U.N. HUMAN RIGHTS COMMITTEE

Submission for the Periodic Review of the United States

February 2014

The Open Society Justice Initiative presents this submission to the Human Rights Committee in advance of its examination of the United States' periodic report. This submission addresses U.S. compliance with Article 19 of the International Covenant on Civil and Political Rights, and draws heavily on the Global Principles on National Security and the Right to Information (the "Tshwane Principles") to focus on the right of the public to information, and especially information of high public interest, including information related to the security sector and state surveillance; the obligation of the state to protect from sanctions those who possess or disclose information in the public interest, and to ensure that any sanctions on unauthorized disclosures are necessary and proportionate to protect national security or other legitimate interest; and the lack of appropriate protection in the United States for public interest disclosures in the security sector, including most notably, information related to communications surveillance.

OPEN SOCIETY
JUSTICE INITIATIVE

Executive Summary

The Open Society Justice Initiative[1] makes this submission to the Human Rights Committee prior to its review of the United States' 4th periodic report on compliance with the International Covenant on Civil and Political Rights (ICCPR), ratified by the U.S. in 1992. In its question 22, the Committee asked the U.S. to clarify issues concerning "judicial oversight over National Security Agency surveillance." This submission addresses U.S. compliance with its obligations under Article 19 of the ICCPR, and in particular, focuses on:

- The right of the public to information, and especially information of high public interest, including information related to the security sector and state surveillance;
- The obligation of the state to protect from sanctions those who possess or disclose information in the public interest, and to ensure that any sanctions on unauthorized disclosures are necessary and proportionate to protect national security or other legitimate interest;
- The lack of appropriate protection in the United States for public interest disclosures in the security sector, including most notably, information related to communications surveillance.

This submission draws heavily on the Global Principles on National Security and the Right to Information (the "Tshwane Principles"), issued on 12 June 2013,[2] which are based on international and national law, standards, good practices, and the writings of experts, including the 1995 Johannesburg Principles on National Security, Freedom of Expression and Access to Information ("Johannesburg Principles").[3] . The Tshwane Principles have been endorsed by the Parliamentary Assembly of the Council of Europe (PACE); as well as by the UN special mandate-holders on the protection and promotion of human rights while countering terrorism, and the promotion and protection of the right to freedom of opinion and expression; and the three regional Special Rapporteurs on

[1] 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.

[2] The Tshwane Principles were elaborated by the Justice Initiative, along with 21 other organizations and academic centres, and are named after the municipality in South Africa where the meeting to finalize the Principles was held. http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

[3] These principles are relevant to other countries 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 most relevant to whistleblower protections are Part VI and VII. The principle most relevant to surveillance is Principle 10E.

freedom of expression, information and/or the media of the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE), and the African Commission on Human and Peoples' Rights (ACHPR).[4]

Recommendations

We encourage the Committee to raise the following questions:

- What protections are in place to ensure both the public's right to receive information and the freedom of expression of security sector employees or contractors who uncover information of great public interest?
  - Does U.S. law provide security sector whistleblowers, including contractors, a legal right of action to challenge any improper retaliation against them? If so, which protections and how are they applicable?
  - Does the Presidential Policy Directive, PPD-19, provide for binding remedies on the intelligence agency if a violation (improper retaliation for disclosures) has been found?
  - Do protections exist for security sector whistleblowers who disclose information *publicly* because internal disclosures or disclosures to oversight bodies were, or would have been, ineffective?
  - Would PPD-19 have protected from prosecution or other retaliation any of those prosecuted under the Espionage Act during the past six years?
- How does the Espionage Act comply with obligations under international law to protect freedom of expression with only limited restrictions which are clear, necessary and proportionate, and neither arbitrary nor overbroad?
  - How does U.S. law comply with the international law obligation to ensure that any limitation on freedom of expression is necessary to satisfy a compelling public interest and proportionate?
  - How does U.S. law and policy ensure adequate consideration of the public interest in determining whether to prosecute a security sector employee or contractor for an unauthorized disclosure of information?
  - Does U.S. law and policy consider, in compliance with international law, actual or probable harm in a challenged disclosure of information related to defence or national security in considering whether to prosecute such a case?

[4] PACE, Recommendation 2024(2013), para. 1.3, adopted October 2, 2013; and PACE Resolution 1954 (2013), adopted October 2, 2013, paras. 7-9, at http://assembly.coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=20190&lang=en. 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.

