Human Rights Watch Statement on US Protection of Whistleblowers in the Security Sector

The recent public disclosures of US National Security Agency (NSA) dragnet surveillance have given new urgency to an important global debate on what controls are needed to ensure that the rights of people everywhere to privacy, expression, information and association are adequately protected.[1] This debate has been long in gaining prominence, in large part due to the excessive secrecy that shrouds both the security programs and their government oversight. It has taken leaks of classified information to inform the public of the extraordinary scope of NSA surveillance and galvanize political interest in reforms.

The government is entitled to protect sensitive information, and not all leaks deserve protection. However, whistleblowers are those who reveal misconduct or unethical policies in the public interest, and their important role in keeping government honest is recognized in laws that provide at least some protection from retaliation for their disclosures. Yet in the United States, whistleblowers in the intelligence and national security sectors are highly vulnerable to retaliation should they try to bring serious abuses to light.

Congress has failed to give such whistleblowers effective legal protection for the disclosure of secret information; the Obama administration has aggressively prosecuted them under espionage laws designed for spies acting as agents of a foreign power; and the security agencies have found ways to destroy their careers. Despite this hostility, people have continued to bring forward reports of abuses. They deserve protection for revelations that have weighty public interest, such as widespread violation of human rights.

We believe US authorities should exercise discretion when considering prosecuting such leaks under US laws governing classified information. They should not bring charges against whistleblowers who expose government wrongdoing unless they can make a

[1] "US: Urgent Need for Surveillance Reforms," Human Rights Watch news release, June 11, 2013, http://www.hrw.org/news/2013/06/11/us-urgent-need-surveillance-reforms.

compelling case that the harm to national security caused by the disclosure is so significant that it overrides the public's right to know and are prepared to make that case publicly, providing as much detail as possible on the actual harm.

Any law that respects rights should place the burden of this argument on the government, not the whistleblower, and the simple fact that information is classified should never be sufficient on its own to defeat protection for disclosures that are in the public interest. In particular, the Espionage Act, which was framed to punish the passing of sensitive information to a foreign enemy, should never be distorted beyond its intended purpose and used to punish whistleblowers.

Congress should live up to its responsibility to provide effective protection and meaningful recourse to whistleblowers. To start, it should enact meaningful laws on which they can rely, both to challenge official retaliation and to defend themselves from criminal and civil liability. It should insist on greater disclosure from security agencies and share information concerning the dimensions and modalities of security surveillance with the public. And it should work with the administration to cut back on the overwhelming growth of classified information and protect the public's right to know.

Both Congress and the Obama administration should rethink surveillance programs and reform them to ensure that they intrude no more than necessary on the private communications of all people, not just US citizens. The United States has been a strong proponent of Internet freedom, but it risks its reputation when it fails to respect the rights of Internet and phone users.

Human Rights Basis for Whistleblower Protection

Legal protection for government employees who, in the public interest, disclose wrongdoing is a relatively new practice in many countries. Such "whistleblower" laws are often narrowly drawn around specific unlawful acts and notification procedures, and even the best are not always effective in shielding those who disclose wrongdoing from all negative consequences. Yet however imperfect these protections are, they are scant to

non-existent for government employees in the security sector who divulge classified information to the media in an effort to bring wrongs to public attention.[2]

From a human rights perspective, the punishment of those who leak security information can be problematic because it suppresses information that may be vital for the exercise and protection of human rights. Some of the most significant revelations of human rights violations come from disclosures of once-secret information relating to the misconduct of security agencies.

The value of public revelation is only deepened by a disturbing tendency of governments to over-classify official information[3] and to characterize as vital to "national security" interests that fall far beyond protecting a country from the use or threat of force. The well-known Johannesburg Principles on National Security, Freedom of Expression and Access to Information state:

> In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions.[4]

International law requires that any restriction of speech be consistent with the protection of rights in a democratic society and no greater than what is necessary to protect interests such as national security. The International Covenant on Civil and Political Rights, to which the United States is a party, provides in article 19:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all

---

[2] See generally Benjamin S. Buckland and Aidan Wills (DCAF), "Blowing in the Wind? Whistleblower Protection in the Security Sector" (working draft, September 2012), http://www.right2info.org/resources/publications/pretoria-finalization-meeting-april-2013-documents/whistleblowing-and-security-sector-buckland-and-wills/view].

