Inter-American Commission on Human Rights
Organization of American States

Thematic Hearing on
Freedom of Expression and Communications Surveillance by the United States

Written Submission of
Emi MacLean
Open Society Justice Initiative

October 28, 2013

I. INTRODUCTION

1. Unauthorized disclosures in recent months have unearthed massive, and previously little-known, U.S. state surveillance programs. These disclosures were made by a U.S. government contractor and consisted largely of classified documents from the National Security Agency.[1] The government has acknowledged the widespread public interest in the surveillance programs disclosed; and the initial leaks led to subsequent official disclosures. They have also raised serious concerns, in the United States and around the world, about the consistency of U.S. surveillance practices with domestic and international law, and the impact of widespread surveillance on individual privacy and freedom of expression. Other recent unauthorized public disclosures of U.S. government information related to national security have revealed human rights violations,[2] fraud and waste,[3] and other information of public interest.[4]

2. The public servants who have made unauthorized disclosures have increasingly faced the imposition, or threat, of severe sanctions for their actions. In recent years, the U.S. government has pursued an unprecedented number of leak investigations and prosecutions. At the time of this submission, the U.S. government has pursued eight leak prosecutions under the 1917 U.S. Espionage Act since President Barack Obama took office in 2009, as compared to three people charged under the Act for such unauthorized disclosures in all prior years since World War II.[5] Further, those who have received, or were suspected of receiving,

---

[1] Scott Shane, *Ex-contractor is charged in leaks on N.S.A. surveillance*, N.Y. Times, June 21, 2013, at http://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html.

[2] Julie Tate, *Judge sentences Bradley Manning to 35 years*, Washington Post, August 21, 2013, at http://articles.washingtonpost.com/2013-08-21/world/41431547_1_bradley-manning-david-coombs-pretrial-confinement. Not all, but certainly some, of Manning's disclosures qualify as related to human rights violations.

[3] *See* Jane Mayer, *The Secret Sharer*, THE NEW YORKER, May 23, 2011, at http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.

[4] Scott Shane, *U.S. Analyst Is Indicted in Leak Case,* N.Y. Times, August 27, 2010, at http://www.nytimes.com/2010/08/28/world/americas/28leak.html.

[5] Charlie Savage, *Court Rejects Appeal Bid by Writer in Leak Case*, N.Y. TIMES, October 15, 2013, at http://www.nytimes.com/2013/10/16/us/court-rejects-appeal-bid-by-writer-in-leak-case.html.

unauthorized disclosures – including journalists – have in some instances been subject to targeted surveillance and threatened with prosecution themselves, ordered to disclose their sources, or penalized for the refusal to do so. While no journalist has thus far been prosecuted under the Espionage Act, the aggressive enforcement of unauthorized disclosures in recent years suggests that may be a threat.[6]

3. The severe, and increasingly frequent, sanctions in the United States for public servants in the security sector who disclose information in the public interest raises concerns about U.S. compliance with its international law obligations to protect freedom of expression and the public right of access to information. While national security may justify legitimate restrictions on the public's right to access information when certain conditions are met, restrictions must be limited and well-grounded to comply with international law. They must also be clear and not arbitrary or overbroad. The threat of arrest or prosecution, even where there is no eventual arrest or prosecution, may chill protected expression, and constitute improper, unnecessary or disproportionate interference on freedom of expression.

4. The lack of adequate protection for members of the public, including journalists, who possess or disclose information related to national security raises related concerns. Members of the media and other public watchdogs must be permitted to both investigate and publish information of public interest, including in the security sector, without intimidation or improper surveillance, and also to protect their sources.

5. Public scrutiny of state activities, including in the security sector, safeguards against abuse by public officials and ensures democratic participation and oversight of policymaking in a sector where there is otherwise significant executive discretion and sometimes undue deference. A government's over-invocation of national security concerns, or the undue deference to national security assertions, can seriously undermine the main institutional safeguards against government abuse: independence of the courts, the rule of law, legislative oversight, media freedom, and open government.

6. On behalf of the Open Society Justice Initiative ("Justice Initiative"), I am honored to have the opportunity to participate in this thematic hearing concerning freedom of expression and communications surveillance by the United States. The Justice Initiative, an operational arm of the Open Society Foundations, has programs in 70 countries. The Justice Initiative uses law to protect and empower people around the world. Through litigation, advocacy, research and technical assistance, the Justice Initiative promotes human rights and builds legal capacity for open societies. The Justice Initiative expands freedom of information and expression, addresses abuses related to national security and counterterrorism, fosters accountability for international crimes, combats racial discrimination and statelessness, supports criminal justice reform, and stems corruption linked to the exploitation of natural resources.

7. I present this written submission in support of my oral testimony. This submission concerns: (1) the right of the public to information, and especially information of high public interest, including information related the security sector and state surveillance; (2) the obligation of the State to protect from sanctions those who possess or disclose information in the public interest, and to limit sanctions on unauthorized disclosures more generally; and (3) the lack of appropriate protection in the United States for public interest disclosures in the security sector.

---

[6] *See* Section III.B, below.

8. This submission is based in significant part on the Global Principles on National Security and the Right to Information (the "Tshwane Principles," named after the municipality in South Africa where the meeting to finalize the Principles was held), issued on 12 June 2013.[7] These Principles are based on international and national law, standards, good practices, and the writings of experts, and build off of the 1995 Johannesburg Principles on National Security, Freedom of Expression and Access to Information ("Johannesburg Principles").

9. **With this submission, and on behalf of the other drafters of the Principles, the Justice Initiative requests this Commission to endorse the Tshwane Principles**. This would be relevant to U.S. law and practice, but also to other countries in the region grappling with questions related to the appropriate limits of national security secrecy.[8]

10. The Tshwane Principles were elaborated by the Justice Initiative, along with 21 other organizations and academic centers,[9] in collaboration with the UN Special Rapporteurs on the protection and promotion of human rights while countering terrorism, and on the promotion and protection of the right to freedom of opinion and expression; and the three regional Special Rapporteurs on freedom of expression, information and/or the media of the Organisation of American States (OAS), the Organisation for Security and Co-operation in Europe (OSCE), and the African Commission on Human and Peoples' Rights (ACHPR). The Tshwane Principles have been endorsed by the Parliamentary Assembly of the Council of Europe (PACE); as well as the above-mentioned special mandate-holders.[10] We are currently engaged with the Special Rapporteur of the African Commission on Human and Peoples' Rights to seek endorsement of the Principles within the African system as well.

---

[7] Global Principles on National Security and the Right to Information (the "Tshwane Principles"), 2013, at http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

[8] This is relevant to other countries in the region seeking, e.g., clear standards or procedures for classifying or otherwise withholding information on security grounds; encouraging the proactive disclosure of information of high public interest; protecting whistleblowers; and punishing – and also limiting the punishment for – unauthorized disclosures. The parts of the Principles that are most relevant to whistleblower protections are Part VI on "Public Interest Disclosures by Public Personnel" and Part VII on "Limits on Measures to Sanction or Restrain the Disclosure of Information to the Public." The principle most relevant to surveillance is Principle 10 on "Categories of Information with a High Presumption or Overriding Interest in Favor of Disclosure," including 10E on Surveillance. If the Commission is not inclined to endorse the whole of the Tshwane Principles, then we invite the Commission to endorse at least these sections.

[9] In addition to the Justice Initiative, the following organizations contributed substantially to the drafting of the Tshwane Principles: Africa Freedom of Information Centre; African Policing Civilian Oversight Forum; Alianza Regional por la Libre Expresión e Información; Amnesty International; Article 19, the Global Campaign for Free Expression; Asian Forum for Human Rights and Development; Center for National Security Studies; Central European University; Centre for Applied Legal Studies University; Centre for European Constitutionalization and Security (CECS), University of Copenhagen; Centre for Human Rights, University of Pretoria; Centre for Law and Democracy; Centre for Peace and Development Initiatives; Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law; Commonwealth Human Rights Initiative; Egyptian Initiative for Personal Rights; Institute for Defense, Security and Peace Studies; Institute for Security Studies; International Commission of Jurists; National Security Archive; Open Democracy Advice Centre.

[10] PACE, Recommendation 2024(2013), para. 1.3, adopted October 2, 2013. PACE, Resolution 1954 (2013), adopted October 2, 2013, paras. 7-9. Open Society Justice Initiative, Press Release: New Principles Address the Balance between National Security and the Public's Right to Know, June 12, 2013, at http://www.opensocietyfoundations.org/press-releases/new-principles-address-balance-between-national-security-and-publics-right-know.

II. THE RIGHT OF THE PUBLIC TO INFORMATION AND THE LIMITED RESTRICTIONS ON THE RIGHT TO EXPRESSION

11. This section outlines the international legal standards that inform an analysis of sanctions and protections for unauthorized disclosures of information in the public interest. *First*, it presents the broad consensus as to the content of the right to information, which includes at its core the principle of maximum disclosure. *Second*, it elaborates the requirement that any restrictions to the right to expression, including the right to information, be limited, and consequently necessary and proportionate. *Third*, it applies these standards in the national security context, and concerning information related to government surveillance. *Finally*, it establishes that the right of the public to access information requires states to limit penalties for the unauthorized receipt, possession or disclosure of information.

A. Content of the Right to Information

12. The right of access to information is fundamental and applies to all state institutions and officials, including security sector institutions, employees of these institutions, and the information they hold, including when related to national security.[11]

13. The right to access information derives in part from the fact that the state holds public information a properly informed citizenry requires. That body of information is produced, collected and processed using public resources, and it ultimately belongs to the public. The right of access to information is fundamental on its own, but has also been recognized as a precondition for the exercise of the basic rights of political participation and representation.[12]

14. Jurisprudence of the Inter-American Court, as well as decisions of the Inter-American Commission and declarations and reports of the OAS Special Rapporteur for Freedom of Expression, support a regional consensus on the content of the right of access to information.[13]

15. The right has at its core the principle of maximum disclosure—the presumption that all government-held information (and privately held information related to the performance of government functions or the use of public funds) should be subject to disclosure *unless* there is an overriding public or private interest justifying non-disclosure. Disclosure is the rule, withholding the exception, and any doubts must be resolved in favor of disclosure.[14]

---

[11] American Convention on Human Rights, Article 13. International Covenant on Civil and Political Rights ("ICCPR"), Article 19. UN Human Rights Committee, General Comment No. 34 on Article 19, UN Doc. CCPR/C/GC/34, September 12, 2011 ("General Comment No. 34").

[12] *Claude Reyes v. Chile*, IACtHR, September 9, 2006, para. 86 ("access to information held by the State may permit participation in public governance by virtue of the social oversight role that can be exercised through such access").

[13] *Ibid.*, para. 78. Office of the Special Rapporteur for Freedom of Expression, I/A Comm. H.R., Inter-American Legal Framework Regarding the Right to Access to Information (2010) (summary of the state of the right in the region drawing on the decisions of the Inter-American Court and the Inter-American Commission, and other regional authorities). Organization of American States, Inter-American Model Law on Access to Public Information of 2010 ("Inter-American Model RTI Law"), adopted at fourth plenary session, 8 June 2010, by OAS General Assembly Resolution 2607 (XL-O/10). Commentary to the Inter-American Model Law.

[14] *Claude Reyes v. Chile*, note 12 above, para. 92.

