 2013), *available at* http://www.wunrn.com/news/2013/09_13/09_16/091613_safety.htm.

91 *Id.*

92 No. 77551/01, 2006 ECHR.

chilling effect on journalists. This interference is not necessary in a democratic society and threatens to inhibit the press' public watchdog role on matters of public interest.

47. The same standard articulated by the ECtHR is echoed by the UN and regional rapporteurs on freedom of expression, who have clearly and repeatedly emphasized that publishers must face no liability for the receipt and dissemination of classified information:

> Public authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately classified information under their control. Other individuals, including journalists, media workers and civil society representatives, who receive and disseminate classified information because they believe it is in the public interest, should not be subject to liability unless they committed fraud or another crime to obtain the information.[93]

48. The OAS draft model law on whistleblowers warns against reprisals against the companions or others associated with whistleblowers.[94] The OAS rapporteur for freedom of expression has also made it clear (while citing past statements of the rapporteurships on WikiLeaks) that "under no circumstance, journalists, members of the media or members of civil society who merely disseminate public information classified as reserved, because they consider it to be of public interest, may be subjected to subsequent punishments for the mere fact of publication."[95]

49. The Tshwane Principles on National Security provide for an absolute defense from sanctions or conspiracy charges for publishers of classified information. Principle 47 provides:

> (a) A person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information;
> (b) A person who is not a public servant may not be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information.[96]

50. Germany amended its criminal law in 2012 to prevent journalists from being charged with aiding and abetting the "violation of official secrets" for disclosing classified information.[97]

51. Finally, the Council of Europe's Committee of Ministers observe the necessity that means of mass communication serve for "civil society representatives, whistleblowers and human rights defenders" and specifically warn against "politically motivated pressure exerted on privately operated Internet platforms and online service providers, and of other attacks against websites of independent media, human rights defenders, dissidents, whistleblowers and new media actors."[98] The Committee of Ministers in Recommendation No. R (2000) 7 also stipulates that

93 Ambeyi Ligabo, Miklos Haraszti, and Eduardo Bertoni, International Mechanisms for Promoting Freedom of Expression, Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, Joint Declaration on access to information and secrecy legislation (Apr. 2012).

94 OAS Model Law, Art. 28.

95 Catalina Botero Marino, Annual Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II.149 Doc. 50 (Dec. 31, 2013) [OAS Rapporteur 2013 Annual Report], para. 334.

96 Global Principles on National Security and the Right to Information (The Tshwane Principles) (June 12, 2013), Principle 47, Protection against Sanctions for the Possession and Dissemination of Classified Information by Persons Who Are Not Public Personnel.

97 Criminal Code (Germany), Section 353(b)(3)(a).

98 Council of Europe, Committee of Minsiters, Declaration of the Committee of Ministers on the protection of freedom of

States must protect journalists from judicial search, interception, or surveillance orders especially those seeking correspondence or contacts.[99]

52. **WikiLeaks has been subject to unrelenting persecution as a result of its publication. The US Department of Justice continues to attempt to prosecute WikiLeaks for its publications, including under a theory of conspiracy. This raises serious and substantial concerns for the fundamental rights of freedom of expression and association.**

53. WikiLeaks' position is that it maintains a dropbox for documents and sources submit materials to that dropbox. In other cases, CCR's experience is that journalists and media outlets will often meet and interact with sources. However, in both situations the US Justice Department insists that the publishers are associated with their sources and are subject to potential legal sanctions as a result.

54. **United States attempts to prosecute WikiLeaks for its publications are confirmed to be ongoing, in their fifth year, as of April 2015.**[100] On March 4, 2015, a US federal court in the District of Columbia confirmed that there is an "ongoing multi subject" and "national security" investigation into WikiLeaks.[101] On April 25, 2014, the DOJ described that there were:

> criminal/national security investigation(s) in to the unauthorized disclosure of classified information that was published on the WikiLeaks website. The investigation of the unauthorized disclosure is a multi-subject investigation and is still active and ongoing.[102]

---

expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers (Adopted by the Committee of Ministers on 7 December 2011 at the 1129th meeting of the Ministers' Deputies), para. 7.

99 Council of Europe, Committee of Ministers, Recommendation No. R (2000) 7, Of the Committee of Ministers to Member States on the Right of Journalists Not to Disclose Their Sources of Information (Adopted by the Committee of Ministers on 8 March 2000, at the 701st Meeting of the Ministers' Deputies), Principle 6.

100 On April 27, 2015, a spokesperson for the US Department of Justice (DOJ) stated to a reporter in an e-mail regarding WikiLeaks that "The Department of Justice is conducting an investigation, and it remains ongoing." Kashmir Hill, *Three Days in Beijing with Three of the World's Most Famous Dissidents*, FUSION **(**Apr. 27, 2015), *available at* http://fusion.net/story/125475/ai-weiwei-jacob-appelbaum-and-laura-poitras/.