[3] See Elizabeth Goitein, "A Mixed Message for National Security Whistleblowers," Huff Post Politics Blog, December 22, 2012, http://www.huffingtonpost.com/elizabeth-goitein/obama-whistleblowers_b_1989629.html.

[4] See Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1996, principle 2(b), http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.

> kinds, regardless of frontiers…. [The exercise of these rights may] be subject to certain restrictions, but these shall only be such as are provided by law and are necessary….[f]or the protection of national security.

The United Nations Human Rights Committee, in General Comment No. 34 interpreting this article, has noted that governments must take "extreme care" to ensure that laws relating to national security are not invoked "to suppress or withhold from the public information of legitimate public interest that does not harm national security" or to prosecute journalists, researchers, activists, or others who disseminate such information.[5]

A new set of standards based on best practices and human rights law deals with the problem of national security whistleblowers in detail. The Tshwane Principles, released June 12, 2013, were developed through broad consultation with civil society, academia, government security officials, and UN experts on expression, media, and counter-terrorism. They outline circumstances where the person who discloses classified security information of important public concern should be explicitly protected from punishment or retaliation, and recommend that governments provide both internal complaint mechanisms as well as independent oversight bodies to which such disclosures can be made confidentially.[6] Even if internal mechanisms exist, disclosures should be protected if the internal process is ineffective or if the leaker reasonably believes that resorting to the internal procedures would result in concealment of wrongdoing, destruction of evidence, retaliation, or an imminent risk of harm.[7] The actual motive of the person making disclosures is irrelevant, so long as the person has a reasonable belief that the public interest in having the wrong exposed outweighs the harm in disclosure.[8] Even if the whistleblower reveals more information than is necessary to expose a wrong, that person should be protected from retaliation unless the harm outweighs the public's interest in these disclosures. Because

---

[5] Human Rights Committee, General Comment No. 34, Freedoms of opinion and expression, September 12, 2011, CCPR/C/GC/3, para. 30, http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf.

[6] Global Principles on National Security and the Right to Information ("The Tshwane Principles"), particularly Part VI: Public Interest Disclosures by Public Personnel, released June 12, 2013, http://www.opensocietyfoundations.org/sites/default/files/Global%20Principles%20on%20National%20Security%20and%20the%20Right%20to%20Information%20%28Tshwane%20Principles%29%20-%20June%202013.pdf. While the Tshwane Principles list discrete grounds for protected disclosures at principle 37, it is the view of Human Rights Watch that these should be considered illustrative of the sorts of weighty public interests which merit protection, and not an exclusive enumeration, particularly in view of the evolving understanding of human rights and threats to individual dignity and security.

[7] See Tshwane Principles, principle 40.

[8] See ibid., principles 38(b) and (c) and 40(c).

the government has the greater power of investigation, it should bear the burden of proving a case for sanction, and the whistleblower should always have recourse in any adjudicative proceeding to a public interest defense that requires prosecutorial and judicial authorities to consider the extent and risk of actual harm threatened.[9]

Lack of Whistleblower Protection for Disclosure of National Security Information in the US

Government whistleblowers who reveal classified information have little protection in the United States, a problem that, while flagged by experts for years,[10] has taken on great urgency in the face of aggressive prosecution policies under the Obama administration. Security whistleblowers have tried to expose a variety of problems, from mismanagement of surveillance programs, to botched secret operations, wrongful or criminal conduct, or unethical government policies. In some cases whistleblowers have made great efforts to use internal processes, such as reporting problems to others within their agency, to the inspector general for the Department of Defense, or to congressional oversight committees, but with little protection from retaliation and with little immediate result; in other cases, they went straight to the media. The Obama administration has charged more security sector employees who passed information to the media with violation of the Espionage Act than all previous US administrations combined.

The federal Whistleblower Protection Act exempts from its protections whistleblowers in the intelligence community, including defense contractors. The most legal protection on which such employees can rely is the Intelligence Community Whistleblower Protection Act, which provides a channel for whistleblowers to take matters of "urgent concern" first to the inspector general of the Department of Justice and then to a congressional intelligence oversight committee. However, this law does not provide any legal right of action for such whistleblowers to protect themselves against retaliation for reporting their concerns in these ways, and in practice, even continuing access to congressional committees can be

---

[9] See ibid., principles 40(b)(note) and 43.