16. The scope of entities and type of information covered by a right to information regime should be broad. The scope should include all public bodies "and organizations which operate with public funds or which perform public functions."[15]

17. The right of access to information mandates a corresponding duty of public authorities to disclose information.[16] The burden of proof to justify any withholding rests with the public authority. In addition to the right to request information, and the duty incumbent on the public authority to respond to such requests, there has also been a growing recognition of the importance of proactive disclosure.[17] Many democratic countries, in the Americas and beyond, require public authorities to proactively collect, generate and publish information on a number of issues that are considered important to democratic accountability.[18]

B. Legitimate Restrictions on Freedom of Expression

18. The right to freedom of expression, including access to information, is not absolute. However, restrictions on the right must be narrowly drawn exceptions necessary to protect legitimate interests, and strictly interpreted in line with the presumption of access.[19] Under Article 13 of the American Convention and the jurisprudence of the Inter-American Court, limitations on the right to information must comply with a three-part test:

19. *First*, there must be a clear and precise legal foundation for the limitation.[20] The principle of legality ensures a reasonable expectation of the interpretation of the law, and that the limitation is not a result of discretionary state action.[21] The requirement that a restriction be prescribed by law refers to both the existence and quality of the law, which must prevent arbitrary interference with the right to information.[22]

20. This Commission expressly found that a criminal law that permitted punishment for statements that "in any way damage or compromise the economic stability of the nation" or "harm the national defense" was impermissibly vague and overbroad.[23] The UN Sub-Commission Special Rapporteurs on Freedom of Expression similarly condemned restrictions that are "so broad in scope or drafted in such terms as to put the right itself in jeopardy. … [L]imitations which would otherwise be permissible under article 19, paragraph 3 (for instance

---

[15] *See, e.g.*, Inter-American Juridical Committee, Principles on the Right of Access to Information, adopted August 7, 2008 at the 73rd Regular Session (Rio de Janeiro), Principle 2. Inter-American Model RTI Law, note 13 above, Art. 3.

[16] *See Claude Reyes v. Chile*, note 12 above, para. 120.

[17] *See* 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, December 6, 2004 ("2004 Joint Special Rapporteurs Declaration").

[18] *See generally* Helen Darbishire, *Proactive transparency: the future of the right to information?* (World Bank Institute Governance Working Paper Series), 2010. Inter-American Model RTI Law, note 13 above, Art. 12.

[19] *Claude Reyes v. Chile*, note 12 above, para. 92. General Comment No. 34, note 11 above, para. 11.

[20] *Ibid.,* at para. 89,

[21] *Ibid.,* at paras. 89, 98.

[22] General Comment No. 34, note 11 above, para. 25.

[23] *Report on the Situation of Human Rights in Nicaragua*, IACommHR, O.A.S. Doc. OEA/Ser.L/V/II.53, doc.25 (1981), at 118, para. 6.

laws relating to official secrecy) may be defined too vaguely or too broadly and thus jeopardize the right to freedom of expression."[24]

21. The UN Rapporteurs noted that the requirement of precision is particularly important regarding laws that provide for sanctions, and especially regarding the element of intent:

> [T]he laws should rule out any possibility of a presumption of bad faith . . . . If sanctions are based on laws that are vague or manifestly imprecise or formulated with clear intent to provide a "legal" basis for silencing people, they come close to "informal" or arbitrary sanctions.[25]

22. *Second*, the limitation on the right to information must respond to a legitimate purpose recognized by Article 13 of the American Convention. The only legitimate purposes recognized by Article 13(2) of the American Convention are "respect for the rights or reputations of others," and "the protection of national security, public order, or public health or morals."[26]

23. *Third*, the limitation must be necessary in a democratic society to satisfy a compelling public interest[27] and proportionate to the interest that justifies it.[28]

24. In terms of the third part of this test, for a limitation to be necessary it must be the least restrictive means for achieving the legitimate aim.[29] Limitations "must be subjected to an interpretation that is strictly limited to the 'just demands' of 'a democratic society,' which takes account of the need to balance the competing interests involved and the need to preserve the object and purpose of the Convention."[30]

25. For a restriction on freedom of information to be proportionate: (i) the restriction must be related to a legitimate aim; (ii) the public authority must demonstrate that disclosure of the information threatens substantial harm to the aim;[31] and (iii) the public authority must demonstrate that the harm to the legitimate interest is greater than the public interest impeded.[32] The principle of proportionality must be "respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law."[33]

---

[24] Danilo Türk & Louis Joinet, in *The Right to Freedom of Opinion and Expression: Final Report by Mr. Danilo Türk and Mr. Louis Joinet, Special Rapporteurs*, UN Commission on Human Rights, UN Doc. E/CN.4/Sub.2/1992/9 (July 14, 1992), at para. 29.

[25] *Ibid.*, paras. 72, 74.

[26] *Claude Reyes v. Chile,* note 12 above, at para. 90. *See* ICCPR, Arts. 19, 21. General Comment No. 34, note 11 above, para. 22.

[27] *Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism*, IACtHR, Advisory Opinion OC-5/85, November 13, 1985, paras. 39, 46 (proving the "necessity" of restrictions requires a showing of "compelling governmental interest … that clearly outweigh[s] the social need for the full enjoyment" of Article 13 rights).

[27] *Ibid.*, para. 39.

[28] *Claude Reyes v. Chile*, note 12 above, paras. 89-91. *See also* Office of the Special Rapporteur for Freedom of Expression, Annual Report of the Inter-American Commission on Human Rights, 2011 ("OAS Special Rapporteur 2011 Report"), Ch. III, paras. 342-43, 347.

[29] *See Claude Reyes v. Chile*, note 12 above, para. 91.

[30] *Compulsory Membership Opinion*, note 27 above, para. 67.

[31] *See* Commentary to Inter-American Model RTI Law, note 13 above, at 10.

[32] Inter-American Legal Framework Regarding the Right to Access to Information, note 13 above, p. 53.

[33] General Comment No. 34, note 11 above, para. 34, *quoting* General comment No. 27, para. 14.

26. There is an evolving trend in national laws to consider the harm that disclosure would cause to the protected interest in adjudging whether a classification is legitimate. Various countries in the region, including Guatemala and Nicaragua, have a harm test incorporated into their laws governing classification or withholding of information, thereby limiting the justification for the non-disclosure of information to where the "damage or harm that could occur with the release of the information is greater than the public interest in knowing the information."[34]

27. A public authority must also weigh the harm that disclosure would cause to the protected interest against the public interest served by disclosure of the information.[35]

28. The public's interest in disclosure is heightened where the information concerns wrongdoing, "including [by] members of the secret services."[36] Further, the right of the public to information is inviolable where it concerns gross human rights violations or serious violations of international humanitarian law.[37] This follows from the Inter-American Court's recognition of an autonomous right to truth under the American Convention.[38] The Inter-American Model Law,[39] and laws of various countries in the region,[40] have recognized that exceptions to disclosure do not apply in the case of information related to human rights violations or crimes against humanity. The withholding of this information cannot be "necessary in a democratic society" as there is no benefit from the cover-up of human rights abuses.[41]

29. However, the public interest in disclosure extends beyond simply where there is demonstrated wrongdoing. The European Court of Human Rights, for its part, has recognized "little scope … for restrictions on debate on questions of public interest," reasoning that "the acts or omissions of government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the media and public opinion."[42]

---

[34] Law on Access to Public Information (Guatemala), Decree No. 57/2008, Art. 26. Law on Access to Public Information, Law 621 of 2007 (Nicaragua), Art. 3(7).

[35] The existence of a public interest test in an access to information law is generally considered a sign of the strength of the right. Nearly half of the laws surveyed in a recent comparative analysis included a public interest test. Maeve McDonagh, *The public interest test in FOI legislation*, at 6 (44 of 93 countries).

[36] *See, e.g.*, PACE, Resolution 1838 (2011) on the abuse of state secrecy and national security, adopted October 6, 2011, para. 8.

[37] Office of the High Commissioner for Human Rights (OHCHR), *Study on the Right to the Truth*, February 8, 2006, para. 59. *Updated Set of Principles for the Protection and Promotion of Human Rights Through Action to Combat Impunity*, Resolution 2005/81, UN Doc. E/CN.4/2005/102/Add.l, February 8, 2005 ("UN Impunity Principles"), Principles 2, 16.("[e]very people has the inalienable right to know the truth about past events concerning the perpetration of heinous crimes and about the circumstances that led, through massive or systematic violations, to the perpetration of those crimes").

[38] *See, e.g.*, *Gomes Lund v. Brazil*, IACtHR, November 24, 2010, paras. 200-01. *Gelman v. Uruguay*, IACtHR, February 24, 2011, paras. 118, 192, 243.

[39] Inter-American Model RTI Law, note 13 above, Art. 44 (exceptions to the right of access provided for in the law "do not apply in cases of serious violations of human rights or crimes against humanity").

[40] Transparency and Access to Public Information Act No. 27806 of 2002 (Peru), Art. 15. Federal Law on Transparency and Access to Public Information of 2002 (Mexico), Art. 14. Law on Access to Public Information, adopted by Congressional Decree 57-2008 of 2008 (Guatemala), Art. 24. Law on Access to Public Information, Law No. 12.527 of 2011 (Brazil), Art. 21. Right of Access to Public Information Act No. 18.381 of 2008 (Uruguay), Art. 12.

[41] *Gomes Lund v. Brazil*, note 38 above, para. 200. *See also El-Masri v. Macedonia*, ECtHR (Grand Chamber), December 13, 2012, paras. 191-94 (condemning the invocation of "State secrets" to "obstruct the search for the truth").

[42] *Guja v. Moldova*, ECtHR (GC), February 12, 2008, paras. 72, 74. *See also Palamara-Iribarne v. Chile*, IACtHR, November 22, 2005, para. 88.

30. Further, non-disclosure must be time- and context-limited, as any legitimate justifications for the non-disclosure of records become progressively weaker over time.[43] Excessively long periods of withholding information undermine the very essence of the Article 13 right of access to information.[44] Moreover, information originating in the security services of a prior authoritarian regime should be subject to presumptive disclosure obligations as the non-disclosure of information over a lengthy period is particularly unjustifiable for records related to violations of human rights implicating the security sector of prior authoritarian regimes.[45]

C. Access to Information and National Security

31. The right of access to information, and the underlying justifications for the right, apply to guarantee public access to information held by security sector institutions and information related to national security.[46] Although the state may impose restrictions on the right to expression and information on the ground of national security in certain circumstances, any national security restriction must comply with the above principles, and national security must not be a "pretext" for unjust restrictions.[47] Information related to national security, including where classified, is not exempt from public access for that reason alone; decisions to classify must be justified and limited.[48]

32. As elaborated in the Global Principles on National Security and the Right to Information (or "Tshwane Principles"), referenced above (see paras. 8-10), the right of access to state information, "including information that relates to national security," is necessary for the public to "monitor the conduct of their government and to participate fully in a democratic society."[49]

33. Tshwane Principle 3 provides that: "No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts."

---

[43] *See also Turek v. Slovakia*, ECtHR, February 14, 2006, para. 115 (rejecting an assumption "that there remains a continuing and actual public interest in imposing limitations on access to materials classified as confidential under former regimes").

[44] In the region, Chile, Colombia, Guatemala, Nicaragua and Panama provide for a maximum period of classification. OAS Special Rapporteur 2011 Report, note 28 above, Ch. III, para. 357. Inter-American Model Law, note 13 above, Art. 4, provides that most categories of reserved or classified information should be made public after a period of 12 years; for the most sensitive records, the initial classification could be extended by another 12 years, subject to the approval of an independent information authority.

[45] *See Myrna Mack v. Guatemala*, IACtHR, November 25, 2003, para. 180. *See also Turek v. Slovakia*, note 43 above, para. 115.

[46] General Comment No. 34, note 11 above, paras. 7, 18.

[47] *See, e.g.*, PACE, Resolution 1551 (2007), Resolution on espionage and divulging State secrets, April 19, 2007, paras. 1, 9 ("the State's legitimate interest in protecting official secrets must not become a pretext to unduly restrict the freedom of expression and of information").

[48] *Gomes Lund v. Brazil*, note 38 above. *Toktakunov v. Kyrgyzstan*, UN Human Rights Committee, Decision of March 28, 2011, UN Doc. CCPR/C/101/D/1470/2006, paras. 7.7-7.8 (finding a violation of Article 19 of the ICCPR where the State party classified and withheld on national security grounds death penalty statistics, given the public's "legitimate interest in having access to information on the use of the death penalty"). General Comment No. 34, note 11 above, para. 30.