  - How does U.S. law consider the element of intent in promulgating sanctions for unauthorized disclosures of information related to defence and national security?
  - Under international law, restrictions on freedom of expression must be the least restrictive to achieve the legitimate objective to which they are directed. Given the relative severity of penalties within the Espionage Act, does the Espionage Act comply with this standard? In U.S. law, are there any restrictions on how many prison terms for public disclosure of information may be ordered to be served consecutively?
- Does U.S. law comply with the increasingly recognized right of the public to information relating to gross human rights violations or serious violations of international humanitarian law, recognized as part of the right to truth?
- Other than the First Amendment, do safeguards exist in compliance with international law to protect members of the public generally, and journalists in particular, who disclose information in the public interest, whether or not it is classified?[5] How does U.S. law satisfy international legal obligations to ensure protection of journalistic sources?How does U.S. law and policy comply with the Global Principles on National Security and the Right to Information (the "Tshwane Principles")?

We urge the Committee to recommend to the U.S.:

- Amend the Espionage Act to (a) appropriately limit the intent and harm requirements in a manner consistent with international law; (b) provide exceptions to penalty for disclosures in the public interest; (c) eliminate the penalty for conspiracy to commit an offence for non-public servants; (d) distinguish between penalties available for public servants and for private persons; and (e) ensure that penalties are proportionate.
- Exercise prosecutorial discretion to limit the prosecution of unauthorized disclosures to situations in which there is real and demonstrable harm to national security resulting from the disclosure, and the harm is greater than the public interest in the disclosure.
- Ensure that legislation adequately protects public servants, including security sector employees and service members, who disclose information concerning human rights violations, wrongdoing or other information in the public interest.

[5] Four incidents have been highlighted as of particular concern in demonstrating the weakening protections, in practice, for journalists and others without security clearance who have been involved in the disclosure of information : (1) the grand jury empanelled to investigate and consider charges against Julian Assange; (2) the U.S. government effort, upheld thus far by an appellate court, to compel journalist James Risen to testify in a case about the source for information he reported in his book; (3) the extensive investigation of reporter Jeffrey Rosen, including the tracking of personal phone and e-mail records, and the official allegation that he was a "co-conspirator and/or aider and abettor" as part of a leak prosecution; and (4) the subpoenaing of months of communications records of more than 20 phone lines connected to the Associated Press, without advance notice and a possibility to contest legally this invasion of privacy and infringement of freedom of expression.

U.S. Non-Compliance with Article 19

Actual or Threatened Sanctions Chill Journalists and Their Sources

1. **Unauthorized disclosures in recent months have unearthed massive, and previously little-known, U.S. state surveillance programs that should have been the subject of public debate before they were approved and should be subject to effective democratic oversight mechanisms.** These disclosures were made by a U.S. government contractor and consisted largely of classified documents from the National Security Agency. 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, fraud and waste, and other information of public interest.[6]

2. 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. As 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 since World War II.

3. Further, those who have received, or were suspected of receiving, unauthorized disclosures – including journalists – have faced sanctions or intimidation. They have in some instances been subject to targeted surveillance and threatened with prosecution, ordered to disclose their sources, or been penalized for the refusal to do so. In connection with one leak investigation, the Obama Administration argued that the journalist who received the allegedly leaked information must testify, a position initially rejected by the trial court and then upheld by an appellate court. In connection with another investigation, prosecutors monitored a journalist including by tracking his phone records and engagements at the State Department, and issuing search warrants for his e-mail communications. It also labeled the journalist a "co-conspirator and/or aider and abettor," but did not indict him. Further, while the government has not attempted to prosecute "traditional" journalists thus far, the secret

[6] Julie Tate, *Judge sentences Bradley Manning to 35 years*, Washington Post, August 21, 2013. Jane Mayer, *The Secret Sharer*, THE NEW YORKER, May 23, 2011. Scott Shane, *U.S. Analyst Is Indicted in Leak Case*, N.Y. Times, August 27, 2010.

grand jury investigation of Julian Assange suggests that the government may try to prosecute him and others who disclose information publicly via the internet.

