# Re: Call for comments on the protection of sources and whistleblowers

Dear Special Rapporteur Kaye:

I appreciate this opportunity to comment on the protections available to whistleblowers, those individuals exposing human rights violations, corruption and other abuses. As an independent security researcher working at the intersection of technology, law and policy, I teach digital security to journalists and help media organizations improve their security posture.

In this comment I will provide examples of how states breach source anonymity in practice even where it is provided for in law; how whistleblowers face retaliation even when using proper channels; and how source protection has gone from being a legal matter to being a technical challenge.

## States breach source anonymity in practice even where it is provided for in law

In 2013 the EU parliamentary committee on Organised Crime, Corruption, and Money Laundering called for[1] the creation of a legislative proposal establishing an effective, comprehensive and cross-border European whistleblower protection program. The European Commission rejected the request and asked *Transparency International* (TI) to write an in-depth report[2] on whistleblower legislation among EU member states.

The report notes that while many EU countries have at least partial legal protections for individuals exposing various types of abuse, the provisions that are in place contain loopholes and exceptions. One example is laws that cover only one employment category. The result, writes TI, "*is that employees who believe they are protected from retaliation could discover, after they blow the whistle, that they actually have no legal recourse.*"

The ratings in the report do not take into consideration how well or whether a country's whistleblower laws and regulations work *in practice.* As noted in your report on the promotion and protection of the right to freedom of opinion and expression[3], many countries recognize the lawfulness of maintaining the anonymity of sources. Over time, however, pressure on groups such as journalists may undermine such protections.

Despite providing for source anonymity in law, corporations and states break source anonymity in practice. A breach of source anonymity under the guise of national security is still a breach of source anonymity, and many news articles have been written on this topic. For instance, here are nine concrete examples from Sweden, Norway, the United Kingdom and the United States.

**Sweden**

Sweden extends broad freedoms to its citizens to report wrongdoing to government authorities and the media - so much so that retaliating against a whistleblower in the public sector is considered a criminal offence[4].

In December 2010[5] the *Equality Ombudsman*, a Swedish government agency tasked with supervising laws relating to discrimination, was suspected of investigating sources in a case involving an energy company. The agency was investigated for press freedom violations, but the case was dropped in May 2011.

In February 2015[6] the Head of Security at the National Agency for Social Insurance was found to have breached the law of source anonymity when he attempted to identify the sources used by Expressen, a Swedish newspaper, for an investigative piece about the agency. He was given a 30.000 SEK fine.

**Norway**

The Norwegian *Working Environment Act*[7] affords all workers, in both public and private sectors, a statutory right to notify wrongdoing and requires employers to develop internal reporting procedures. Retaliation against an employee who notifies pursuant to this act is prohibited, and anyone who has been subjected to retaliation may claim compensation.

In 2014[8] a homicide detective feared a case he was working on had been closed too soon. He voiced his concerns to his superiors and requested further investigation, but was told to drop the matter. The case was not reopened until after the detective went public with his findings. The detective later changed roles and was promoted to superintendent.

Every now and then, we see examples of situations where the journalist receiving the leaked material is more in need of protection than the source. The Norwegian *Dispute Act*[9] and the *Criminal Procedure Act*[10] state that a newspaper editor can refuse to name her source. Other persons who have acquired knowledge of the source through their work with the publishers, editors, press agency or printing office in question have the same right as the editor.

In 2007[11] a journalist had his documents and notes seized as he went through a security checkpoint at a court house. Despite arguing his right to protect his sources, police officers held on to - and read - the documents for about an hour. The Parliamentary Ombudsman did not issue a public statement about the incident until 2011.

In June 2015[12] officers from the Norwegian Police Security Service seized material from a documentary filmmaker as part of an ongoing investigation into Islamist groups in Norway. The filmmaker had begun working on this project in January 2014, and the documentary was nearing completion.

**United Kingdom**

The United Kingdom has one of the most comprehensive whistleblower protection laws in the world, according to the report by TI. The *Public Interest Disclosure Act*[13] applies to the majority of workers across all sectors and covers a range of employment categories. The law, however, does not cover those who receive, carry or store the leaked material.

In August 2013, UK authorities detained David Miranda[14], the partner of journalist Glenn Greenwald, as he was passing through Heathrow airport and questioned him under schedule 7 of the *Terrorism Act 2000.* He was held for nine hours, the maximum the law allows before officers must release or formally arrest the individual.

That same month, the government ordered The Guardian[15] to destroy computer hard drives containing copies of some of the material provided by NSA whistleblower Edward Snowden. The order was served in an attempt to stop reporting on the secret files.

In December 2013, The Guardian's editor-in-chief, Alan Rusbridger, found himself the subject of extraordinary questioning[16] during a session of the Home Affairs Select Committee as MPs probed the circumstances surrounding the newspaper's disclosure of the files. In one exchange, Keith Vaz, the committee's chairman, asked Rusbridger if he loved his country.