[49] Tshwane Principles, notes 7 & 10 above, Preamble.

34. The Tshwane Principles acknowledge that governments may legitimately withhold information in narrowly defined areas, such as defense plans, weapons development, and the operations and sources used by intelligence services.[50] However, in each instance, the government bears the burden of proof to demonstrate the necessity of restrictions on the right to public information, including a duty on the public authority to "provide specific, substantive reasons to support its assertions" that there is a "risk of harm" from disclosure of identifiable information.[51]

35. The Principles specifically identify categories of information for which the government should have a presumptive, or overriding, obligation of disclosure because of the high public interest in the information. The public should have a right to know about the existence of all security sector entities, the laws and regulations that govern them, and their budgets, as well as information concerning violations of international human rights and humanitarian law. [52]

36. Relevant to a review of U.S. mass surveillance practices conducted in secrecy, Principle 10E identifies information concerning government surveillance for which there should be a "very strong presumption" of public and proactive disclosure:

    (1) "the overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material;"[53]
    (2) "information about entities authorized to conduct surveillance, and statistics about the use of such surveillance;"[54] and
    (3) "the fact of any illegal surveillance."

37. The importance of public access to government information concerning the security sector is notably important because of the discretion typically afforded the Executive in this area; the state's great powers, including to wage war and counterterrorism operations, conduct surveillance, detain and interrogate persons; and its oversight of significant public funds. Undue deference to arguments concerning national security secrecy can contribute to human rights violations, corruption, waste and abuses, with accountability hampered by secrecy.[55]

---

[50] *Ibid.*, Principle 9.

[51] *Ibid.*, Principle 4.

[52] *Ibid.*, Principles 10A, 10C, 10F.

[53] "Note [to Prnciple 10E(1)]: This information includes: (a) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining, and the types of surveillance measures that may be used; (b) the permissible objectives of surveillance; (c) the threshold of suspicion required to initiate or continue surveillance; (d) limitations on the duration of surveillance measures; (e) procedures for authorizing and reviewing the use of such measures; (f) the types of personal data that may be collected and/or processed for national security purposes; and (g) the criteria that apply to the use, retention, deletion, and transfer of these data."

[54] "Notes [to Principle 10E(2): This information includes the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity.

The right of the public to be informed does not necessarily extend to the fact, or operational details, of surveillance conducted pursuant to law and consistent with human rights obligations. Such information may be withheld from the public and those subject to surveillance at least until the period of surveillance has been concluded."

[55] *N.Y. Times v. United States* ("The Pentagon Papers Case"), 403 U.S. 713, U.S. Supreme Court, 1971 (Stewart, J., concurring) ("In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie

D. Limitations on Penalties for Disclosure of National Security Information and Related Acts

38. The right to freedom of expression requires that sanctions on the unauthorized possession or disclosure in the public interest of government information, including information that is classified or concerns national security, must be limited, necessary and strictly proportionate. In this section, I submit that where the public interest in disclosure of information outweighs the harm from disclosure, disclosure by public servants should not be subject to penalties. Further, disclosure of such information by the media or other members of the public should not be punished.

1. Public Interest Disclosures by Public Servants Should Not Be Criminalized and Whistleblower Protections Should be Available

39. Not all disclosures by public servants are protected. However, a public servant has a right, and in some cases a duty, to disclose otherwise confidential government information where in the public interest. Increasingly, international and national law and practice recognize the restrictions on punishment of disclosure of such information.[56]

40. Freedom of expression extends to the workplace, including for those who work in the security sector.[57] Freedom of expression, including the right to seek, receive and impart national security information held by public authorities, requires that measures to sanction or restrain the disclosure of information to the public be limited. A government employer can expect a public servant to protect confidential information from disclosure, and indeed, it is often in the public interest to keep such information confidential.[58] Yet the duties of "loyalty, reserve and discretion" which restrain the public servant from disclosing certain confidential information are not absolute.[59] Restrictions on the right of public servants to communicate information must comply with the three-part test governing all restrictions on the right to information (see Section II.B, above).

41. Increasingly, international law provides for protections for public servants who release information showing wrongdoing, or otherwise in the public interest, despite general or specific employee duties of loyalty and confidentiality. In addition to the disclosure of wrongdoing, sanctions should be limited where the information would, for example, contribute to important public debate about government policy, heighten accountability, allow oversight of government expenditures, or protect the public health. Moreover, the unauthorized possession or disclosure of improperly classified information should not be

---

in an enlightened citizenry – in an informed and critical public opinion which alone can here protect the values of democratic government."). *See* PACE, Resolution 1507 (2006), Alleged secret detentions and unlawful inter-state transfers of detainees involving Council of Europe member states, para. 19.5. *Stoll v. Switzerland*, ECtHR (GC), December 10, 2007, para. 110 ("[p]ress freedom assumes even greater importance in circumstances in which State activities and decisions escape democratic or judicial scrutiny on account of their confidential or secret nature").

[56] General Comment No. 34, note 11 above, para. 30.

[57] *See, e.g.*, *Grigoriades v. Greece*, ECtHR (GC), November 25, 1997 ("Article 10 [freedom of expression rights] do not stop at the gates of the army barracks" and the enforcement of military discipline cannot be used "for the purpose of frustrating the expression of opinions, even if these are directed against the army as an institution"). *Palamara-Iribarne v. Chile*, note 42 above (finding a violation of freedom of expression in Chile's retaliation against a retired Chilean Navy officer for public statements and an attempted book publication concerning intelligence and ethics).

[58] *Guja v. Moldova*, note 42 above, paras. 70-71.

[59] *Ibid.*, at para. 72. *Grigoriades v. Greece*, note 57 above, para. 45. *Bucur v. Romania*, ECtHR, January 8, 2013, paras. 115, 120. *See also* General Comment No. 34, note 11 above, para. 30.

subject to sanction.[60] Public disclosures can serve as an important check on the "pervasive over-classification" of government-held information found in the State practice of various jurisdictions.[61]

42. The UN Human Rights Committee has stated authoritatively that it is not compatible with Article 19(3) of the ICCPR for a state to invoke state secrecy laws to "withhold from the public information of legitimate public interest that does not harm national security," and that public disclosure should be subject to punishment only "where the release of such information would be harmful to national security."[62]

43. The European Court of Human Rights has twice held in recent years that sanctions for disclosure of classified or otherwise sensitive information were unnecessary, and therefore violated the right to impart information, where the information was of public interest and efforts to seek remedies for the wrongdoing through official channels would have been ineffective.[63]

44. *Guja v. Moldova* concerned the dismissal of the head of the press department of the prosecutor general's office for sending to a newspaper copies of letters received from public officials applying undue influence on the prosecutor's office to drop criminal proceedings against some police officers. The Court's Grand Chamber, in finding a violation of the right to freedom of expression and information, noted that while "the duty of loyalty and reserve assumes special significance" for civil servants in a democratic society as "the public has a right to expect that they will help and not hinder the democratically elected government," these duties are not absolute[64]:

> [A] civil servant, in the course of his work, may become aware of in-house information, including secret information, whose divulgation or publication corresponds to a strong public interest…[T]he signaling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection. This may be called for where the employee or civil servant concerned is the

---

[60] *See* PACE, Resolution 1838 (2011) on abuse of state secrecy and national security, adopted October 6, 2011, para. 9. Dick Marty, Abuse of state secrecy and national security, Report of Rapporteur to the PACE, September 7, 2011, paras. 5, 45.

[61] Morton Halperin, *Criminal Penalties for Disclosing Classified Information to the Press in the United States*, 2012, at http://www.right2info.org/exceptions-to-access/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf, 1. Tshwane Principles, notes 7 & 10 above, Principle 47, Note. *See* Testimony of Thomas Blanton, National Security Archive, before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, U.S. House of Representatives, March 2, 2005, at http://www.gwu.edu/~nsarchiv/news/20050302/index.htm. *See* Testimony of Michael Hayden, former C.I.A. Director before Senate Select Committee on Intelligence, July 2013, in Shane, *Ex-Officer Is First from C.I.A. to Face Prison for a Leak*, N.Y. Times, January 5, 2013, at http://www.nytimes.com/2013/01/06/us/former-cia-officer-is-the-first-to-face-prison-for-a-classified-leak.html?pagewanted=1&smid=tw-nytimes&_r=0 ("So much of that is in the public domain that right now this witness, with my experience, I am unclear what of my personal knowledge of this activity I can or cannot discuss publicly. That's how muddled this has become.").

[62] General Comment No. 34, note 11 above, para. 30. *See also* Concluding observations on the Russian Federation (CCPR/CO/79/RUS), December 1, 2003, para. 22. UN Human Rights Committee, Concluding Observations on United Kingdom (CCPR/CO/73/UK), December 6, 2001, para. 21.

[63] *Guja v. Moldova*, note 42 above, para. 72. *Bucur v. Romania*, note 59 above. *See also Palamara-Iribarne v. Chile*, IACtHR, 22 November 2005, para. 88.

[64] *Guja v. Moldova*, note 42 above, para. 71.

only person, or part of a small category of persons, aware of what is happening at work and is thus best placed to act in the public interest by alerting the employer or the public at large.[65]

45. The Court, recognising "little scope … for restrictions on debate on questions of public interest," reasoned that "the acts or omissions of government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the media and public opinion."[66] Accordingly, the Court concluded that "the interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence."[67]

46. *Bucur v. Romania* concerned the disclosure by a telecommunications analyst in one of Romania's military intelligence units of "top secret" information about "irregular" surveillance. The European Court found that the general interest in the disclosure of information revealing irregular surveillance authorized by high-ranking officials was so important in a democratic society that it prevailed over the interest in maintaining public confidence in the intelligence agency.[68] The Court ruled that divulging the information directly to the public had been justifiable, and that the criminal prosecution and two-year prison sentence violated the public servant's right to communicate information.[69]

47. The European Court, in both of the above summarised cases, considered several factors in its analysis of whether the public interest in disclosure outweighed the harm: the availability of any effective, alternative remedies; the public interest in the information; the actual harm caused by the disclosure weighed against the public interest in the information's release; the reasonableness of the public official's belief in the accuracy and importance of the information; and the severity of the penalty.[70]

48. Several states recognize a limitation on the prosecution of unauthorized disclosure of classified information in the public interest similar to that identified by the European Court in *Guja* and *Bucur*. The Canadian Security of Information Act, for instance, makes it an offence to improperly communicate special operational information,[71] but provides a public interest defense where a public servant discloses illegal activity, considering virtually the same factors as does the European Court.[72] Danish criminal law provides a public interest defense for publication of state secrets where the person is acting in "the legitimate exercise of obvious public interest,"[73] which has been interpreted to require that this interest shall exceed the interest in keeping the information secret.[74] A Danish criminal court, applying the public

---

[65] *Ibid.*, para. 72..

[66] *Ibid.*, para. 74.

[67] *Ibid.*

[68] *Bucur v. Romania*, note 59 above, paras. 115, 120.

[69] *Ibid.*, para. 120.

[70] *Guja v. Moldova*, note 42 above, para. 73-77. *Bucur v. Romania*, note 59 above, paras. 95-119.

[71] Security of Information Act (Canada) (R.S.C., 1985, ch. O-5), Arts. 13, 14.

[72] *Ibid.*, Art. 15 (defining public interest defense considering available alternative remedies; the seriousness of the wrongful governmental activity disclosed, and the public interest served in its disclosure; the harm caused by the disclosure; the reasonableness of the public servant's belief that information was in the public interest; the extent of disclosure; and any exigent circumstances justifying disclosure).

[73] Criminal Code (Denmark), Section 152(e) (2010).