101 *Electronic Privacy Information Center v. Dep't of Justice Criminal Division et al.*, Memorandum Opinion, Granting in Part & Denying in Part Defendants' Motion for Summary Judgment; Granting in Part & Denying in Part Plaintiff's Motion for Summary Judgment, No. 12-127 (D.D.C. Mar. 4, 2015), *available at* https://epic.org/foia/doj/wikileaks/EPIC-v-DOJ-Wikileaks-Opinion.pdf. This was in response to a freedom of information law request filed to three branches of the Justice Department including the Criminal Division and the Federal Bureau of Investigation (FBI) and National Security Division seeking records related to government surveillance of supporters of WikiLeaks. The court allowed the Criminal Division and FBI to withhold records based on the ongoing status of the investigation, but held that the National Security Division failed to justify its nondisclosure. The investigation into WikiLeaks began by the US Diplomatic Security Service as early as February 18, 2010, following WikiLeaks' publication of an Icelandic diplomatic cable. *See* Alexa O'Brien, Under-Secretary of State Patrick Kennedy's testimony in the Bradley Manning trial, Transcript (Aug. 5, 2013), *available at* https://www.documentcloud.org/documents/748337-20130805-am-fop-transcript-of-us-v-pfc-bradley.html#document/p26/a145019.

102 *Electronic Privacy Information Center v. Dep't of Justice Criminal Division et al.*, Defendant's Supplemental Brief in Response to the Court's March 17, 2014 Minute Order, and in Further Support of Defendant's Motion for Summary Judgment, No. 12-127 (D.D.C. Apr. 25, 2014), *available at* http://epic.org/foia/doj/wikileaks/33_Def_Sup_Brief.pdf.

55. The Justice Department in 2012 seized the Google accounts, e-mails, contacts, and metadata of several WikiLeaks staff seeking evidence of conspiracy and conspiracy to commit espionage.[103] WikiLeaks staff were not notified until December 2014. CCR wrote to Google and the Justice Department in January 2015 demanding an explanation for the execution of warrants for publishers and astonishing delay in notification;[104] in the process CCR learned that Google "litigated up and down" against the Justice Department to notify WikiLeaks of the warrants, but was still gagged from disclosing them.[105]

56. Prosecutors in the court-martial of alleged WikiLeaks source Pfc. Manning continuously attempted to draw a link from Assange to Manning, and Assange's name was mentioned repeatedly throughout Manning's court martial proceedings, "over and over" and over twenty times by the military in its closing arguments.[106] Search warrants executed for Manning's Youtube accounts specifically sought evidence of communications with WikiLeaks.[107] The cruel, inhuman and degrading treatment found by UN Torture Rapporteur Juan Méndez, was, in the view of Manning's lawyer and over 250 law professors analyzing the case, part of an effort by the US Army to pressure Manning to implicate Assange.[108]

57. Indeed, this 'conspiracy theory' for investigation has been widely criticized by the UN and

103 In the Matter of the Search of information associated with [REDACTED] that is stored at premises controlled by Google, Inc., Search and Seizure Warrant, No. 1:12-SW-227 (E.D.V.A. Mar. 22, 2012) (Sarah Harrison), *available at* https://wikileaks.org/google-warrant/227-harrison.html; *see also* In the Matter of the Search of information associated with [REDACTED] that is stored at premises controlled by Google, Inc., Search and Seizure Warrant, No. 1:12-SW-228 (E.D.V.A. Mar. 22, 2012) (Joseph Farrell); In the Matter of the Search of information associated with [REDACTED] that is stored at premises controlled by Google, Inc., Search and Seizure Warrant, No. 1:12-SW-229 (E.D.V.A. Mar. 22, 2012) (Kristinn Hrafnsson).

104 *Google Hands Data to US Government in WikiLeaks Espionage Case*, WIKILEAKS (Jan. 26, 2015), *available at* https://wikileaks.org/google-warrant.html.

105 Ellen Nakashima & Julie Tate, *Google Says it Fought Gag Orders in WikiLeaks Investigation*, WASHINGTON POST (Jan. 28, 2015), *available at* http://www.washingtonpost.com/world/national-security/google-says-it-fought-gag-orders-in-wikileaks-investigation/2015/01/28/e62bfd04-a5c9-11e4-a06b-9df2002b86a0_story.html.

106 "In the course of making that argument, the government's prosecutors keep mentioning Assange's name. Over and over. So far in the trial, he has been referenced 22 times." Matt Sledge, *Julian Assange Emerges As Central Figure In Bradley Manning Trial*, HUFFINGTON POST (June 19, 2013), *available at* http://www.huffingtonpost.com/2013/06/19/julian-assange-bradley-manning-trial_n_3462502.html.

107 In the Matter of the Search of the Youtube Account BRADMANNING, Maintained on the Computer Systems of Google, Inc., Application for a Seizure Warrant, No. 1:13-SW-492 (E.D.V.A. July 5, 2013), p. 10-12, *available at* https://www.documentcloud.org/documents/811547-1-13sw446-application-for-search-warrant.html (seeking evidence of communications between Manning and the "sunshinepress" account which prosecutors alleged to be "associated with and/or controlled by WikiLeaks").