**United States**

According to a 2013 report[17] from the Government Accountability Project on the existing whistleblower protections found throughout Europe, the US has a comprehensive whistleblower protection regime. While the protections may seem impressive on paper, the media continues to publish articles documenting the government's hunt for sources and retaliation against journalists who publish leaked material.

In May 2015 Chelsea Manning, a soldier serving a 35-year sentence for leaking state secrets, wrote a comment article[18] on citizens' right to criticize the government without fear. In the article, Manning stated that the current administration has launched "*more national security and criminal investigations into journalists and prosecutions of their sources than at any other time in the nation's memory.*"

Further, Manning also proposed a bill[19] that would extend protections against prosecution to anyone engaging in journalism and rein in the Espionage Act that has been used by the administration to prosecute whistleblowers. Manning used Twitter to announce the proposed *National Integrity and Free Speech Protection Act* (NIFSPA), and has since encouraged Americans to lobby for the bill.

## Whistleblowers face retaliation even when using proper channels

Ever since the first leak by Edward Snowden in June 2013, politicians and government officials have been making statements about how whistleblowers should go through "proper channels." Yet, here are three cases documenting more than a dozen whistleblowers who did use "proper channels" and still faced retaliation:

In 2014 the Government Accountability Project published a report[20] detailing ten representative whistleblower cases from the United Nations and its funds, programs and agencies. The sample cases mentioned in the report demonstrate how the whistleblower policies are implemented in practice and show that retaliation does happen, even in the UN.

In May 2015 former CIA officer Jeffrey Sterling was sentenced to three and a half years in prison for violating the Espionage Act. Sterling's battle[21] against the government began more than 15 years ago when he was fired by the CIA after filing a racial discrimination complaint. He later filed two federal lawsuits against the agency, one for retaliation and discrimination, another for obstructing the publication of his autobiography. He also spoke as a whistleblower to Congress to let them know his concerns about the mismanagement of a classified program he worked on at the agency.

In June 2015 the Senate Committee on Homeland Security and Governmental Affairs held a hearing[22] where whistleblowers testified about retaliation they experienced after making protected disclosures to members of Congress. One whistleblower said the Army suspended his clearance, removed him from his job, launched a criminal investigation and deleted his retirement orders.

## Source protection has gone from being a legal matter to being a technical challenge

Most journalists feel an obligation to protect their confidential sources, but a verbal or written promise of anonymity is not enough in today's world. The Secretary General for the Norwegian Press Association, Kjersti Løken Stavrum, has accurately stated[23] that "*source protection has gone from being a legal matter to being a technical challenge.*" Here are three examples illustrating how technological mishaps can have a negative impact on source protection:

In 2009 the Department of Justice began investigating[24] Stephen Jin-Woo Kim, a State Department Contractor, for leaking classified information about North Korea to Fox News reporter James Rosen. In its investigation, it monitored Rosen by tracking his visits to the State Department and the timing of calls and his personal email.

In December 2012 VICE.com found itself at the center of a media storm when it forgot[25] to scrub metadata from a photo accompanying an article about the fugitive millionaire John McAfee. The photo contained the GPS location data embedded by the iPhone 4S that took it.

In 2012 Norwegian law enforcement began investigating a lawyer for leaking documents concerning the 2011 Norway attacks to the media. Phone logs were presented as evidence[26] during the trial to show that the lawyer had repeatedly been in contact with at least one journalist. The lawyer was found guilty of leaking the documents and lost his license to practice law.

## Conclusion

Journalists rely on encryption and anonymity to protect themselves, their sources and the information that they receive. No whistleblower or journalistic source is safe if states impose any restrictions on the use of encryption, such as by inserting backdoors into or criminialzing the use of secure communication tools. A full exploration of the role of media organizations to protect their sources online is likely beyond the scope of this report. However, I implore you to engage states, civil society organizations and corporations in a campaign to bring encryption and privacy by design and default to users - and future whistleblowers - around the world.

Thank you.

Sincerely,

Runa A. Sandvik

---

1. *European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering,* European Parliament, *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0444&language=EN&ring=A7-2013-0307 (June 18 2015)↩
2. *Whistleblowing in Europe,* Transparency International, *available at* https://www.transparency.de/fileadmin/pdfs/Themen/Hinweisgebersysteme/EU_Whistleblower_Report_final_web.pdf (June 18 2015)↩
3. *Report of the Special Rapporteur on freedom of expression,* OHCHR, *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (June 18 2015)↩