[74] Amanda Jacobsen, *National Security and the Right to Information in Europe*, 2013, at http://www.right2info.org/resources/publications/national-security-page/national-security-expert-

interest defense in 2006, considered as factors the national security interest, the degree of actual harm to the interest, and the significance of the public interest in knowing the information and facilitating debate on the issues raised.[75]

49. In other countries, related arguments may be raised in defense of unauthorized disclosures. In the Netherlands and the United Kingdom, although the criminal law itself does not mention a public interest defense, the European Convention on Human Rights, and judgments of the European Court, are directly applicable by the courts, and accordingly *Guja* and *Bucur* may be invoked. The laws of some countries include provisions prohibiting the classification of information concerning corruption, crimes or human rights violations; or either permitting or requiring that such information be disclosed to authorities.[76]

50. In various countries – including 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. Additional countries allow the lack of harm to be raised as a defense or mitigating circumstance.[77]

51. Various countries have mechanisms that allow for internal disclosures, but these are often found wanting. Increasingly, international instruments also recognize, as the European Court did in *Guja* and *Bucur*, that a public servant need not first use official channels before disclosing publicly if the attempted use of any such channels would likely be ineffective. For instance, the Parliamentary Assembly of the Council of Europe has asserted that there should be protections from penalty for public disclosures "where internal channels either do not exist, have not functioned properly or could reasonably be expected not to function properly given the nature of the problem raised by the whistleblower."[78]

52. The Tshwane Principles recommend protection against any form of sanction or penalty for the disclosure of wrongdoing.[79] Whistleblower protections against any form of retaliation, including prosecution, should be available in such instances. Even in the absence of wrongdoing, the Tshwane Principles delineate a public interest defense, similar to the analysis found in the European Court jurisprudence, if the public interest in the disclosure of the information outweighs the harm in its disclosure. There should be a consideration of the resulting harm, whether the person had reasonable grounds to believe that the disclosure would be in the public interest, the use of internal or independent oversight mechanisms prior to public disclosure where existent and effective, and any "exigent circumstances."[80]

---

papers/jacobsen_nat-sec-and-rti-in-europe (survey of the University of Copenhagen, in collaboration with the Open Society Justice Initiative) ("Jacobsen, *National Security and the Right to Information in Europe*"), 48-49.

[75] *Denmark v. Larsen*, Copenhagen City Court, Case No. SS 24.13764/2006, December 4, 2006.

[76] *Ibid.*

[77] This is true in at least Denmark, France and Hungary.

[78] PACE, Resolution 1729, adopted April 29, 2010, Arts. 6.1.2, 6.2.3. 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. Jacobsen, *National Security and the Right to Information in Europe*, note 74 above, p. 49. *See also* Whistleblower protection: a comprehensive scheme for the Commonwealth public sector, 7.119 (recommending that public disclosure be protected from retaliation "where an agency has failed to meet its obligations … or where the whistleblower considers on reasonable grounds, that the matter has not been handled appropriately by the agency").

[79] Tshwane Principles, notes 7 & 10 above, Principles 39-41, 43.

[80] *Ibid.*, Principle 43.

53. Consistent with international law and good practice outlined above, the Tshwane Principles assert that criminal penalties should only be available, if at all, if the information disclosed poses a "real and identifiable risk of causing significant harm" that overrides the public interest in disclosure, and if the law clearly sets forth "narrow categories of information" whose disclosure poses a high likelihood of causing harm.[81]

2. Public Interest Disclosures by the Media and Other Members of the Public Should Not Be Punished

54. The primary, or exclusive, responsibility to protect the confidentiality of government information, when confidentiality is justified, lies with the State. Public servants are subject to reasonable and qualified obligations of confidentiality to which members of the public are not. Among the members of the public, journalists and other similarly protected persons with a special responsibility to act as public watchdogs, can only be sanctioned for disclosing government information in extraordinary circumstances. We submit that those circumstances are limited to when they have committed a crime not predicated upon the possession or disclosure of the information, or have a specific intent to cause serious harm to a legitimate public interest.

55. The duties of loyalty and confidentiality do not apply to members of the public; they arise from statutes, employment contracts and/or common law, and apply only to public servants or those who are contractually bound.

56. This is particularly true with regard to journalists or public watchdogs. Indeed, the duties of loyalty and confidentiality are in direct conflict with the duties that define journalistic professional ethics—the ethical dissemination of information rather than its withholding.[82] Thus, the UN Human Rights Committee has declared unambiguously that the prosecution of "journalists, human rights defenders and others … for having disseminated … information of legitimate public interest that does not harm national security" violates Article 19(3) of the ICCPR.[83] Further, journalists and others similarly protected must be permitted to retain information without fear of sanction, even if the information is not subsequently deemed by the journalist or public watchdog to be in the public interest or disclosed.[84]

57. Thus, to comply with Article 13, general laws which sanction unauthorized possession or disclosure must have adequate safeguards to protect freedom of expression. Otherwise, such laws are liable to be abused. Laws which target journalists in the language of their provisions, or in practice, raise heightened concerns about violations of freedom of expression.[85]

---

[81] *Ibid.*, Principles 3, 43, 46

[82] *See, e.g.*, Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, December 7-8, 1994), Principles 3, 6-8.

[83] General Comment No. 34, note 11 above, para. 30. *See also* UN Human Rights Committee, Concluding observations on the Russian Federation (CCPR/CO/79/RUS), December 1, 2003, para. 22; & Concluding observations on Hong Kong (CCPR/C/HKG/CO/2), April 21, 2006, para. 14.

[84] International Federation of Journalists, Status of journalists and journalism ethics: IFJ Principles, May 5, 2003, Principle 1.7 ("the law should not interfere in matters which are the proper responsibility of working journalists: namely, the preparation, selection and transmission of information").

[85] *See, e.g.*, *O'Neill v. Canada (Att'y Gen.)*, Ontario Sup. Ct. J., 82 O.R. 3d 241, 2006, para. 163. Canada's largest superior trial court, serving 13 million people, struck down a portion of the offenses section of Canada's Security of Information Act as overbroad and unnecessary after Canadian security forces raided the home and office of a journalist who had, relying on unauthorized disclosures, published a story about a Canadian citizen subjected to extraordinary rendition. The

58. In part due to the public interest in receiving information from anonymous sources, there must be a strong presumption of source protection and, relatedly, a similarly strong presumption against the sanction of journalists for receipt or disclosure of government information.[86] Even where unrelated to source disclosure, the imposition or threat of sanctions on journalists for disclosure of information in the public interest will generally fall afoul of the protections required pursuant to Article 13. Sanctions or the threat of sanctions against members of the media for disclosing information may chill others from releasing information in the public interest, effectively thereby undermining their vital role and function.[87]

59. The UN Special Rapporteur on the right to freedom of opinion and expression, in a statement joined by the UN Rapporteur on the protection and promotion of human rights while countering terrorism, expressed concern over the United Kingdom's short-term detention and interrogation of the partner of a journalist with travel sponsored by a media outlet:

> "Under no circumstances, journalists, members of the media, or civil society organizations who have access to classified information on an alleged violation of human rights should be subjected to intimidation and subsequent punishment … The protection of national security secrets must never be used as an excuse to intimidate the press into silence and backing off from its crucial work in the clarification of human rights violations."[88]

60. In 2004, the three international rapporteurs on freedom of expression (for the UN, OAS, and OSCE) issued a Joint Declaration on Access to Information and Security Legislation.[89] They "stress[ed] the need for informational 'safety valves' such as protection of whistleblowers and protection for the media and other actors who disclose information in the public interest":

> "Other individuals [who are not public authorities or their staff], including journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the information. Criminal law provisions that don't restrict liability for the dissemination of State secrets to those who are officially entitled to handle those secrets should be repealed or amended."

61. Similarly, the Special Rapporteurs on Freedom of Expression of the UN and the Inter-American Commission on Human Rights, commenting on WikiLeaks, recognized that public servants could be penalized for disclosing "legitimately classified information," but called on

---

security forces alleged in the search warrant that she had violated the law's provisions prohibiting the unauthorized receipt and retention of information. The Court stated that provisions criminalizing the receipt and communication of certain government information, in the absence of protections for journalists, "restrict[ed] the free flow of government information" and violated freedom of expression.

[86] Peter Omtzigt, Rapporteur, The protection of "whistle-blowers", Report for the Parliamentary Assembly of the Council of Europe Committee on Legal Affairs and Human Rights September 14, 2009, Doc. 12006, para. 33. *See Sanoma v. The Netherlands*, ECtHR (GC), September 14, 2010, at para. 50. *Tillack v. Belgium*, ECtHR, November 27, 2007, para. 65 (source protection not "mere privilege to be granted or taken away").

[87] *Stoll v. Switzerland*, ECtHR (GC), December 10, 2007, para. 110.

[88] Office of the High Commissioner for Human Rights, UK: "National security concerns must never justify intimidating journalists into silence," warn UN experts (Frank LaRue and Ben Emmerson), September 4, 2013.

[89] 2004 Joint Special Rapporteurs Declaration, note 17 above. *See also* Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression, December 20, 2006. Joint Statement of the UN Special Rapporteur on Freedom of Opinion and Expression & the OAS Special Rapporteur on Freedom of Expression, December 21, 2010, para. 3 ("2010 Joint Statement on Wikileaks").

states not to penalise the media and other members of the public for the disclosure constituted by sharing or publishing the information.[90]

62. There is an emerging consensus distinguishing the sanctions that can be applied to journalists, and in some cases other members of the public, compared with those available for public servants, for the public disclosure of information of public interest. States increasingly distinguish between the offenses or penalties available for the unauthorized disclosure of information by members of the public on the one hand, and public servants on the other.

63. If the unauthorized disclosure does not amount to treason or espionage, and is not in wartime, several countries – including Brazil, Chile, Colombia, Mexico, Moldova, the Russian Federation and Slovenia – limit criminal responsibility for unauthorized disclosures only to public servants.[91] Many other countries provide separate or heightened offences for public servants who disclose information to which private persons, including the media, are not subject.[92] Colombian law specifically establishes that journalists are not obliged to protect the confidentiality of government information when exercising their professional responsibilities.[93] In Germany, the criminal law was amended in 2012 to release journalists from the risk of being charged with aiding and abetting the "violation of official secrets" for disclosing classified information.[94] Irrespective of whether or not the sanctions contemplated on public servants are rights compliant under these laws, it is clear that these States have made a clear distinction between public servants and others making disclosures, including journalists and public watchdogs.

64. In the first ever Danish prosecution of journalists for the unauthorized publication of classified information, a criminal court in 2006 unanimously acquitted two journalists who had published information questioning the presence of weapons of mass destruction in Iraq. The court found that the public interest justified the disclosures, even though the courts had previously convicted the intelligence officer who provided the journalists with the information.[95]

65. There is also growing support in international and national law and practice disfavoring sanctions for unauthorized possession, including in the area of national security and especially for members of the public. For instance, the laws of Bolivia, Brazil, Chile, Colombia, Mexico,[96]

---

[90] 2010 Joint Statement on Wikileaks, note 89 above, para. 3.

[91] Criminal Code (Brazil), Decree Law No. 2.848, 1940, at http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm, Art. 154. Criminal Code (Chile), Law 20653 of 1984, at http://www.leychile.cl/Navegar?idNorma=1984, Art. 246. Criminal Code (Colombia), 2000, at http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html, Art. 418. Federal Criminal Code (Mexico), 1931 (as of June 7, 2013), at http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf, Art. 210. Criminal Code (Moldova), 2009, Art. 344. Criminal Code (Russian Federation), 1996 (as of June 29, 2013), Art. 283(1), (2). Criminal Code (Slovenia), 2008, (as of June 14, 2012), Arts. 260(1).

[92] *Some offences only for public servants*: Albania, Argentina, Belgium, Canada, Czech Republic, Denmark, France, Guatemala, Nigeria, Panama, Paraguay, Poland, Serbia, Sweden, Turkey, United Kingdom, United States, Uruguay. *Less severe penalties for private persons as compared to public servants*: Albania, Argentina, Belgium, Bolivia, Czech Republic, Denmark, Ecuador, France, Germany, Hungary, Norway, Panama, Paraguay, Romania, Serbia, Sweden.