108 Kim Zetter, *UN Torture Chief: Bradley Manning Treatment Was Cruel, Inhuman*, WIRED (Mar. 12, 2012), *available at* http://www.wired.com/2012/03/manning-treatment-inhuman; Bruce Ackerman & Yochai Benkler, *Private Manning's Humiliation*, N.Y. REVIEW (Apr. 28, 2011), *available at* http://www.nybooks.com/articles/archives/2011/apr/28/private-mannings-humiliation/.

regional rapporteurs on freedom of opinion and expression,[109] as well as by Juan Méndez.[110] Free speech and human rights organizations worldwide, including Article 19, Reporters Without Borders, Human Rights Watch and Freedom of the Press Foundation observe that:

> prosecution of WikiLeaks or Mr. Assange for publishing classified material or interacting with sources could criminalize the newsgathering process and put all editors and journalists at risk of prosecution.[111]

58. The attempts to prosecute WikiLeaks have been described by US diplomats as "unprecedented" in "scale and nature"[112] and have involved grand jury proceedings,[113] searches and surveillance of WikiLeaks staff, affiliates, and perceived affiliates,[114] and placement of editor-in-chief Julian Assange on an NSA "MANHUNTING" timeline with members of terrorist organizations.[115] An ongoing, extrajudicial financial blockade of WikiLeaks was condemned by the UN freedom of expression rapporteur,[116] called "completely illegal" by Reporters Without Borders, and held unlawful by the Icelandic Supreme Court.[117] The Federal Bureau of Investigation (FBI)

---

109 *See* UN Special Rapporteur on the Promotion and Protection the Right to Freedom of Opinion and Expression, Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression, Joint Statement On Wikileaks (Dec. 21, 2010) [Freedom of Expression Rapporteurs, Joint Statement on WikiLeaks] (reiterating the obligations of States to respect the right to access information in responding to publications of WikiLeaks and mainstream publishers, warning against "illegitimate interference" and "illegitimate retributive action").

110 *UN Special Rapporteur Juan Méndez: Instead of Focusing on Assange, U.S. Should Address WikiLeaks' Disclosures of Torture*, DEMOCRACY NOW! (Dec. 2, 2010), *available at* http://www.democracynow.org/2010/12/2/un_special_rapporteur_juan_mendez_instead.

111 *Letter to Eric Holder in Support of WikiLeaks*, ARTICLE 19 (June 24, 2014), *available at* http://www.article19.org/resources.php/resource/37599/en/letter-to-eric-holder-in-support-of-wikileaks.

112 Philip Dorling, *Assange Targeted by FBI Probe, US Court Documents Reveal*, SYDNEY MORNING HERALD (May 20, 2014), *available at* http://www.smh.com.au/world/assange-targeted-by-fbi-probe-us-court-documents-reveal-20140520-38l1p.html.

113 E.g., Glenn Greenwald, *FBI Serves Grand Jury Subpoena Likely Relating to WikiLeaks*, SALON (Apr. 27, 2011), *available at* http://www.salon.com/2011/04/27/wikileaks_26.

114 *See, e.g.*, Meredith Bennett-Smith, *Google Gave U.S. Government Emails from WikiLeaks* Volunteers Smari McCarthy, Herbert Snorrason, HUFFINGTON POST (June 24, 2013), *available at* http://www.huffingtonpost.com/2013/06/24/google-wikileaks-smari-mccarthy-herbert-snorrason_n_3492076.html; *see also USA v. In re a Search Warrant Issued to Google, Inc. on August 24, 2011*, Docket (E.D.V.A. Aug. 24, 2011), *available at* http://alexaobrien.com/archives/1293.

115 Glenn Greenwald & Ryan Gallagher, *Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and its Supporters*, THE INTERCEPT (Feb. 18, 2014), *available at* https://firstlook.org/theintercept/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/ [WikiLeaks Surveillance Article, THE INTERCEPT].

116 Freedom of Expression Rapporteurs, Joint Statement on WikiLeaks ("Direct or indirect government interference in or pressure exerted upon any expression or information transmitted through any means of oral, written, artistic, visual or electronic communication must be prohibited by law when it is aimed at influencing content . . . Calls by public officials for illegitimate retributive action are not acceptable.").

117 On 24 April 2013, Iceland's Supreme Court ordered VISA subcontractor Valitor to reopen the gateway for WikiLeaks donations, one of the arms of the economic blockade. *Court Orders Visa Subcontractor to Lift Block on Payments to WikiLeaks*, REPORTERS WITHOUT BORDERS (Apr. 26, 2013), a*vailable at* http://en.rsf.org/iceland-court-orders-visa-subcontractor-to-26-04-2013,44440.html. Since November 2010, financial companies blocked all payments for WikiLeaks following active calls and correspondence by US Senator Joseph Lieberman and US Representative Peter King demanding US companies to cut any support for WikiLeaks. Michael Tennant, *Documents Show Lieberman, King Behind Financial Blockade of WikiLeaks*, NEW AMERICAN (Nov. 28, 2012), *available at* http://www.thenewamerican.com/usnews/congress/item/13762-documents-show-lieberman-king-behind-financial-

represented in court in 2012 that its file on WikiLeaks was then 42,135 pages long.[118]