[10] Various organizations have produced useful reports and recommendations on this topic. See, e.g., Goodman, Crump, and Corris, *Disavowed: The Government's Unchecked Retaliation against National Security* Whistleblowers American Civil Liberties Union, 2007, https://www.aclu.org/pdfs/safefree/disavowed_report.pdf; German and Stanley, *Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Secret Security Establishment,* American Civil Liberties Union, July 2011, http://www.aclu.org/files/assets/secrecyreport_20110727.pdf; National Whistleblowers Center, "National Security Whistleblowers Not Effectively Protected by New Presidential Directive," October 11, 2012, http://www.whistleblowers.org/index.php?option=com_content&task=view&id=1426&Itemid=229.

thwarted by agency heads, who usually can identify the whistleblower concerned.[11] In October 2012, the Obama administration released a Presidential Policy Directive (PPD-19) intended to bolster protection for national security whistleblowers; it requires agencies to establish a process by which whistleblowers can seek review of prohibited retaliatory actions. The directive was widely criticized as window-dressing, however, because it explicitly denies whistleblowers the ability to obtain legal enforcement of any rights or procedures set forth under the directive.[12]

The case of the "NSA Four" is illustrative of the effective lack of protection. Bill Binney, Kirk Wiebe, Ed Loomis, and Thomas Drake were all targets of a leak investigation beginning in 2007, following a *New York Times* report on the Bush administration's warrantless wiretapping programs.[13] Each had years earlier tried to bring attention to waste and mismanagement in the NSA's spending billions of dollars on a failed signals intelligence system, Trailblazer, when a much cheaper and more effective one, ThinThread, was at hand. Because they had earlier voiced their concerns internally, to Congress and the inspector general, each suffered retaliation from the government and later was included among the targets of an expansive FBI investigation based on the *New York Times* report, including gunpoint raids on their homes. Drake was charged with leaking documents under the Espionage Act, charges that ultimately collapsed.

The Espionage Act, drafted in 1917, makes it a serious crime for anyone in possession of various sorts of "national defense" documents (interpreted to include all classified documents) to communicate them to someone not entitled to possess them; likewise it is a criminal offense to communicate national defense "information" to one not authorized to receive it if the leaker has reason to believe it "could be used to the injury of the United

---

[11] See Goodman, Crump, and Corris, *Disavowed*, ACLU, 2007.

[12] See, e.g., National Whistleblower Center Press Release, "National Security Whistleblowers Not Effectively Protected by New White House Directive: Directive Lacks Due Process and Real Legal Protections," October 11, 2012, http://www.whistleblowers.org/index.php?option=com_content&task=view&id=1426&Itemid=229.

[13] For various accounts, see Tim Shorrock, "Obama's Crackdown on Whistleblowers," *The Nation*, March 26, 2013, http://www.thenation.com/article/173521/obamas-crackdown-whistleblowers?page=0,0#axzz2WOp5gTDi; Government Accountability Project, "NSA Domestic Spying Revelation Vindicates GAP Clients, June 6, 2013, http://www.whistleblower.org/press/press-release-archive/2013/2745-nsa-domestic-spying-revelation-vindicates-gap-clients; Kelley B. Vlahos, "Diane Roark talks NSA retribution," Ladies of Liberty Alliance, September 18, 2012 , http://www.iamlola.org/posts/diane-roark-talks-nsa-retribution (accessed June 18, 2013). For a roundtable discussion of Edward Snowden's role and revelations as a whistleblower by Drake, Binney, and Wiebe, see Peter Eisler and Susan Page, "3 NSA veterans speak out on whistleblower: We told you so," *USA Today*, June 16, 2013, http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/.

States or to the advantage of any foreign nation."[14] While various administrations have tended to assert a literal reading of the statute, many others believe its sweeping wording must be interpreted in light of the US Constitution's free speech protections, particularly given the enormous amounts of information that are classified without compelling reason. This would mean that the government must show not just a disclosure, but also that the leaker made the disclosure in bad faith, and demonstrate that the harm to national security posed by the disclosure outweighs the public interest in the information.[15]

US soldier Bradley Manning, who leaked tens of thousands of documents to the media organization Wikileaks, at least some of which exposed wrongdoing and serious human rights abuses, is the latest security leaker to be prosecuted under the Espionage Act, despite having pled guilty to other offenses that would subject him to 20 years' imprisonment. The court in the ongoing Espionage Act case ruled that the government would have to prove beyond a reasonable doubt that Manning had reason to believe that the material transmitted to Wikileaks would aid the enemy. Disturbingly, the prosecution has argued that knowingly releasing classified documents to a public website was enough because Manning should have known that enemies such as Osama Bin Laden read Wikileaks postings, as did millions of other people. Should this interpretation prevail, it could swallow First Amendment free speech consideration whole, as information of interest to enemies is sometimes also crucial for the public in a democracy to know. In the context of the Internet, any public disclosure might eventually become available to an enemy, but the public accessibility of information alone should not overcome First Amendment protections.