[93] Law No. 1621 (Colombia), Art. 33(4).

[94] Criminal Code (Germany), Section 353(b)(3)(a).

[95] *Denmark v. Larsen*, Copenhagen City Court, Case No. SS 24.13764/2006, December 4, 2006. *See* Reporters without Borders, *Three Berlingske Tidende Journalists Acquitted of State Security Charges*, December 4, 2006.

[96] A limited offence exists for "knowing or copying information in State information systems protected by a security mechanism."

Moldova, Poland,[97] and Uruguay, do not provide any punishment for the unauthorized possession of such information, by members of the public *or* public servants, unless there is espionage, demonstration of intent to harm, or actual harm. Other states – including Germany, Paraguay, Serbia, and Slovenia – require that one who possesses classified information have an intent to disclose the information or that the possession resulted in actual harm in order to prosecute for unauthorized possession.[98] In the Czech Republic, possession by private persons is an offence only upon proof of intent to disclose, or if "substantial damage" results or the possession is for personal gain. Romanian law requires that the act is "likely to jeopardize state security."[99] U.S. law concerning possession and possession-related offences are inconsistent with this developing consensus.

66. Tshwane Principle 47, reflecting the above and other good law and practice, states that "[a] person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information." Nor may a person who is not a public servant "be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information" if intended for public disclosure.[100] Placing the onus on the State to keep confidential information secret strikes a proper balance between the needs of legitimate secrecy and the high public interest in robust watchdogs and the disclosure of certain information.

III. ANALYSIS OF U.S. LAW

67. This section provides (A) an analysis of U.S. law related to sanctions and protections for unauthorized disclosures of information related to national security; (B) an analysis of sanctions imposed on both public servants and private persons in connections with possession or disclosure of information to the media; and (C) an assessment of U.S. compliance with international human rights law in its law and policy related to whistleblowers and others who disclose information.

A. Relevant U.S. Law: The Espionage Act and Limited Whistleblower Protections

68. Relevant U.S. law governing sanctions for the unauthorized possession or disclosure of classified information, or information otherwise related to national security, is largely, but not exclusively, found in the 1917 U.S. Espionage Act. The Espionage Act was enacted in the World War I era to punish spies, who disclose protected information to a foreign enemy, but it has been used more broadly to punish disclosures to the public, or the unauthorized possession of information without any intent to disclose to a foreign enemy.[101] It provides for

---

[97] A limited offence exists for "use" of information.

[98] Criminal Code (Germany), 1998 (as of October 2, 2009), at http://www.gesetze-im-internet.de/stgb/BJNR001270871.html, Sec. 96. Criminal Code (Paraguay), Law 1970, 1997, at http://www.mre.gov.py/v1/Adjuntos/Privacidad/Ley1160.pdf, Art. 285(2). Criminal Code (Serbia), 2005 (as of 2009), at http://www.propisinet.me/PDF/Krivicni%20zakonik.pdf, Art. 389(1). Criminal Code (Slovenia), 2008, (as of 14 June 2012), at http://www.wipo.int/wipolex/en/details.jsp?id=6074, Art. 260(2).

[99] Criminal Code (Czech Republic), 2009 (as of 2012), at http://www.zakonycr.cz/seznamy/040-2009-sb-zakon-trestni-zakonik.html, Arts. 317(1), 317(2)(b).

[100] Tshwane Principles, notes 7 & 10 above, Principle 47.

[101] Espionage Act (United States), 18 U.S.C. Sec. 793-98, 1917, Arts. 106a, 92, 104, 134. Several other statutes restrict the unauthorized disclosure of classified information: 18 U.S.C. Sec. 641, 952, 1030, 1924, 50 U.S.C. Sec. 783; Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. Sec. 421-26. *See generally* Jennifer Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, Congressional Research Service, June 24, 2013, at http://www.fas.org/sgp/crs/secrecy/R41404.pdf.

ten years imprisonment for each count of unauthorized possession[102] or disclosure[103] of classified or national defense information, or for the conspiracy to do so.[104] The offense of possession requires that the person has "reason to believe" the information could be used "to the injury of the United States or to the advantage of any foreign nation." The offense of disclosure requires either the "willful" transfer of defense information,[105] or the "knowing[] and willful[]" communication "prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States" [106]

69. U.S. law includes certain (limited) provisions unique to public servants or those otherwise with authorized access to information.[107] However, most provisions sanctioning the unauthorized possession or disclosure of defense or security-related information are universally applicable.

70. A more traditional espionage provision is found in 18 U.S.C. Sec. 794(a), under which a person who transmitted national defense information to a foreign government, or conspired to do so, "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation," is punishable by any term of imprisonment, and up to the death penalty for severe cases.[108]

71. The United States has a whistleblower protection regime, but its availability is virtually non-existent for security sector personnel.[109] The federal Whistleblower Protection Act (WPA)

---

[102] 18 U.S.C. Sec. 793(e), (f). *See also* 18 U.S.C. Sec. 793(b), (c); 18 U.S.C. Sec. 1030(a)(1); 18 U.S.C. Sec. 1924(a) (up to one year imprisonment for public servant or contractor who "knowingly removes [classified information] without authority and with the intent to retain such documents or materials at an unauthorized location").

[103] 18 U.S.C. Sec. 798(a) (concerning certain categories of classified information); 18 U.S.C. 793(e), (f) (concerning national defense information); 18 U.S.C. Sec. 793(d), (f) (unauthorized communication by those with lawful access to information). *See also* 18 U.S.C. Sec. 1030(a)(1) (retention or communication through unauthorized computer access to a computer, with reason to believe that information "could be used to the injury of the United States, or to the advantage of any foreign nation"); 18 U.S.C. Sec. 641 (theft or conversion of government property or records); Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. Sec. 421-26 (up to 3 years imprisonment for disclosure of the identity of a covert agent, with reason to believe that such activities would impair U.S. foreign intelligence efforts).

[104] 18 U.S.C. Sec. 793(g).

[105] 18 U.S.C. 793(e), (f).

[106] 18 U.S.C. Sec. 798(a).

[107] *See, e.g.*, 18 U.S.C. Sec. 793(d), (f) (unauthorized communication by those with lawful access to information); 18 U.S.C. Sec. 952 (unauthorized disclosure of certain diplomatic material obtained "by virtue of … employment by the United States."); 18 U.S.C. Sec. 1924 (unauthorized retention of classified documents or material by public servants); 50 U.S.C. Sec. 783 (unauthorized disclosure of classified information to an agent of a foreign government, unauthorized receipt by foreign government official).

[108] 18 U.S.C. Sec. 794(a), (c). Severe cases punishable by the death penalty include those resulting in the death of an undercover agent, or concerning communications surveillance or major weapons systems. *See also* 50 U.S.C. Sec. 783(a) (up to 10 years imprisonment for government employees who communicate classified information to a person whom the employee has reason to suspect is a foreign government agent). Members of the military are also subject to the Uniform Military Criminal Code, with a similar definition but lower standard for imposition of the death penalty. Uniform Code of Military Justice, Art. 106a, Arts. 92 (failure to obey order or regulation), 104 (aiding the enemy), 134 ("all disorders and neglects to the prejudice of good order and discipline" and "all conduct of a nature to bring discredit upon the armed forces").

[109] *See generally* Statement of Thomas F. Gimble, Acting Inspector General, Department of Defense, before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform on National Security Whistleblower Protection, February 14, 2006, at http://www.fas.org/irp/congress/2006_hr/021406gimble.pdf.

excludes the intelligence community, including contractors, from protections.[110] An Intelligence Community Whistleblower Protection Act (ICWPA) permits internal, but not public, disclosures of matters of "urgent concern" by some parts of the intelligence sector, and disclosure to Congress.[111] However, it does not protect even internal whistleblowers from retaliation, and any disclosures outside of the designated oversight mechanisms – the Inspector General of the Department of Justice or an intelligence oversight committee in the U.S. Congress – are never protected.

72. A Military Whistleblower Protection Act protects members of the Armed Forces for communications concerning certain types of wrongdoing, including crimes, gross mismanagement or wastes of funds, or substantial dangers to public safety. The law only protects disclosures internally to Congress, an Inspector General, or a Defense Department investigative authority. Further, because the law protects only lawful" communications, it arguably does not protect an individual whose disclosure would be illegal under the Espionage Act, which would cover most if not all of the relevant disclosures.

73. A Presidential Policy Directive, PPD-19 issued in October 2012, purports to support security sector reporting of "waste, fraud, and abuse," in recognition of the limitations of the ICWPA. It orders public servants not to take retaliatory action for "protected disclosures," requires covered government agencies to establish processes to report improper retaliation, and appoints the Inspector General of the Intelligence Community to oversee an external review, at his or her discretion. However, the Policy Directive does not provide for any legal mechanism to redress retaliation, and does not even make the determination and proposed remedy of the administrative review mechanism binding on the intelligence agency. Further, it does not apply to contractors or members of the Armed Forces.[112]

B. Relevant U.S. Practice: Eight Leak Indictments and Unprecedented Incursions on Media Freedom

74. Before the Obama administration, the U.S. government had only issued indictments for the unauthorized disclosure of information pursuant to the Espionage Act in three cases unrelated to spying. Daniel Ellsberg and Anthony Russo, a contracted researcher and an employee, respectively, with the Rand Corporation, famously disclosed the so-called Pentagon Papers, concerning the Vietnam War, to the New York Times, and were prosecuted under the Espionage Act before the case was dismissed on account of prosecutorial misconduct.[113]

---

[110] Whistleblower Protection Act of 1989, Pub.L. 101-12 as amended by the Whistleblower Protection Enhancement Act of 2012 ("WPEA"), Pub.L. 112-199. The WPA does not protect disclosures if they are "specifically prohibited by law and … specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."

[111] The Act defines "urgent concern" as a "serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters"; a false statement to Congress; and taking or threatening to take certain personnel actions in retaliation for making the report to Congress.

[112] Presidential Policy Directive/PPD-19: Protecting Whistleblowers with Access to Classified Information, October 10, 2012, at https://www.fas.org/irp/offdocs/ppd/ppd-19.pdf.

[113] Ellsberg and Russo were charged with unlawfully transmitting defense information under Section 793 of the Espionage Act, theft of government property, and conspiracy to deprive the government of a lawful function, presumed related to the undermining of the government's classification system. The government left out the public disclosure through the *New York Times* from the indictment and instead alleged that Ellsberg provided information to two unauthorized individuals who had no connection to the publication of the Pentagon Papers, one of whom was Anthony Russo, prosecuted for inappropriately accessing the documents, and jailed for refusing to testify against Ellsberg. The

Samuel Loring Morison, a Navy analyst who disclosed photographs of a Soviet ship to the media, was convicted in 1985. This is the only Espionage Act conviction for unauthorized disclosures after trial, a conviction upheld by the Court of Appeals.[114] In the only appellate decision on the interpretation of the Espionage Act, a majority of the Fourth Circuit Court of Appeals, while upholding the conviction, in concurring opinions, recognized that there were significant First Amendment considerations at issue in the use of the Espionage Act to prosecute public servants for unauthorized disclosures.[115]

75. Finally, Lawrence Franklin, a Defense Department analyst was prosecuted for disclosing U.S. policy concerning Iran indirectly to Israel, through lobbyists. He pled guilty to conspiracy charges and, in 2006, received a 13 year prison sentence, later reduced to ten months house arrest.[116] The George W. Bush administration also indicted the two lobbyists, Steven Rosen and Keith Weissman, under the Espionage Act, with conspiracy to disclose classified national security information to journalists and a foreign power, the first ever such charges against non-government officials. The case against the lobbyists was dropped by Obama administration prosecutors after a decision by the trial court judge that the government would have to prove the disclosure harmed the national interest.[117]

76. In a dramatic shift from the past, the Obama administration has issued eight indictments under the Espionage Act in connection with unauthorized disclosures related to national security.