59. **The net of the investigation of WikiLeaks has significantly expanded beyond WikiLeaks' publication and association with whistleblowers, but also to individuals associated with or perceived to be associated with WikiLeaks.** In June 2015, journalist, security expert and TOR developer Jacob Appelbaum revealed that the US Justice Department had executed orders for his Google records in 2011 as part of the WikiLeaks investigation.[119] The Justice Department aggressively litigated to prevent Google from notifying Appelbaum for over four years. The Justice Department asserted that "journalists have no special privilege to resist compelled disclosure of their records, absent evidence that the government is acting in bad faith."[120]

60. Indeed, since 2010 the Justice Department has executed scores of search warrants and electronic communications orders, only a fraction of which are publicly known,[121] targeted toward perceived associates of WikiLeaks. Internal NSA documents disclosed by Edward Snowden reveal GCHQ surveillance of all visitors to WikiLeaks website as well as an "international effort to focus the legal element of national power upon non-state actor Assange, *and the human network that supports WikiLeaks*."[122]

61. WikiLeaks continues to publish documents submitted by sources. WikiLeaks is widely credited for ensuring that whistleblower Edward Snowden was able to exercise his legal right to seek asylum.[123] Julian Assange remains one of the world's premiere writers and thinkers on whistleblowers, freedom of the press, geopolitics and surveillance, and is highly-sought after as an author and keynote speaker.[124] He presently sits on the board of directors of the Courage

blockade-of-wikileaks; *see generally Banking Blockade*, WIKILEAKS (Oct. 24, 2011), *available at* https://www.wikileaks.org/Banking-Blockade.html. The companies that complied with their pressure include VISA, PayPal, MasterCard, Bank of America, Western Union. Further, WikiLeaks and Assange were placed on bank blacklists, according to internal correspondence from one financial firm.

118 In the court-martial of Pfc. Chelsea Manning, the FBI file on WikiLeaks was represented by the government prosecutor in June 2012 to be 42,135 pages or 3,475 documents. Alexa O'Brien, *U.S. v. Pfc. Manning*, Article 39(a) Session, Transcript (June 6, 2012), *available at* http://alexaobrien.com/archives/1523.

119 Ryan Gallagher, REVEALED: HOW DOJ GAGGED GOOGLE OVER SURVEILLANCE OF WIKILEAKS VOLUNTEER, THE INTERCEPT (June 20, 2015), *available at* https://firstlook.org/theintercept/2015/06/20/wikileaks-jacob-appelbaum-google-investigation; *see also* Julia Angwin, *Secret Orders Target Email: WikiLeaks Backer's Information Sought*, WALL STREET JOURNAL (Oct. 10, 2011), *available at* http://www.wsj.com/articles/SB10001424052970203476804576613284007315072.

120 In the Matter of the 2703(d) Order and 2703(f) Preservation Request Relating to Gmail Account, Response of the United States to Google's Motion to Modify 2703(d) Order for Purpose of Providing Notice to User, No: 1:10GJ3793 (E.D.V.A. Jan. 28, 2011), p. 7, *available at* https://www.documentcloud.org/documents/2108000-unsealed-documents-google-appelbaum-wikileaks-case.html.

121 Alexa O'Brien, *List of every sealed search warrant in Eastern District of Virginia, May 2010-April 2013* (June 22, 2013), *available at* http://alexaobrien.com/archives/1308.

122 WikiLeaks Surveillance Article, THE INTERCEPT (emphasis added).

123 *See, e.g.*, Glenn Greenwald, NO PLACE TO HIDE, ACKNOWLEDGMENTS (2014) ("Snowden was able to remain free and thus able to participate in the debate he helped trigger because of the daring, indispensable support given by WikiLeaks and its official, Sarah Harrison, who helped him leave Hong Kong and then remained with him for months in Moscow at the expense of her ability to safely return to the Untied Kingdom, her own country. ").

124 *See, e.g.* Julian Assange, THE WIKILEAKS FILES: THE WORLD ACCORDING TO US EMPIRE (forthcoming 2015); Assange, *Who Should Own the Internet?* N.Y. TIMES (Dec. 4, 2014), *available at* http://www.nytimes.com/2014/12/04/opinion/julian-assange-on-living-in-a-surveillance-society.html; Assange, WHEN

Foundation,[125] an international organization committed to the defense of whistleblowers and others seeking access to information in the public interest. Courage runs the official defense funds of Edward Snowden as well as several truth-tellers.

62. The US Justice Department has on other occasions executed search warrants against journalists on the basis of their association with whistleblowers. Prominently, the Justice Department in 2010 executed a search warrant for the e-mail account of FOX News reporter James Rosen on the basis that he "aided/abetted" and was a "co-conspirator" for a source.[126]

63. CCR presents the aforementioned evidence to provide a brief overview of the ongoing attempts to prosecute WikiLeaks, rather than to construct a comprehensive timeline of all known steps taken against WikiLeaks by the Justice Department. The investigation of WikiLeaks on basis of its publishing work raises serious issues for the fundamental rights of freedom of expression and association.