4. *Efterforskningsförbudet,* Swedish legal resource, *available at* https://www.sjf.se/yrkesfragor/yttrande-tryckfrihet/efterforskningsforbud (June 18 2015)↩
5. *DO anmäls för brott mot efterforskningsförbud,* Resumé (Swedish), *available at* http://www.resume.se/nyheter/media/2010/12/22/do-jk-anmals-for-brott-mot/ (June 18 2015)↩
6. *Döms för brott mot efterforskningsförbud,* Expressen (Swedish), *available at* http://www.expressen.se/nyheter/doms-for-brott-mot-efterforskningsforbud/ (June 18 2015)↩
7. *Norway – Whistleblowing Protection,* an overview of whistleblowing law in Norway, *available at* https://blueprintforfreespeech.net/document/norway (June 19 2015)↩
8. *Varslet om Monika-saken – sluttet i jobben,* Norwegian Broadcasting Corporation, *available at* http://www.nrk.no/hordaland/varslet-om-monika-saken-_-sluttet-i-jobben-1.12004548 (June 19 2015)↩
9. *The Dispute Act, Section 22-11,* University of Oslo, *available at* http://app.uio.no/ub/ujur/oversatte-lover/data/lov-20050617-090-eng.pdf (June 19 2015)↩
10. *The Criminal Procedure Act, Section 125,* University of Oslo, *available at* http://app.uio.no/ub/ujur/oversatte-lover/data/lov-19810522-025-eng.pdf (June 19 2015)↩
11. *Dagbladet får støtte fra Sivilombudsmannen,* Journalisten (Norwegian), *available at* http://journalisten.no/2011/05/dagbladet-far-stotte-fra-sivilombudsmannen (June 19 2015)↩
12. *PST-razzia hos den prisbelønte filmskaperen Ulrik Imtiaz Rolfsen,* Dagbladet (Norwegian), *available at* http://www.dagbladet.no/2015/06/09/nyheter/innenriks/ulrik_imtiaz_rolfsen/film/dokumentarfilm/39575267/ (June 19 2015)↩
13. *Public Interest Disclosure Act 1998,* UK legal resource, *available at* http://www.legislation.gov.uk/ukpga/1998/23/contents (June 18 2015)↩
14. *Glenn Greenwald's partner detained at Heathrow airport for nine hours,* The Guardian, *available at* http://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow (June 18 2015)↩
15. *NSA files: why the Guardian in London destroyed hard drives of leaked files,* The Guardian, *available at* http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london (June 18 2015)↩
16. *Alan Rusbridger and the home affairs select committee: the key exchanges,* The Guardian, *available at* http://www.theguardian.com/world/2013/dec/03/rusbridger-home-affairs-nsa-key-exchanges (June 18 2015)↩
17. *The Current State of Whistleblowing Law in Europe,* Government Accountability Project, *available at* http://whistleblower.org/sites/default/files/TheCurrentStateofWhistleblowerLawinEurope.pdf (June 20 2015)↩
18. *We're citizens, not subjects. We have the right to criticize government without fear,* The Guardian, *available at* http://www.theguardian.com/commentisfree/2015/may/06/were-citizens-not-subjects-we-have-the-right-to-criticize-government-without-fear (June 20 2015)↩
19. *Chelsea Manning writes bill to protect journalism and curb Espionage Act,* The Guardian, *available at* http://www.theguardian.com/us-news/2015/may/07/chelsea-manning-bill-journalism-espionage-act (June 19 2015)↩
20. *Representative Cases in Which the United Nations or its Funds, Programmes or Agencies have not Complied with Best Practices in Whistleblower Protection,* Government Accountability Project, *available at* http://whistleblower.org/sites/default/files/Representative%20UN%20Cases.pdf (June 20 2015)↩
21. *How Jeffrey Sterling took on the CIA - and lost nearly everything,* The Intercept, *available at* https://firstlook.org/theintercept/2015/06/18/jeffrey-sterling-took-on-the-cia-and-lost-everything/ (June 21 2015)↩
22. *Blowing the Whistle on Retaliation: Accounts of Current and Former Federal Agency Whistleblowers,* Senate Committee on Homeland Security and Governmental Affairs, *available at* http://www.hsgac.senate.gov/hearings/blowing-the-whistle-on-retaliation-accounts-of-current-and-former-federal-

agency-whistleblowers (June 20 2015)↩

23. *Vil at journalistikken skal merkes,* Journalisten (Norwegian), *available at* http://journalisten.no/2014/12/generalsekretaerens-har-ett-nyttarsonske (June 20 2015)↩

24. *Destroyted by the Espionage Act,* The Intercept, *available at* https://firstlook.org/theintercept/2015/02/18/destroyed-by-the-espionage-act/ (June 20 2015)↩

25. *In Pursuit of McAfee, Media Are Part of Story,* The New York Times, *available at* http://www.nytimes.com/2012/12/10/business/media/in-pursuit-of-john-mcafee-media-are-part-of-story.html (June 20 2015)↩

26. *Fare på ferde,* Dagbladet (Norwegian), *available at* http://www.dagbladet.no/2014/02/17/kultur/meninger/hovedkronikk/kronikk/22_juli/31862582/ (June 20 2015)↩