77. Thomas Drake, a former career civil servant with the N.S.A., faced the threat of 35 years imprisonment for his alleged role in the 2007 disclosure to a journalist of information about "financial waste, bureaucratic dysfunction, and dubious legal practices in N.S.A. counterterrorism programs." He was indicted for the unauthorized "willful retention" of government documents, not for their public disclosure. In a pre-trial ruling, the trial court judge ordered that the government prove that the documents at issue were properly classified, after some of the records at issue were found not to be. After the case unraveled significantly; Drake eventually pled guilty to a misdemeanor.[118]

---

case was dismissed because the government was, among other things, the government had intercepted telephonic communications with Ellsberg and misplaced the records. *See* Halperin, note 61 above, 8. Elaine Woo, *Rand staffer encouraged Pentagon Papers leak*, L.A. Times, August 8, 2008, at http://articles.latimes.com/2008/aug/08/local/me-russo8.

[114] Morison was convicted of being in violation of the Espionage Act and committing theft of government property. He was subsequently pardoned by President Bill Clinton. *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988). Stephen Engelberg, *Spy Photos' Sale Leads to Arrest,* N.Y. Times, October 3, 1984, at http://www.nytimes.com/1984/10/03/world/spy-photos-sale-leads-to-arrest.html. *Damming a Leak*, Time Magazine, October 28, 1985, at http://content.time.com/time/magazine/article/0,9171,960226,00.html.

[115] *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Wilkinson, J., concurring, at 1081; and Phillips, J., concurring, at 1085). They noted, in particular, that Morison had a security clearance, knew that the publication would cause harm, and was motivated by personal gain rather than public disclosure of wrongdoing. *See* Halperin note 61 above, 9.

[116] Franklin was prosecuted for unauthorized communication of national defense information, and conspiracy to communicate unauthorized defense information to those not entitled to receive it and to an agent of a foreign government. David Johnston, *Pentagon Analyst Gets 12 Years for Disclosing Data*, N.Y. Times, January 20, 2006, at http://www.nytimes.com/2006/01/20/politics/20cnd-franklin.html?ei=5094&en=1a2688daa350509b&hp=&ex=1137819600&partner=homepage&pagewanted=print.

[117] *Ibid.* Neil Lewis and David Johnston, *U.S. to Drop Spy Case Against Pro-Israel Lobbyists*, N.Y. Times, May 1, 2009, at http://www.nytimes.com/2009/05/02/us/politics/02aipac.html. *See* Halperin, 2012, note 61 above, 10-12.

[118] *See* Jane Mayer, *The Secret Sharer*, The New Yorker, May 23, 2011, at http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all. Drake was charged under

78. Shamai Kedem Leibowitz, a former FBI contract linguist, pled guilty in 2010 to providing a blogger, alleged to be Richard Silverstein, with classified FBI records "concerning the communication intelligence activities of the United States." Leibowitz received a sentence of 20 months imprisonment. Regarding what information was disclosed, the judge overseeing the case said at the sentencing only: "All I know is that it's a serious case. I don't know what was divulged other than some documents—and how it compromised things, I have no idea." Silverstein asserted later that the information consisted of transcripts of FBI wiretaps of the Israeli Embassy purportedly depicting Israel's efforts to gain support for military intervention in Iran. Leibowitz denied this assertion, stating recently that the information he disclosed was never published but related to "the FBI's illegal practices, very similar to what Snowden has reported about the NSA." Leibowitz asserted that he disclosed information in an effort "to inform the American public about the FBI's abuses of their powers," but that he pled guilty in face of the threat of a lengthy imprisonment.[119]

79. In July 2013, former U.S. soldier Chelsea Manning, then known as Private Bradley Manning, was convicted in a court-martial of various violations of the Espionage Act and theft of government property for her disclosure of over 700,000 diplomatic cables and military records to Wikileaks. She was sentenced to 35 years imprisonment. The records were sensitive, and in some cases classified, and included a video documenting the killing of journalists in Iraq. Wikileaks in turn published many of the records online as part of a collaboration with various media outlets, including the New York Times and The Guardian. Among the other charges, the prosecution alleged that Manning indirectly aided the enemy through her public disclosures—effectively asserting that the public disclosures in online fora presented information which Manning knew Al Qaeda could and would access.[120] In the end, she was found not guilty of aiding the enemy, the most serious charge, though the judge refused to dismiss the charge outright. Also, before her court-martial began, Manning had been detained

---

18 U.S.C. 993(e) for unlawful possession and retention, but not for the transmission of information to journalists, though that was referenced in the indictment. In the end, he made a misdemeanor guilty plea to exceeding authorized computer use. Indictment, *United States v. Thomas Andrews Drake*, N.D. MD, April 14, at http://www.fas.org/sgp/news/2010/04/drake-indict.pdf. *See generally*: Federation on Government Secrecy, USA v. Thomas A. Drake: Selected Case Files, at http://www.fas.org/sgp/jud/drake. Marcy Wheeler, *Government Case Against Whistleblower Thomas Drake Collapses*, The Nation, June 13, 2011, at http://www.thenation.com/article/161376/government-case-against-whistleblower-thomas-drake-collapses#. Halperin, 2012, note 61 above, at 12.

[119] *United States v. Shamai Kedem Leibowitz*, Judgment, Md. Dist. Ct., May 24, 2010, at https://www.documentcloud.org/documents/323919-liebowitz-order.html. Department of Justice, *Press Release: Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to a Blogger*, December 17, 2009, at http://www.justice.gov/opa/pr/2009/December/09-nsd-1361.html. Shamai Leibowitz, *Edward Snowden and the Crackdown that Backfired*, The Leibowitz Blog, June 24, 2013, at http://www.shamaileibowitz.com/2013/06/edward-snowden-man-of-conscience.html. Leibowitz was charged with disclosing classified information under 18 U.S.C. Sec. 798. Scott Shane, *Leak Offers Look at Efforts by U.S. to Spy on Israel*, N.Y. Times, September 5, 2011, at http://www.nytimes.com/2011/09/06/us/06leak.html?_r=0.

[120] The prosecution justified the charge on the ground that Manning "was trained specifically that Al Qaeda used the internet to get this information, that the enemy was looking for this specific type of information." *See* Yochai Benkler, *Bradley Manning 'aiding the enemy' charge is a threat to journalism*, The Guardian, July 19, 2013 (aiding the enemy charge "establishes a chilling precedent: leaking classified documents to the these newspapers can by itself be legally sufficient to constitute the offense of 'aiding the enemy,' if the leaker was sophisticated enough about intelligence and how the enemy uses the internet").

for two years without charge, including eight months in solitary confinement, provoking a domestic and international outcry.[121]

80. Wikileaks founder Julian Assange is the subject of a secret grand jury investigation, reportedly ongoing from 2010 until at least mid-2013, as a result of the Manning disclosures. According to reports, the government is seeking to bring conspiracy charges against Assange, and offered Manning a plea deal, prior to his court-martial, if he would testify against Assange. The government has refused to officially acknowledge this years-long investigation, yet various individuals have reported that they have been subpoenaed to testify and provided official documentation to confirm their assertions.[122]

81. In 2010, the Department of Justice charged Stephen Jin-Woo Kim, a State Department intelligence advisor, with disclosing national defense information concerning North Korea's nuclear aspirations and advances to a journalist, James Rosen of Fox News. The trial court judge rejected a First Amendment challenge to the Espionage Act prosecution, but required that the government prove that the information was legitimately national defense information reasonably expected to harm national security, and that Kim had reason to believe that disclosure would be harmful to the United States or beneficial to a foreign government. Kim has pled not guilty and his case is ongoing.[123]

82. In connection with the Kim indictment, prosecutors monitored Rosen, the journalist alleged to be the recipient of Kim's communications, including by tracking his phone records and engagements at the State Department, and issuing search warrants for his e-mail communications with Kim, as well as his other private communications around the time of the story or with other actual or potential sources. While the Department of Justice has not indicted Rosen, it labeled Rosen a "co-conspirator and/or aider and abettor" in court filings and asserted that "there is probable cause to believe that the reporter has committed or is committing a violation of the law against national security leaks." In making such assertions, the government relied in part on e-mail communications in which Rosen indicates he is "interested in, as you might expect, … breaking news ahead of my competitors" and expressing that he would "love to see some internal State Department analyses."[124]

---

[121] Julie Tate, *Judge sentences Bradley Manning to 35 years*, Washington Post, August 21, 2013, at http://articles.washingtonpost.com/2013-08-21/world/41431547_1_bradley-manning-david-coombs-pretrial-confinement.

[122] Charlie Savage, *U.S. Tries to Build Case for Conspiracy by Wikileaks* , N.Y. Times, at http://www.nytimes.com/2010/12/16/world/16wiki.html?_r=1&hp. December 15, 2010, at David Carr and Ravi Somaiya, *Assange, Back in the News, Never Left U.S. Radar*, N.Y. Times, June 24, 2013, at http://www.nytimes.com/2013/06/25/world/europe/wikileaks-back-in-news-never-left-us-radar.html. Julie Tate, *Judge sentences Bradley Manning to 35 years*, Washington Post, August 21, 2013, at http://articles.washingtonpost.com/2013-08-21/world/41431547_1_bradley-manning-david-coombs-pretrial-confinement.

[123] Kim was charged under 793(d) of the Espionage Act as well as 18 U.S.C. Sec. 1001(a)(2), for making false statements to the F.B.I. *United States v. Stephen Jin-Woo Kim*, Indictment, D.C. Dist. Ct., August 19, 2010, at http://www.fas.org/sgp/jud/kim/indict.pdf. Scott Shane, *U.S. Analyst Is Indicted in Leak Case, N.Y. Times*, August 27, 2010, at http://www.nytimes.com/2010/08/28/world/americas/28leak.html. *United States v. Stephen Jin-Woo Kim*, Notice of Declassification, D.C. Dist. Ct., June 6, 2013 (naming Rosen and Fox News), at http://www.fas.org/sgp/jud/kim/060613-declass.pdf. *See generally*, Federation of American Scientists Project on Government Secrecy, USA v. Stephen Kim; Selected Case Files, at http://www.fas.org/sgp/jud/kim/.

[124] The judge's order granting the search warrant request accepted that there was sufficient justification that Rosen was a co-conspirator. Ann Marimow, May 19, 2010, *A rare peek into a Justice Department leak probe,* Washington Post, May 19, 2010, at http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-

83. Former C.I.A. officer Jeffrey Sterling faces prosecution under the Espionage Act in connection with the alleged disclosure of U.S. government efforts to sabotage the Iranian nuclear program to New York Times journalist James Risen. The efforts were described in Risen's book, *State of War*, in which Risen asserts that, according to an unnamed C.I.A. officer, a C.I.A. intervention may have inadvertently enhanced Iran's nuclear capabilities. Sterling purportedly reported this to a Congressional intelligence committee without result. After the alleged disclosures, Sterling was indicted on charges of unauthorized retention of national defense information and its disclosure to Risen. His case is ongoing.[125]

84. In connection with the Sterling case, the Obama Administration has made the unprecedented argument that Risen, the journalist who is the recipient of the allegedly leaked information, must testify. A trial judge ruled that the First Amendment prevented the government from ordering Risen's testimony, but that decision was overturned by the appellate court on the ground that Risen is "without dispute the only witness who can offer … critical testimony" as to "the illegal disclosure of classified, national security information by one who was entrusted to protect national security, but who is charged with having endangered it instead." One dissenting judge, Roger L. Gregory, asserted that the majority decision would eviscerate the reporter's privilege to protect her sources: "The majority exalts the interests of the government while unduly trampling those of the press, and in doing so, severely impinges on the press and the free flow of information in our society." Judge Gregory said in a later ruling (rejecting *en banc* review) that the case is of "exceptional importance" as, for "public opinion to serve as a meaningful check on governmental power, the press must be free to report to the people the government's use (or misuse) of that power."[126]

85. In January 2013, John Kiriakou, the former senior C.I.A. officer who led the capture of Abu Zubaydah, pled guilty to a violation of the Intelligence Identities Protection Act in connection with the disclosure to a journalist (who never published the information) of the identity of a C.I.A. officer. He had originally been indicted on charges of Espionage Act violations and making false statements as well. He asserted that he accepted the plea agreement because of the threat of an extended prison term (50 years) and mounting legal fees (more than $500,000). With the plea, he was sentenced to 30 months imprisonment in a plea agreement.