64. CCR's experiences representing WikiLeaks and Julian Assange underscore the issue that persecution and censorship of whistleblowers does not stop at the whistleblower, but encompasses human rights monitors and publishers as well. The ultimate effect of these restrictions is an unacceptable chilling on the free flow of information, rights to access information, and freedom of expression.

II. States must ensure that cyber laws properly conform to their obligations to protect freedom of expression. States must not prosecute whistleblowers for technical computer crimes for using work computers to access information with the intent of whistleblowing.

> *In any case, in adopting a criminal policy in this field [cyber crime], States must ensure that it is in conformance with international obligations in the field of human rights and particularly avoid it disproportionately restricting the freedom to seek, receive and disseminate information and ideas of all kinds or generating dissuasive effects in the exercise of those rights.*[127]

A. International standards on "unauthorized access"

65. Every regional instrument on cyber crime requires that States criminalize some form of "unauthorized access" to computer systems. The broadest convention is the Council of Europe Convention on Cybercrime CETS, adopted in 2001 and ratified by forty-six countries including

---

GOOGLE MET WIKILEAKS (2014); Assange; CYPHERPUNKS: FREEDOM AND THE FUTURE OF THE INTERNET (2012); Assange, *Why the World Needs WikiLeaks*, TEDGLOBAL (July 2010).

125 *About Courage*, COURAGE FOUNDATION, *available at* https://couragefound.org/about-the-courage-foundation/.

126 In the Matter of the Search of E-mail Account [REDACTED]@gmail.com on Computer Servers Operated by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California, Application for a Search Warrant, No. 10-291-M-01 (D.D.C. May 28, 2010), para. 40.

127 OAS Rapporteur 2013 Annual Report, para. 713.

the United States and Japan.[128] In addition, unauthorized access is criminalized by respective recommendation/mandate of the African Union,[129] the European Union,[130] the Organization of American States,[131] the Arab League,[132] Commonwealth,[133] Commonwealth of Independent States,[134] Caribbean countries,[135] and the Shanghai Cooperation Organization.[136]

66. The UN General Assembly has stipulated that "security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and

128 Council of Europe, Convention on Cybercrime, Adopted by the Committee of Ministers, 109th Session on 8 November 2001, Budapest (Nov. 23, 2001). Article 2 on "illegal access" sets forth: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

129 African Union Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) (2014), Art. 29. "State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to: a) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access; b) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence."

130 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013). "Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor." Further, "without right" means conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.

131 Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity AG/RES. 2004 (XXXIV-O/04), p. 10, reiterated in Inter-American Committee Against Terrorism (CICTE), Declaration Strengthening Cyber-Security in the Americas, OEA/Ser.L/X.2.12 CICTE/DEC.1/12 rev. 1 (Mar. 9, 2012), *available at* https://ccdcoe.org/sites/default/files/documents/OAS-120307-DeclarationCSAmericas.pdf ("Conduct, such as accessing computers without authorization, illegal interception of data, interference with the availability of computer systems, and theft and sabotage of data, should be deemed illegal under the law of each member state."). OAS Member States also give consideration to applying the principles of the Council of Europe's Convention on Cyber-Crime. OAS Member State Legislation, DEPARTMENT OF LEGAL COOPERATION, *available at* http://www.oas.org/juridico/english/cyber_legis.htm.

132 Arab League Cyber Crime Convention, Art. 6. "Offense of Illicit Access: 1-Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. Arab Convention on Combating Information Technology Offences."

133 Report of the Commonwealth Working Group of Experts on Cybercrime, Model Law on Computer and Computer Related Crime, (LMM(02)17) (Oct. 2002), *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb%20rev_final_CoE.pdf ("A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.").

134 Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information (Jan. 15, 2008), *available at* https://cms.unov.org/documentrepositoryindexer/GetDocInOriginalFormat.drsx?DocID=5b7de69a-730e-43ce-9623-9a103f5cabc0. "The Parties shall, subject to their national legislation, establish the following as criminal acts, where

transparency."[137]

67. It is critical to anticipate the impact of these measures on freedom of expression. Many sources and whistleblowers, particularly those working for a government, will use a computer to access primary documents. And increasingly, whistleblowers who access materials via computer systems prosecuted not only under espionage laws, but also under computer crime laws.

B. Technical computer violations are displacing secrecy laws as a tool to restrict the rights of expression of whistleblowers and publishers

68. Whistleblowers must not be punished for using a computer to blow the whistle. Yet, in the United States, the cases of Pfc. Chelsea Manning, NSA whistleblower Thomas Drake, and WikiLeaks show that technical violations are used against whistleblowers and publishers for exercising their fundamental rights to expression. Emerging cyber crime conventions, particularly those of the League of Arab States and the Shanghai Cooperation Organization, explicitly curtail access to and dissemination of information. In other States, civil society organizations have begun to address the serious risk that cyber laws pose to whistleblowers and publishers. These laws threaten to punish individuals based purely on their intent to disseminate information.