NSA Surveillance Disclosures: A Perfect Storm

There is no doubt that the substance of the latest disclosures made by Edward Snowden of massive NSA data collection from Verizon, and the cooperation of major communications companies in the NSA's intelligence-gathering,[16] is a matter of widespread public interest.

---

[14] See offenses enumerated at 18 U.S.C. sec. 793.

[15] See Morton H. Halperin, "Criminal Penalties for Disclosing Classified Information to the Press in the United States," http://www.right2info.org/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf (accessed June 18, 2013).

[16] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations," *Guardian*, June 9, 2013, http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed June 18, 2013). See also Barton Gellman, Aaron Blake and Greg Miller, "Edward Snowden comes

President Obama himself has welcomed debate on the balance between privacy and security.[17] These disclosures have already impelled legislators to introduce bills to limit the secrecy of the Foreign Intelligence Service Act processes; prompted new revelations on the scope of dragnet surveillance orders and the evolution of these practices[18]; and prompted the NSA to disclose more to legislators who have expressed surprise that surveillance exceeds even what has been publicly exposed.[19] The story of how the present policies evolved from contested actions of the Bush administration continues to unfold.

Yet even had no public storm ensued, disclosures of this nature fall squarely within the most serious concerns of a democratic polity and all concerned with human rights globally. The rights violated by mass surveillance are not only the privacy of millions of people who themselves were not a target of investigation, but also freedom of expression, which is chilled by official monitoring. Surveillance can also set the stage for many other potential rights violations, particularly when data is retained indefinitely and authority and limitations on search are not public. In April 2013, the UN special rapporteur on freedom of expression and information called attention to the particular threat to rights of unchecked access of states to communications data held by third party providers:

> When accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone. By combining information about relationships, location, identity and activity, States are

---

forward as source of NSA leaks," *Washington Post*, June 9, 2013, http://articles.washingtonpost.com/2013-06-09/politics/39856642_1_extradition-nsa-leaks-disclosures (accessed June 18, 2013).

[17] "Transcript: Obama's Remarks on NSA Controversy," Wall Street Journal, June 7, 2013, http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/ (accessed June 18, 2013).

[18] Barton Gellman, "U.S. surveillance architecture includes collection of revealing Internet, phone metadata," *Washington Post*, June 15, 2013, http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html (accessed June 18, 2013).

[19] Daniel Strauss, "NSA revelations only 'tip of the Iceberg' says Dem lawmaker," *The Hill*, http://thehill.com/video/house/305047-dem-rep-lawmakers-learned-significantly-more-about-surveillance-programs-in-nsa-briefing (accessed June 18, 2013). Rep. Loretta Sanchez was quoted as saying most lawmakers at the briefing were "astounded" that programs are much broader than what the public has heard.

> able to track the movement of individuals and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with.[20]

In the United States, a complex set of circumstances have rendered the data surveillance policies of the government invisible and impervious to public oversight. Extremely broad interpretations of the Foreign Intelligence Surveillance Act and the USA PATRIOT Act have resulted in secret court approval of sweeping surveillance measures that are arguably far beyond the intent of Congress and the boundaries of US human rights obligations. Congressional oversight of the administration is limited to a small number of legislators, who have been prohibited from disclosing the reports they receive, and who often have not received information from security agencies that claim the information is too sensitive to share. The administration has pressed the state secrets privilege to block court consideration of disclosed national security abuses, and prosecuted leakers more aggressively than any of its predecessors. As noted above, Human Rights Watch is particularly disturbed by the US government's repeated resort to the Espionage Act, a law aimed at spies and saboteurs, against security sector whistleblowers who leak classified information to the media.