86. The Kiriakou investigation reportedly began with the 2009 discovery that lawyers for prisoners in Guantánamo Bay had names and photographs of C.I.A. officers, and were seeking to name

---

probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html. *United States v. Stephen Jin-Woo Kim*, Application for a Search Warrant, D.C. Dist. Ct., May 28, 2010, at http://www.newyorker.com/online/blogs/newsdesk/2013/05/the-doj-versus-journalist-gmail.html.

[125] *United States v. Jeffrey Alexander Sterling*, Indictment, E.D. Va. Dist. Ct., December 22, 2010, at http://www.fas.org/sgp/jud/sterling/indict.pdf. The New York Times never published the relevant information which appeared in Risen's book, due to government assertions that the information would harm national security. Charlie Savage, *Ex-C.I.A. Officer Named in Disclosure Indictment*, N.Y. Times, January 6, 2011, at http://www.nytimes.com/2011/01/07/us/07indict.html. *See generally* Federation of American Scientists Project on Government Secrecy, USA v. Jeffrey Alexander Sterling: Selected Case Files, at http://www.fas.org/sgp/jud/sterling/.

[126] Charlie Savage, *Court Tells Reporter to Testify in Case of Leaked C.I.A. Data*, N.Y. Times, July 19, 2013, at http://www.nytimes.com/2013/07/20/us/in-major-ruling-court-orders-times-reporter-to-testify.html. Charlie Savage, *Court Rejects Appeal Bid by Writer in Leak Case*, N.Y. Times, October 15, 2013, at http://www.nytimes.com/2013/10/16/us/court-rejects-appeal-bid-by-writer-in-leak-case.html. The appeals court majority ruled: "There is no First Amendment testimonial privilege, absolute or qualified, that protects a reporter from being compelled to testify by the prosecution or the defense in criminal proceedings about criminal conduct that the reporter personally witnessed or participated in, absent a showing of bad faith, harassment, or other such non-legitimate motive, even though the reporter promised confidentiality to his source."

them as witnesses in their efforts to challenge the lawfulness of the interrogations of men subjected to waterboarding and other abusive interrogation techniques. The Justice Department alleged that the information provided by Kiriakou to a journalist was subsequently disclosed to Guantánamo lawyers. As part of the investigation into Kiriakou, the F.B.I. also investigated, and subsequently cleared, Guantánamo defense counsel.[127]

87. James Hitselberger, a contracted linguist with the U.S. Navy, was indicted in October 2012 under the Espionage Act for retaining defense information without authorization while in Bahrain. According to the FBI, the information concerned military activities in the Middle East and U.S. intelligence gaps. Some of the records were transferred to public archives at Stanford University. Prosecutors have not alleged espionage, and the judge affirmed that Hitselberger "did not disseminate the classified information to a 'foreign power,'" but little more has been publicly released concerning the facts of the case, and the motivations of Hitselberger, or the motivations of the Department of Justice in prosecuting the case.[128]

88. On June 14, 2013, the U.S. Department of Justice filed charges against Edward Snowden under the Espionage Act for the unauthorized communication of national defense information and willful communication of classified communications intelligence information to an unauthorized source, as well as for theft of government property. He faces a maximum sentence of thirty years, though other charges could be added. Snowden provided N.S.A.

---

[127] Charlie Savage, *Ex-C.I.A. Officer Charged in Information Leak*, N.Y. Times, January 23, 2012, at http://www.nytimes.com/2012/01/24/us/ex-cia-officer-john-kiriakou-accused-in-leak.html. Scott Shane, *Ex-Officer Is First from C.I.A. to Face Prison for a Leak*, N.Y. Times, January 5, 2013, at http://www.nytimes.com/2013/01/06/us/former-cia-officer-is-the-first-to-face-prison-for-a-classified-leak.html?pagewanted=1&smid=tw-nytimes&_r=0. In 2007, Kiriakou asserted in a news interview that Abu Zubaydah started cooperating with interrogators after a single instance of waterboarding, information later rejected by him and challenged by official documents recognizing that the prisoner was waterboarded more than 83 times. Kiriakou was not indicted for disclosing this information, arguably information whose disclosure was favorable to the Bush administration's efforts at the time to defend its use of waterboarding. ABC News, *Transcript: "CIA-Abu Zubaydah:" - Interview with John Kiriakou*, December 10, 2007, at http://abcnews.go.com/images/Blotter/brianross_kiriakou_transcript1_blotter071210.pdf. *See* Brian Stetler, *How '07 ABC Interview Tilted a Torture Debate*, N.Y. Times, April 27, 2009, at http://www.nytimes.com/2009/04/28/business/media/28abc.html. However court documents filed in connection with Kiriakou's leak prosecution indicate that the C.I.A. notified the Department of Justice of the unauthorized disclosure of classified information. Scott Shane, *Ex-Officer Is First from C.I.A. to Face Prison for a Leak*, N.Y. Times, January 5, 2013, at http://www.nytimes.com/2013/01/06/us/former-cia-officer-is-the-first-to-face-prison-for-a-classified-leak.html?pagewanted=1&smid=tw-nytimes&_r=0. Information was reportedly subsequently revealed to the attorneys for Abu Zubaydah and Khalid Sheikh Mohammed. Both men are now imprisoned at Guantánamo, and were held previously in undisclosed "black sites" and subjected by the C.I.A. many times to waterboarding, an act Obama recognized as torture. No one has ever been prosecuted for harsh interrogations in connection with the "war on terror." Said one former C.I.A. officer, Bruce Reidel, "the irony of the whole thing is, very simply, that he's going to be the only C.I.A. officer to go to jail over torture." Scott Shane, *Ex-Officer Is First from C.I.A. to Face Prison for a Leak*, N.Y. Times, January 5, 2013, at http://www.nytimes.com/2013/01/06/us/former-cia-officer-is-the-first-to-face-prison-for-a-classified-leak.html?pagewanted=1&smid=tw-nytimes&_r=0. *See* Ewan MacAskill, *Obama: 'I believe waterboarding was torture, and it was a mistake'*, The Guardian, April 29, 2009, at http://www.theguardian.com/world/2009/apr/30/obama-waterboarding-mistake.

[128] Hitselberger was indicted pursuant to 18 U.S.C. Sec. 793(e). *United States v. James F. Hitselberger*, Indictment, D.C. Dist. Ct., October 26, 2012, at http://www.fas.org/sgp/jud/hitsel/indict.pdf. *See generally* Federation of American Scientists Project on Government Secrecy, *USA v. James F. Hitselberger: Selected Case Files*, at http://www.fas.org/sgp/jud/hitsel/. Josh Gerstein, *Judge Orders Release of Linguist for Navy*, Politico, December 19, 2012, at http://www.politico.com/blogs/under-the-radar/2012/12/judge-orders-release-of-linguist-for-navy-152440.html. *Linguist Charged Under Espionage Act*, Associated Press, November 7, 2012, at http://newsok.com/linguist-charged-under-espionage-act/article/feed/459520.

documents to Glenn Greenwald, a blogger and journalist with The Guardian, and Laura Poitras, a filmmaker.[129]

89. In addition to the indictments already issued, the Department of Justice is pursuing vigorously – and controversially – other leak investigations. In the most criticized, the Department of Justice is pursuing an investigation of the alleged leak to the Associated Press of information related to the purported CIA unraveling of an Al Qaeda plot, disclosed publicly in May 2012.[130] As part of this ongoing investigation, the Department of Justice secretly subpoenaed two months of communications records of more than 20 phone lines connected to the Associated Press. The AP described this as "overbroad" and "unprecedented." The Newspaper Guild of Communications Workers of America called the subpoena "egregious and a direct attack on journalists": "The ability of journalists to develop and protect sources is vital to keeping the public informed about issues affecting their lives."[131] Attorney General Eric Holder, for his part, described the leak that prompted the subpoena one of the most serious and harmful he has seen, and worthy of a strong investigation.[132]

90. Following growing outrage over the government's incursions of media freedom, including especially the broad and secret AP subpoenas, the Obama administration issued new guidelines for leak investigations in July 2013, limiting when the Justice Department may access a journalist's records and requiring a presumption of notice in advance of the filing of a subpoena.[133] The Obama administration also asserted it would seek to establish a media shield law that would increase a judge's ability to quash subpoenas for the testimony of journalists, legislation that the Obama administration was instrumental in preventing previously.[134]

91. New York Times journalist Mark Mazzetti similarly said: "This crackdown has perhaps had its intended effect which was maybe not to go prosecute the cases that have been brought, but also to scare others into not talking."[135] Anthony Romero, the Executive Director of the American Civil Liberties Union, concurred that the investigation into Guantanamo defense counsel as well as other processes challenging unauthorized disclosures had a "chilling effect

---

[129] Snowden was charged under 18 U.S.C. 641, 18 U.S.C. 793(d), and 18 U.S.C. 798(a)(3)). Scott Shane, *Ex-contractor Is Charged in Leaks on N.S.A. Surveillance*, N.Y. Times, June 21, 2013, at http://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html?pagewanted=all&_r=0.

[130] *See* Adam Goldman and Matt Apuzzo, *US: CIA thwarts new al-Qaida underwear bomb plot*, Associated Press, May 7, 2012.

[131] Alejandro Martinez, *U.S. government secretly obtains phone records from AP reporters, editors*, Journalism in the Americas blog, May 14, 2013, at https://knightcenter.utexas.edu/blog/00-13881-us-government-secretly-obtains-phone-records-ap-reporters-editors.

[132] There are reportedly other major ongoing leak investigations, including investigations related to the disclosures of information about U.S.-Israeli cyberattacks in Iran and targeted killing procedures. *See* NBC News, at http://www.nbcnews.com/video/nightly-news/52334927/?ocid=twitter#52334927.

[133] U.S. Department of Justice, *Report on Review of News Media Policies*, July 12, 2013, at http://www.justice.gov/iso/opa/resources/2202013712162851796893.pdf. Under the new guidelines, the Attorney General may overcome the presumption of advance notice of a subpoena only with an assertion that notice would seriously harm the investigation, national security, or human life or safety.

[134] Charlie Savage, *Court Tells Reporter to Testify in Case of Leaked C.I.A. Data*, N.Y. Times, July 19, 2013, at http://www.nytimes.com/2013/07/20/us/in-major-ruling-court-orders-times-reporter-to-testify.html. Charlie Savage and Jonathan Weisman, *Holder Faces New Round of Criticism After Leak Inquiries*, N.Y. Times, May 29, 2013, at http://www.nytimes.com/2013/05/30/us/politics/holder-faces-a-new-round-of-criticism.html?pagewanted=all&_r=0.

[135] *The Way of the Knife: NYT's Mark Mazzetti on the CIA's Post-9/11 Move from Spying to Assassinations*, Democracy Now, April 10, 2013, at http://www.democracynow.org/2013/4/10/the_way_of_the_knife_nyts.

on government whistle-blowers and journalists."[136] Eric Lichtblau, long-time national security reporter for the New York Times, said that the "threat of the subpoena" informed his departure to a less risky field of journalism; veteran national security journalist Jane Mayer has asserted that national security disclosures have come to a "standstill."[137]

C. Assessment of U.S. Compliance with International Human Rights Law

92. U.S. law and practice is non-compliant with international legal standards and deviates from trends of good practice among democratic states outlined above.