4. Moreover, during an investigation of the alleged leak to the Associated Press of information related to the purported CIA unraveling of an Al Qaeda plot, the Department of Justice secretly subpoenaed two months of communications records of more than 20 Associated Press phone lines. The Newspaper Guild of Communications Workers of America called the subpoena "egregious and a direct attack on journalists."[7]

5. Following growing outrage over the government's incursions on media freedom, 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.[8] 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.[9]

6. While no journalist has thus far been prosecuted under the Espionage Act, the aggressive enforcement of unauthorized disclosures creates a real threat. New York Times journalist Mark Mazzetti 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."[10] Veteran national security journalist Jane Mayer has asserted that national security disclosures have come to a "standstill."[11]

Article 19 Requires Limited Penalties for Unauthorised Disclosures

7. International law requires limited restrictions on freedom of expression and access to information. The severe and increasingly frequent sanctions in the U.S. for public servants in the security sector who disclose information in the public interest raise concerns about U.S. government compliance with its international law obligations,

[7] Alejandro Martinez, U.S. government secretly obtains phone records from AP reporters, editors, Journalism in the Americas blog, May 14, 2013.

[8] 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.

[9] Charlie Savage, Court Tells Reporter to Testify in Case of Leaked C.I.A. Data, N.Y. Times, July 19, 2013. Charlie Savage and Jonathan Weisman, Holder Faces New Round of Criticism After Leak Inquiries, N.Y. Times, May 29, 2013.

[10] 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.

[11] See generally Molly Redden, Is the 'Chilling Effect' Real? National security reporters on the impact of federal scrutiny, The New Republic, May 15, 2013.

found in Article 19 of the ICCPR, to protect freedom of expression and the public right of access to information. As this Committee made clear in its General Comment 34 on Article 19, while national security may justify legitimate restrictions on the public's right to access information when certain conditions are met, restrictions to the right, including the right of access to information, must be limited, well-founded, prescribed by law, necessary and proportionate, and the least restrictive means for achieving the legitimate aim.[12] For a restriction on freedom of information to be proportionate, the public authority must demonstrate that there is harm to a legitimate interest which is greater than the public interest impeded.[13]

8. National security must not be a pretext for unjust restrictions.[14] As this Committee has stated, 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.[15]

9. The Tshwane Principles acknowledge that governments may legitimately withhold information that falls into certain narrowly defined categories, such as defence plans, weapons development, and the operations and sources used by intelligence services.[16] 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 demonstrate that there is a "risk of harm" from disclosure of identifiable information.[17]

10. The right of the public to access information requires states to limit penalties for the unauthorized receipt, possession or disclosure of information.[18] Where the public interest in disclosure of information outweighs the harm from disclosure, disclosure by public servants should not be subject to penalties.[19] This Committee has stated authoritatively that it is not compatible with Article 19(3) of the ICCPR for a state to

[12] UN Human Rights Committee, General Comment No. 34 on Article 19, UN Doc. CCPR/C/GC/34, September 12, 2011 ("General Comment No. 34"), para. 11.

[13] 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).

[14] *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").

[15] *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, para. 30.

[16] Tshwane Principles, Principle 9.

[17] *Ibid.*, Principle 4.

[18] 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.

[19] General Comment No. 34, para. 30.

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."[20]

11. 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 public interest in disclosure outweighed the harm and efforts to seek remedies for the wrongdoing through official channels would have been ineffective.[21]

12. In *Guja v. Moldova*, the Grand Chamber recognized "little scope … for restrictions on debate on questions of public interest," and 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."[22] In *Bucur v. Romania*, 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.[23]

13. The Tshwane Principles recommend protection against any form of sanction or penalty for the disclosure of wrongdoing.[24] 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 defence, similar to the analysis found in European Court jurisprudence, if the public interest in the disclosure of the information outweighs the harm in its disclosure.[25] 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.[26]

---

[20] General Comment No. 34, 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.

[21] *Guja v. Moldova*, ECtHR (GC), February 12, 2008, para. 73-77. *Bucur v. Romania*, ECtHR, January 8, 2013, paras. 95-119. *See also Palamara-Iribarne v. Chile*, IACtHR, 22 November 2005, para. 88.

[22] *Guja v. Moldova*, para. 74.

[23] *Bucur v. Romania*, paras. 115, 120.

[24] Tshwane Principles, Principles 39-41, 43.

[25] *Ibid*., Principle 43.