69. Manning's court-martial is an illustrative case of the use of technical violations to punish a whistleblower. Manning was court-martialed under two counts of the Computer Fraud and

---

such acts are committed intentionally: (a) The illegal accessing of computer information protected by the law, where such act results in the destruction, blocking, modification or copying of information or in the disruption of the functioning of the computer, the computer system or related networks . . . (c) The violation of regulations governing the use of computers, computer systems or related networks by a person who has access to those computers, systems or networks, resulting in the destruction, blocking or modification of computer information protected by the law, where such act causes significant harm or serious consequences."

135 Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR), Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts (2012), p. 12 ("There shall be a provision criminalizing the intentional and illegal access to a computer system as well as illegally remaining in a computer system. An aggravation of penalty in cases where protection measures were circumvented to intercept the transmission could be taken into consideration."); s*ee also id.* at p. 19 ("Illegal Access 1. (1) A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. (2) A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent."); *id. a*t p. 20 ("Data Espionage 8. (1) A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification obtains, for himself or for another, computer data which are not meant for him and which are specially protected against unauthorized access, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. (2) A country may limit the criminalisation to certain categories of computer data.").

136 Shanghai Cooperation Organization Cyber Crime Treaty. Signed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan in 2008.

137 Resolution on the 'Creation of a global culture of cyber security', U.N. Doc. A/RES/57/239 (Jan. 31, 2003).

Abuse Act (18 U.S.C. § 1030) for 'exceeding authorized access' to a computer system.[138] Manning had clearance to access the systems from which she obtained documents, and used a commonplace utility called 'WGet' to retrieve them. In response to objections from Manning's defense team, Judge Denise Lind held that she would "adopt a narrow meaning of 'exceeds authorized access' under the Computer Fraud and Abuse Act and will instruct the fact finder that the term 'exceeds authorized access' is limited to violations of restrictions on access to information and not restrictions on its use." Judge Lind was clear that exceeding access cannot include mere violation of terms-of-use agreements. Manning was nevertheless convicted of both counts.

70. There is substantial evidence that WikiLeaks remains under investigation on a conspiracy theory for the alleged computer offenses of its sources. In December 2014, Google revealed to several WikiLeaks staff that in 2012 the US government served several search warrants on the company for all the e-mail account content, metadata, contacts, and subscriber information on several WikiLeaks staff. The search warrants sought evidence of violations of the US Computer Fraud and Abuse and conspiracy statutes.[139]

71. In another instance from the United States, former NSA employee Thomas Drake faced 35 years imprisonment for his alleged role in the 2007 disclosure to a journalist of information about massive financial waste, abuse, and bureaucratic dysfunction in NSA counterterrorism and surveillance programs.[140] He was initially indicted under the espionage act. Drake ultimately pled guilty to a misdeameanor count of "exceeding authorized access" to a computer system; the Justice Department maintained that using existing access to a system with the intent of whistleblowing is unlawful.[141]

72. The use of access statutes based on the *mens rea* of an individual who may already possess clearance to access a system raises significant concerns under the principle of legitimacy.

73. The problem is not limited to the United States: the relevant League of Arab States Convention explicitly requires its member States to prosecute disclosure of state secrets under cyber laws. It

138 *United States v. Pfc. Bradley Manning*, Charge Sheet (Mar. 1, 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/03/PFC-Manning_Additional-Charge-Sheet_REDACTED_02MAR11.pdf.

139 In the Matter of the Search of information associated with [REDACTED] that is stored at premises controlled by Google, Inc., Search and Seizure Warrant, No. 1:12-SW-227 (E.D.V.A. Mar. 22, 2012) (Sarah Harrison), *available at* https://wikileaks.org/google-warrant/227-harrison.html; *see also* In the Matter of the Search of information associated with [REDACTED] that is stored at premises controlled by Google, Inc., Search and Seizure Warrant, No. 1:12-SW-228 (E.D.V.A. Mar. 22, 2012) (Joseph Farrell); In the Matter of the Search of information associated with [REDACTED] that is stored at premises controlled by Google, Inc., Search and Seizure Warrant, No. 1:12-SW-229 (E.D.V.A. Mar. 22, 2012) (Kristinn Hrafnsson).

140 Marcy Wheeler, *Government Case Against Whistleblower Thomas Drake Collapses*, THE NATION (June 13, 2011), *available at* http://www.thenation.com/article/161376/government-case-against-whistleblower-thomas-drake-collapses.

141 U.S. Department of Justice, Former NSA Senior Executive Pleads Guilty to Unauthorized Access of Government Computer, Office of Public Affairs, (June 10, 2011), *available at* http://www.justice.gov/opa/pr/former-nsa-senior-executive-pleads-guilty-unauthorized-access-government-computer ("Individuals who are granted special access to our nation's most sensitive information cannot unilaterally decide to disregard the law and agreements they make with the government on how that information may be handled.").

stipulates that punishment "shall be increased" if it leads to "the acquirement of secret government information." The Convention also requires "Every State Party shall commit itself to increasing the punishment for traditional crimes when they are committed by means of information technology."[142]

74. The Shanghai Cooperation Organization cyber agreement declares as a threat "[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environments of other States" or:

> appearance and replication of information in digital (radio and television) and other mass media, on the Internet and other information exchange networks that: distorts the perception of the political system, social order, domestic and foreign policy, important political and social processed in the State, spiritual, moral and cultural values of its population.[143]