(1) The offenses are vague and overbroad, and lack requisite intent and harm requirements. Nor has the Executive or the courts read such requirements into the statutes.

(2) The offenses and penalties also do not sufficiently take into account the public interest in disclosure of certain information, or provide adequate whistleblower protections for security sector personnel.

(3) Moreover, for most offenses, the law does not distinguish between public servants, on the one hand, and the media and the public, on the other, in terms of applicable offences or penalties. Further, U.S. law criminalizes conspiracy to commit an offense, at the same level as the actual offense, and unauthorized possession, without sufficient protections for journalists or public watchdogs.

(4) Finally, the penalties for unauthorized possession and disclosure under U.S. law are disproportionately severe, with chilling effects.

93. *First*, the Espionage Act provisions criminalizing unauthorized possession and disclosure of security-related information are vague and overbroad, and lack the requisite intent and harm requirements. The Espionage Act offenses are not limited to factors typically associated with spying, but can instead be used, and have increasingly been used, for the criminalization of simple possession and disclosure. While the government has not attempted to prosecute "traditional" journalists thus far, the secret grand jury investigation of Julian Assange suggests that the government may try to prosecute others who disclose information publicly via the internet, at the very least an incremental extension of the scope of the Act. The official government assertion that James Rosen was an unindicted aider and abetter or co-conspirator is another ominous sign. While the history suggests the law was intended for the narrow purpose of prosecuting (and deterring) spies who transfer information to foreign enemies to harm the United States or benefit the foreign enemy, the language of the law permits such a broad reading. The broad reading is not only a major deviation from the law's intent, and its use in the past; it is also inconsistent with international law.

---

[136] Charlie Savage, *Ex-C.I.A. Officer Charged in Information Leak*, N.Y. Times, January 23, 2012, at http://www.nytimes.com/2012/01/24/us/ex-cia-officer-john-kiriakou-accused-in-leak.html.

[137] *See generally* Molly Redden, *Is the 'Chilling Effect' Real? National security reporters on the impact of federal scrutiny*, The New Republic, May 15, 2013, at http://www.newrepublic.com/article/113219/doj-seizure-ap-records-raises-question-chilling-effect-real (Lichtblau: "While the Justice Department never made good on the threat, it certainly made it more difficult to do my job in dealing with confidential sources when you realize you may be forced to testify before a grand jury or risk going to jail to protect a source"; Mayer: "chilling isn't quite strong enough, it's more like freezing the whole process into a standstill").

94. An individual can be sanctioned pursuant to the Espionage Act even where the disclosure does not harm U.S. national security interests.[138] The "advantage" to a foreign nation is generally sufficient to result in criminal sanction. International standards, in contrast, require proof of the actuality or likelihood of harm as an element of any offence that could be applied to the receipt, possession or disclosure of information.[139]

95. Further, there is no requirement of any bad faith—of the *intent* to cause harm, or even the intent to benefit a foreign state except in the more traditional espionage provision—for the imposition of criminal sanctions for unauthorized possession or disclosure under U.S. law. For the offense of unauthorized disclosure of documents, the law only requires the intent to transfer the information. The standard for unauthorized possession or disclosure of information requires only that the offender has "reason to believe" that the information could harm the United States or benefit a foreign state.

96. Indeed, even for a more traditional espionage offense of "aiding the enemy," the current U.S. administration has asserted that the public disclosure of sensitive security-related information on the internet would demonstrate sufficient intent as it would provide the enemy access to the information, alongside the public.

97. Vagueness and over-breadth are particularly problematic in criminal laws that restrict possession or communication of information given the high potential to chill the legitimate exercise of the right to freedom of expression, especially when there is vagueness in the element of intent (see paras. 20-21, above).

98. *Second*, there are insufficient protections for disclosures in the public interest. As noted above (in Section II.D.2), the evolving trend in international and national law and practice is to prohibit the sanctioning of public servants for disclosing government-held information where the public interest in the disclosure outweighs the harm, and further, to protect from retaliation any disclosures of wrongdoing. In addition, as described above (at para. 28), the right to truth in international law creates a strong presumption, or overriding obligation, in favor of the disclosure of information concerning gross human rights violations or serious humanitarian law violations, regardless of asserted classification status.

99. There is nothing in the Espionage Act or related laws that provide for exceptions for disclosures in the public interest, or concerning human rights violations or violations of international humanitarian law. The improper classification of the information disclosed is also not clearly a defense under the text of the law.

100. Moreover, U.S. whistleblower protections are limited and do not protect security sector employees who disclose information concerning wrongdoing or other information in the public interest. Public disclosures are never protected under U.S. law, even if internal

---

[138] *But see* Tabassum Zakaria, *U.S. to Drop Spy Case*, Reuters, May 1, 2009, at http://uk.reuters.com/article/2009/05/01/us-security-pentagon-idUKTRE54046320090501. In the prosecution by the United States of lobbyists who allegedly disclosed information to Israel concerning the Iranian nuclear program, the trial judge ruled that the government had to prove that U.S. national security interests were harmed in the disclosure of information by lobbyists to a foreign government, and that they wanted to benefit another state and harm the United States by his actions. (This led prosecutors to drop the charges.)

[139] General Comment No. 34, note 11 above, para. 30. *Guja v. Moldova*, note 42 above, paras. 76. *Bucur v. Romania*, note 59 above, paras. 114-15. *See also* Inter-American Model RTI Law, note 13 above, Arts. 41(b), 44 (restrictions on disclosure are legitimate only when disclosure "would create a clear, probable and specific risk of substantial harm" to identified public interests). OAS Special Rapporteur 2011 Report, note 28 above, Ch. III, para. 357.

mechanisms have been or would be ineffective and the information disclosed constitutes, for example, a serious crime, gross human rights violations, or other information of great public interest such as the surveillance programs disclosed by Snowden. The limited Presidential Directive of October 2012, which applies to whistleblowers in the security sector (see para. 73, above), does not permit a right of legal action for retaliation of internal whistleblowing. Reviews of alleged retaliatory action are permitted only within the intelligence community, and only at their discretion—an "independent" review of alleged retaliatory action may be pursued by the Inspector General of the Intelligence Community at his choice. Even remedies ordered by the Inspector General are not mandatory, but are instead at the discretion of the agency subject to review.

101. *Third*, U.S. law, by not distinguishing in this manner between public servants and members of the public in most cases, deviates from the evolving trend identifying the State as primarily, or exclusively, responsible for keeping information secret. (See Section II.D, above.) The concept of proportionality requires no penalties, or at a minimum lesser penalties, for the media and other members of the public who do not have a duty of loyalty or confidentiality to a government employer. This is particularly true for the media and others who have a special watchdog role to play in effectuating the free flow of information and ideas.

102. Further, for the media and members of the public, there are particular concerns attached to the criminalization of conspiracy. The actual or threatened prosecution of journalists and other social watchdogs for conspiracy risks criminalizing their performance of their professional obligations – seeking information from government sources – and jeopardizes their freedom to perform their work without fear of improper pressures to reveal their sources or limit their reporting or analysis. It also compromises the protection of journalistic sources. By allowing private persons to be held criminally responsible for conspiracy, subject to the same penalties as the related offenses, U.S. law violates good law and practice reflected in the Tshwane Principles. (See para. 66, above.)

103. Moreover, U.S. law criminalizes, with significant penalties the unauthorized possession of classified or national defense information, without requiring any disclosure, any intent beyond the intent to possess the information, or evidence or likelihood of harm. The Tshwane Principles are silent regarding penalties for the unauthorized possession of classified information by public servants and explicitly recommend against any sanctions for the receipt or possession of classified information by members of the public.[140] While unauthorized possession by public servants may merit administrative or disciplinary sanctions, criminalization is excessive and disproportionate. Possession by a member of the public, especially where there is no intent to harm national security or disclose directly to a foreign state or hostile non-state actor, does not merit any criminal penalty.

104. *Finally*, U.S. penalties for unauthorized possession and disclosure are disproportionately severe, in law and practice (as they are for most U.S. criminal statutes). International law requires that restrictions on freedom of information be proportionate, and penalties not excessive, whether or not the disclosure of information is in the public interest, in order to protect the rights of persons who disclose and avoid discouraging the free expression of others.[141]

---

[140] Tshwane Principles, notes 7 & 10 above, Principle 47.

[141] *Guja v. Moldova*, note 42 above, para. 78 ("in connection with the review of the proportionality of the interference in relation to the legitimate aim pursued, attentive analysis of the penalty imposed on the applicant and its consequences is required"). *Bucur v. Romania*, note 59 above, para. 119.

105. U.S. law includes criminal penalties that are more severe than the laws of many other democratic countries.[142] They are also more broadly applicable with fewer protections and limitations. Given the vagueness and over-breadth of some of their terms, the lack of a harm test, and the inapplicability of public interest defenses, these provisions and their associated penalties would have an unacceptable chilling effect on freedom of expression. Indeed, the government has repeatedly emphasized that this is the intention.[143] As the penalties will not only affect the wrongdoer, but will prevent others from exercising their rights, the standard for proportionality is higher. Such high penalties are also concerning given the often widespread over-classification of information.

IV. CONCLUSION

106. For the reasons described above, the U.S. law provisions concerning offenses and penalties for the unauthorized possession or disclosure of classified information do not satisfy the obligations that legitimate restrictions on freedom of information be narrowly drawn to provide a reasonable expectation of the interpretation of the law, and necessary in a democratic society. Of particular concern, these provisions stand to deter or actually prevent the disclosure of information in the public interest, in a manner inconsistent with international law and comparative best practices.

107. In light of these concerns, we reiterate our request that this Commission endorse the Tshwane Principles. Such an endorsement would advance, for the United States and other countries in the region, a set of detailed guidelines on the appropriate limits of secrecy, the role of whistleblowers, and limitations on prosecutions for unauthorized disclosures.

---

[142] In many countries, the penalties allowed for the unauthorized public *disclosure* of national security information are limited to five or fewer years' imprisonment where there is no espionage, treason or disclosure to a foreign state. This is true in Brazil (one year, and only applicable to public servants), U.K. (2 years), Slovenia (3 years), Panama and Spain (4 years), Colombia and Norway (4 ½ years), and Belgium, Mexico, Paraguay and Poland (5 years).

Penalties for mere *possession* of classified information are generally substantially less, if they exist at all. For instance, the maximum penalty in the UK is only 51 weeks; in Guatemala and Norway, two years; in Australia, six months for possession and two years for unlawful receipt; and in Ecuador, three years. Demonstrative of the evolving trend, Romanian legal reforms will decrease 2014, will decrease the maximum penalty for unauthorized possession from ten to two years in 2014.

Concerning offences of *espionage, treason or disclosure to a foreign state*, for which there are often more severe penalties, best practice is for penalties to be limited to fewer than 15 years, even when top secret information is disclosed: Poland and Slovenia (8 years), Guatemala and Panama (10 years), Ecuador and Spain (12 years), Nigeria and the United Kingdom (14 years); Brazil, Czech Republic, France, Hungary, Norway, Paraguay, and Serbia (15 years); and Denmark (16 years).

[143] *See, e.g.*, Statement of David S. Kris, Assistant Attorney General for the National Security Division, in *Press Release: Employee of Federal Contractor Charged with Disclosing National Defense Information to National News Reporter*, August 27, 2010, at http://www.fas.org/sgp/news/2010/08/doj082710.html ("Today's indictment should serve as a warning to anyone who is entrusted with sensitive national security information and would consider compromising it."). Statement of David S. Kris, Assistant Attorney General for the National Security Division, in Press Release: Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to a Blogger, December 17, 2009, at http://www.justice.gov/opa/pr/2009/December/09-nsd-1361.html ("Today's guilty plea should serve as a warning to anyone in government who would consider compromising our nation's secrets.").