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

14. Further, disclosure of such information by the media or other members of the public should not be punished. The primary, or exclusive, responsibility to protect the confidentiality of government information, when confidentiality is justified, lies with the State. As affirmed in a 2004 Joint Declaration on Access to Information and Security Legislation by the three international rapporteurs on freedom of expression (for the UN, OAS, and OSCE): 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."[27]

15. Members of the media and other public watchdogs must be permitted to both investigate and publish information of public interest, including information held by the security sector, without intimidation or improper surveillance, and also to protect their sources.[28] Thus, this 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.[29]

16. This requires adequate protection for members of the public, including journalists, who possess or disclose information related to national security.[30] Sanctions or the threat of sanctions against members of the media for disclosing information may chill others from releasing information in the public interest, thereby effectively undermining their vital role and function.[31]

17. 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, stated:

> 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

[27] 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.

[28] *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.

[29] General Comment No. 34, 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.

[30] 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").

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

> … 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.[32]

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.[33]

18. The public's interest in disclosure is heightened where the information concerns wrongdoing, and inviolable where it concerns gross human rights violations or serious violations of international humanitarian law.[34] However, the public interest in disclosure extends beyond simply where there is demonstrated wrongdoing. As affirmed by the European Court of Human Rights, "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."[35]

U.S. Espionage Act Violates Article 19

19. U.S. law concerning penalties for unauthorized disclosures of national security information, largely governed by the U.S. Espionage Act, is non-compliant with international legal standards and deviates from trends of good practice among democratic states.

    a. First, the offences are vague and overbroad, and lack requisite intent and harm requirements. 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 a broader reading. The Espionage Act offences 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. The Espionage Act lacks requirements of the proof of the actuality or

[32] 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.

[33] Morton Halperin, *Criminal Penalties for Disclosing Classified Information to the Press in the United States*, 2012, , 1. Tshwane Principles, 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 ("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.").

[34] 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.

[35] *Guja v. Moldova*, paras. 72, 74.

likelihood of harm as an element of any offence that could be applied to the receipt, possession or disclosure of information;[36] or the 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.[37] The broad reading of the Espionage Act is inconsistent with international law.

b. Second, the offences 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. There is nothing in the Espionage Act or related laws that provide for exceptions for disclosures in the public interest, including disclosures concerning human rights violations or violations of international humanitarian law. The improper classification of the information disclosed is also not clearly a defence under the text of the law. U.S. whistleblower protections are also limited and do not protect security sector employees who disclose information concerning wrongdoing or other information in the public interest.[38]

c. Moreover, for most offenses, the Espionage Act 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. The First Amendment provides some protections for the media and the public, but the Espionage Act makes no distinctions. 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.

d. Further, U.S. law criminalizes conspiracy to commit an offence at the same level as the actual offence, without sufficient protections for journalists or public watchdogs. 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 the performance of their professional obligations – seeking information from

[36] General Comment No. 34, para. 30. *Guja v. Moldova*, para. 76. *Bucur v. Romania*, paras. 114-15.

[37] For the offence 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.

[38] Public disclosures are never protected under U.S. law, even if internal 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, 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.

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.

e. U.S. law also criminalizes, with significant penalties, the unauthorized *possession* of classified or national defence 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.[39] 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.

f. Finally, the penalties for unauthorized possession and disclosure under U.S. law are disproportionately severe, with chilling effects. 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.[40] U.S. law includes criminal penalties that are more severe than the laws of many other democratic countries.[41] They are also more broadly applicable with fewer protections and limitations.

20. Given the vagueness and over-breadth of some of their terms, the lack of a harm test, and the inapplicability of public interest defences, these provisions and their associated penalties have an unacceptable chilling effect on freedom of expression. Indeed, the government has repeatedly emphasized that this is the intention.[42] 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.

---

[39] Tshwane Principles, Principle 47.

[40] *Guja v. Moldova*, 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*, para. 119.

[41] 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. Penalties for mere *possession* of classified information are generally substantially less, if they exist at all. 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.

[42] *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 Defence 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.").

21. For the reasons described above, the U.S. law provisions concerning offences 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.

22. Public scrutiny of state activities, including in the security sector, safeguards against abuse by public officials and ensures democratic participation and oversight of policymaking 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. Public access to government information concerning the security sector is essential to counterbalance the state's great powers to wage war and counterterrorism operations, conduct surveillance, detain and interrogate persons; and its oversight of significant public funds.[43]

[43] *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 defence and international affairs may lie in an enlightened citizenry – in an informed and critical public opinion which alone can here protect the values of democratic government."). *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").

E-mail: info@justiceinitiative.org
www.justiceinitiative.org