Given the common problem of over-classification, and the weak to non-existent protections for security sector whistleblowers, the US government should be prepared to balance the actual harms threatened to national security against the public's strong interest in revelation of wrongdoing, both when it crafts and when it enforces laws on non-disclosure of classified information. Means of internal complaint and independent oversight should always be available, but it should also be recognized that confidential government complaint mechanisms can be ineffective in the face of a pervasive regime of secrecy, high-level approval of the problem, or even bureaucratic inertia. For this reason, disclosure of information to the public should be a potentially defensible option, particularly when other ways of disclosing wrongdoing would be ineffective. A government always has discretion to refrain from prosecution, and it should exercise that discretion

[20] Report of the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, April 17, 2013, A/HRC/23/40, para. 43 (omitting citation), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

with a view towards protecting democratic oversight and preventing serious human rights abuses.

In the case of Edward Snowden, the material he has reportedly shared so far with the *Guardian* and the *Washington Post*[21] has revealed that US agencies have exploited security laws to conduct massive data surveillance that intruded on the rights of millions of people around the world, including many US citizens. Companies, courts, and congressional representatives have been gagged from disclosing anything about these surveillance programs, including the scope of the data collected, how long the government retains it, how and by whom it is searched, and what limits, if any, are placed on these programs. This utter lack of transparency and accountability to the public could easily pave the way for further serious human rights abuses and an erosion of democratic governance. The public's interest in knowing the dimensions of this secret practice, conducted without effective public oversight or check, is extremely high.

It is often difficult for those outside the government to assess the full impact of disclosures on national security, particularly when more revelations may be forthcoming. But the disclosures so far appear to have limited, if any, impact on national security, despite administration claims that they are serious. Ultimately, the burden should be on the US government to make the case that the disclosure actually created a genuine risk of serious and identifiable harm to national security, and that such harm outweighs the value of the disclosures to the public.

Moving Forward to Protect Whistleblowers and Democratic Accountability

In light of these specific facts, Human Rights Watch urges the Obama administration not to prosecute Edward Snowden or other national security whistleblowers until it is prepared to explain to the public, in as much detail as possible, what the concrete and specific harms to national security his disclosures have caused, and why they outweigh the public's right to know. If the administration truly welcomes a debate on issues of privacy, rights, and security, as President Obama has said it does, then prosecuting the man who sparked the debate is not the way to show it.

---

[21] See Greenwald, MacAskill, and Poitras, "Edward Snowden," *Guardian*; and Gellman, Blake and Miller, "Edward Snowden comes forward," *Washington Post*.

In addition, the government should cease using the Espionage Act to charge those who disclose classified information to the public that shows wrongdoing or unethical government programs or policies. In this regard, we note that the penalties for disclosures under the Espionage Act, whose charges carry 10-year prison terms, are significantly heavier than what many other democracies impose on government agents who expose secrets, and that the European Court of Human Rights has ruled in favor of protecting security sector whistleblowers when the public interest in their disclosures outweighs other important state interests.[22]

Finally, Congress should provide effective protections for confidential disclosures and legal rights that security sector whistleblowers can invoke in case of retaliation. Congress has authority to demand greater transparency from the executive branch, and to inform citizens of the scope of secret surveillance programs. It should set firm limits on not only what sort of data may be collected for what purpose, but also how long the NSA and other agencies may retain data not directly connected to an ongoing investigation. All branches of government have a responsibility to minimize the amount of information that is withheld from the public, so that the functioning of government does not have to rely on leaks to be visible to the governed.

[22] See Sandra Coliver, "National Security Whistleblowers: The US Response to Manning and Snowden Examined," Voices, Open Society Foundations, June 12, 2013, http://www.opensocietyfoundations.org/voices/national-security-whistleblowers-us-response-manning-and-snowden-examined (comparing US practices to those of many European Union states. Coliver also highlights the Grand Chamber of the European Court of Human Rights decision in *Guja v. Moldava,* February 12, 2008 (http://echr.ketse.com/doc/14277.04-en-20080212/view/), finding a violation of freedom of expression in the firing of a civil servant who revealed to a newspaper evidence of political interference with the administration of justice, and the January 8, 2013, European Court of Human Rights decision in *Bucur et Toma c. Romanie*, where the court found a violation of freedom of expression in the criminal conviction of an analyst in Romania's Intelligence Service who exposed irregularities and overbreadth in telephone wiretapping). Judgment available in French at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-115844; synopsis in English at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=002-7395.