75. In other States, civil society organizations predict that authorized access cyber laws will be used to prosecute whistleblowers "in breach of international standards of freedom of expression." For example, Article 19, in analyzing Kenya's Cybercrime law, determined that:

> section 4 in its current form would allow the prosecution of potential whistleblowers in breach of international standards of freedom of expression. Indeed, it would suffice that an individual who is authorised to have access to certain types of computer data and programmes 'intends' to commit an offence under any law, without actually having committed the offence itself (which, as noted above is undefined). For instance, individuals who are authorised to have access to classified material, like Mr Snowden, and who merely 'intend' to release that material could be prosecuted even before they release the material in question.[144]

76. Similarly, in analyzing cyber crime legislation in Pakistan, Article 19 and Digital Rights Foundation Pakistan also found a measure to be "hopelessly broad" due to the amorpheous definition of 'authorized':

> For instance, section 3 of the Bill criminalises "whoever intentionally gains unauthorised access to any information system or data". The offence is punishable by imprisonment for a term, which may extend to 3 months or a fine of up to 50,000 rupees or both. This offence is hopelessly broad, in violation of the legality requirement under international human rights law. If the Bill were adopted, individuals seeking access to information on websites blocked by the government could potentially be prosecuted, as access to that information would not be 'authorised'.[145]

C. "Unauthorized access" sanctions must be provided for by law, be proportionate, and respect freedom of expression

77. Restrictions on the right to seek, receive, and impart information pursuant to Article 19 of the

142 Arab League Cyber Crime Convention, Art. 6.

143 Shanghai Cooperation Organization Cyber Crime Treaty.

144 KENYA: CYBERCRIME AND COMPUTER RELATED CRIMES BILL, LEGAL ANALYSIS, ARTICLE 19 (2014), p. 14, *available at* http://www.article19.org/data/files/medialibrary/37652/Kenya-Cybercrime-Bill-129072014-BB.pdf.

145 PAKISTAN: NEW CYBERCRIME BILL THREATENS THE RIGHTS TO PRIVACY AND FREE EXPRESSION,, LEGAL ANALYSIS, ARTICLE 19, DIGITAL RIGHTS FOUNDATION PAKISTAN (2014), p. 2, *available at* http://www.article19.org/data/files/medialibrary/37932/Pakistan-Cybercrime-Joint-Analysis_20-April-2015.pdf.

ICCPR must satisfy a tripartite test: they must be provided for by law under the clearest and most precise terms possible, pursue a legitimate objective recognized by international law, and be necessary to achieve this objective. Under standards of the ECtHR, limitations on Article 10 of the European Convention must be lawful, serve a legitimate purpose, and "necessary in a democratic society."[146]

78. Cyber laws raise issues not only because they may replace secrecy laws as a means to prosecute the free flow of information, but also because they may not conform to principles of legal certainty. Legal certainty requires that criminal offences are precisely defined so that individuals know how to avoid sanctions. Vagueness is not permissible in the definition of criminal offences. The phrase "authorized access" must be "provided for by law," which means that a restriction "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly."[147] When limitations imposed by criminal norms are involved, the Inter-American Court has stated that additionally, the inherent demands of strict legality must be satisfied: "If the restriction or limitation stems from criminal law, the strict requirements characteristic of criminal classification must be observed in order to satisfy the principle of legality in this realm."[148]

79. The definition of "authorized" may be vague or subject to change, according to terms-of-use agreements, the subjective determination of supervisors, or the subsequent use of information. State practice in the United States alone reveals evidence of all three.[149]

80. In its General Comment 34, the Human Rights Committee warned that "extreme care" must be taken when States invoke laws to "suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information."[150]

81. Indeed, the previous UN and regional rapporteurs on freedom of opinion and expression have already addressed the problem of legal certainty specifically in response to the investigation of WikiLeaks:

> Any attempt to impose subsequent liability on those who disseminate classified information *should be grounded in previously established laws* enforced by impartial and independent legal systems with full respect for due process

146 European Convention on Human Rights, Art. 10(2).

147 Human Rights Committee, *de Groot v. The Netherlands*, 1995 CCPR/C/54/D/578/1994, Comm. No. 578/1994, (July 14, 1995).

148 IACtHR, *Case of Usón Ramírez v. Venezuela*, Preliminary Objection, Merits, Reparations and Costs, Series C No. 207 (Nov. 20, 2009), para. 55.

149 US courts, for instance, are split on the issue of whether unauthorized access can apply to employees who already have authority to access systems but use that access for a means not approved by their employer. The First, Fifth, Seventh and Eleventh Circuits have held that employers can bring civil suits against their former employees under the CFAA. *See United States v. John*, 597 F.3d 263 (5th Cir. 2010), *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012); *WEC Carolina Energy Solutions, LLC v Miller, et al*., Case No.11-1201 (4th Cir. 2012).

150 Human Rights Committee, General Comment No. 34, CCPR/C/GC/34 (2011).

guarantees, including the right to appeal.[151]

82. The OAS Rapporteur on Freedom of Expression also expressed concern regarding legal certainty in cyber crime legislation:

> [W]hen taking initiatives to punish cyber crime, the States must include explicit safeguards in the norms to ensure that legitimate conducts are not criminalized, such as the requirement that the involved act involve damages and that they be carried out with the intention of committing a crime.[152]

83. On that same point, the UK Joint Human Rights Committee criticized on grounds of legal certainty the UK government's recent implementation of its Computer Misuse Act, which makes a criminal offence of "unauthorized acts in relation to a computer causing serious damage to human welfare, the environment, the economy or national security in any country."[153]

84. The European Union's framework decision on attacks against information systems requires States to take positive steps principles of legal certainty, holding that "States and public bodies remain fully bound to guarantee respect for human rights and fundamental freedoms, in accordance with existing international obligations," going on to provide that restrictions on access cannot be arbitrary:

> In the context of this Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings.[154]

85. Various jurisdictions have reigned in the scope of authorized access. Australia's Model Criminal Code Officers Committee (MCCOC), an authoritative national interpretative body, recommends that liability for unauthorized access to computers should not occur where a defendant "misuses" existing authorization or uses it for an "ulterior purpose."[155] Australia's criminal code

151 Freedom of Expression Rapporteurs, Joint Statement on WikiLeaks (emphasis added).

152 OAS Rapporteur 2013 Annual Report, para. 764. The report goes on to say "Indeed, this limited focus makes it possible, among other things, to prevent a broad view of the concept of 'cybersecurity' from leading to the creation of new 'computer crimes,' or to an increase in the penalties of criminal conducts that are not aimed at attacking the integrity of the web and the infrastructure of the Internet, or the integrity and confidentiality of the information they contain."

153 Clause 40, inserting new s. 3ZA into the Computer Misuse Act 1990, 1.28-1.38, *available at* http://www.publications.parliament.uk/pa/jt201415/jtselect/jtrights/49/4903.htm (acknowledging that while there is no "doubt the need to ensure that the criminal law provides adequate protection against cyber-attacks on critical infrastructure," the Committee is skeptical that the definitions of damage are written in terms "sufficiently certain in their meaning to justify their inclusion as an ingredient of a criminal offence carrying maximum sentences of 14 years and life imprisonment."); *see also* Sentencing UK Hackers to Life in Prison Is Measure Against Whistleblowers—Activists, RT (Oct 23, 2014), *available at* http://rt.com/uk/198668-uk-cyber-security-prison/.

154 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Aug. 14, 2013).

155 Model Criminal Code Officers Committee of the Standing Committee of the Attorneys-General, Report, Model Criminal Code, Chapter 4, Damage and Computer Offences (2001) [MCCOC Report], p. 141, 145-46.

reflects this.[156] The United Kingdom's House of Lords has held similarly.[157] In *DPP v. Murdoch* (1993) 1 VR 406, Hayne J suggested that entry to a computer system would not be trespassory if the person had a general permission to use the system, even though entry was for the purpose of committing a fraud. MCCOC criticized the scope of a proposed New Zealand illegal access law because it appeared to "risk the creation of opportunities for oppressive prosecution of journalists and others who use information originally obtained by unauthorised access to a computer."[158]

86. In sum, while there exist legitimate cyber crime threats, extreme care must be taken to ensure that restrictions on rights to freedom of expression comply with the tripartite test, particularly with respect to the legality principle. The UN General Assembly has iterated "the necessity of respecting and protecting human rights and fundamental freedoms in the prevention of crime and the administration of, and access to, justice, including criminal justice."[159]

CONCLUSION

87. CCR respectfully asks the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to recognize that:

- Individuals who, in the public interest, access and collect information exposing abuses must be protected from persecution as a category of persons. In this regard, whistleblowers share common ground with human rights fact-finding sources who face particular vulnerability on account of their exercise of rights to freedom of expression.

- Those associated, or perceived to be associated with whistleblowers because they publish face particular risk of persecution in a manner that jeopardizes their rights to seek, receive, and impart information and freedom of association. The risk is particularly aggravated through the use of conspiracy or incitement laws against members of the media.

- States must ensure that cyber laws conform to their obligations to protect freedom of expression. Specifically, cyber laws criminalizing "unauthorized access," based purely on a source's intent to disclose information, risk displacing secrecy laws as a means for prosecuting sources and journalists. Whistleblowers must not be punished for using a computer to blow the whistle. Laws criminalizing access to information must conform to principles of legal certainty and proportionality.

156 Criminal Code Act 476.2, Criminal Code Act 1995 ("Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.").

157 In *R v. Bow Street Metropolitan Stipendiary Magistrate* the House of Lords held that misuse of authorised access for an ulterior purpose would not fall within the scope of prohibitions against unauthorised access. secure access to data "of the kind in question" R v Bow Street Metropolitan Stipendiary Magistrate and another, ex parte Goverment of the United States of America 1999; noted JC Smith, "Case & Comment" [1999] Crim LR 970.

158 MCCOC Report, p. 106 n. 166.

159 Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, adopted in A/RES/65/230 (2010).