# Under What Circumstances Are Insider Leaks Justified?

Ben Lusher
Public Policy & MBA
University of Michigan

Kathryn Reeves
Public Policy
University of Michigan

Amir Rahmati
Computer Science & Engineering
University of Michigan

## 1 Introduction

Though strategic leaks of classified information have become common way of communicating with the press, in the past several years the news has been dominated by massive, unauthorized releases of intelligence documents. Perhaps the most dramatic case since Daniel Ellsberg and the Pentagon Papers is that of Edward Snowden, whose release of thousands of documents detailing the National Security Agency's (NSA) domestic spying apparatus has led to widespread condemnation and catalyzed an impending overhaul of the agency's intelligence-gathering activities [Sav14].

The reaction to recent cases involving unauthorized disclosures, including Wikileaks and the Snowden case, has revealed both the difficulties and inconsistencies in handling the aftermath of leaks. While Ellsberg had charges dropped based on a technicality [Arn73], Chelsea Manning, the Army private whose disclosures uncovered unauthorized killing of civilians during the Iraq war, was detained for more than three years–with almost ten months in solitary confinement–before she faced a judge and was sentenced to 35 years in prison [Tat13]. Fearing retaliation, Snowden left United States, and has since been granted asylum in Russia.

In addition to the inconsistency in responding to leaks, the debate has shifted in recent years over the extent to which a leaker should face punish-

ment if the disclosure provides evidence of illegal or unconstitutional activity on the part of a government official or agency. Specifically, we must address whether wrongdoing is justification for a leak, and determine how this impacts the treatment of the source. It is vital that the current system balance the need to hold leakers accountable while also protecting the public interest. Moving forward, the U.S. should develop a consistent framework in order to determine the justification of intelligence leaks.

In the following, we will analyze a suggested process for deciding whether an unauthorized disclosure was justified. We will then present a brief case study that focuses on the Snowden disclosures. We will also address issues that, given further consideration, can help provide the foundation for the just treatment of individuals who release classified information to the public.

# 2 Constructing a Framework for Justification

In his book *Secrets and Leaks: The Dilemma of State Secrecy*, Rahul Sagar proposes five conditions that must be met in order for a whistleblower's actions to be deemed justified. Although Sagar's criteria have drawbacks, they present observers with a set of guidelines for deciding whether a leaker's actions were acceptable. When determining justification, future disclosures must meet *all* of the conditions discussed below.

1. **Disclosure must reveal wrongdoing.** Any intelligence leak must directly reveal wrongdoing by a government official or agency. While this condition seems relatively straight forward, it poses questions. Can wrongdoing be defined by the whistleblower? Alternatively, should wrongdoing be limited to actions that are clearly illegal or unconstitutional?

   First, allowing the whistleblower to define wrongdoing sets a dangerous precedent, and would "ignore the fact that there tends to be disagreement over how to balance shared interests" [Sag13]. While a whistleblower may see a government surveillance system as an infringement on privacy, others may see it as a tool for national security. Simply defining wrongdoing as an illegal or unconstitutional act creates an inflexible standard. For example, actions not deemed illegal—such as a government employee discovering that a senior official has asked an agency to perform an audit on a specific interest group — still violate

the idea that government should treat all citizens equally under the law.

Given this issue, Sagar recommends that wrongdoing be defined as the "abuse of public authority" [Sag13]. Such a standard would allow for both legal and moral flexibility, while also providing space for public discourse.

2. **Unauthorized disclosures must be based on clear and convincing evidence.** Because unauthorized disclosures have the potential to impact public safety and national security, whistleblowers are only justified if they can present convincing evidence of wrongdoing to the general public. According to Sagar, hard evidence "can be described as clear and convincing when disinterested observers are likely to draw the same inference from it" [Sag13]. Overall, this condition creates a reasonable standard that must be met in order for justification to be considered.

3. **Unauthorized disclosures should not impose a disproportionate burden on national security.** The third condition assumes that any intelligence leak will impact national security. When classified documents are made public, it is reasonable to conclude that such leaks may alter the strategies of targeted parties. Sagar suggests that "officials ought not to make an unauthorized disclosure with a view of exposing the truth at any cost" [Sag13] and that revelations may create new threats that "outweigh the public's otherwise profound interest in uncovering wrongdoing."

   Although Sagar argues that public security may be more important than exposing abuses of public authority, analyzing a leaker's impact on national security is very difficult. The current intelligence apparatus, coupled with the government's classification system, has created an information gap between the government and its citizens. While officials may argue that intelligence disclosures weaken the government's ability to protect its citizens, they are unable to reveal specifics regarding incidents that have been prevented due to these programs. Therefore, measuring a disclosure's impact on national security can be subjective and problematic.

   We recommend that this condition be amended to state that intelligence leaks will only be deemed to have "a disproportionate impact" if

the unauthorized disclosure can be proven to have a direct and discernible impact on national security. Examples of such disclosures would include, but not be limited to, revealing the names and locations of covert operatives or locations of strategic domestic defenses.

4. **The leaker should utilize the least drastic means of disclosure.** Per Sagar, whistleblowers should seek to minimize threats to national security by limiting the scope and scale of their disclosures. This condition implies that an individual "must examine whether it is possible to make an unauthorized disclosure within the confines of the executive branch" [Sag13] prior to going to Congress or the press. Sagar argues that this condition is particularly important for low-ranking government officials as they may "lack the contextual information necessary to determine whether there has been an abuse of authority" [Sag13].

   However, this condition fails to consider the reputational harm and retribution that may be directed towards a whistleblower in their attempt to uncover wrongdoing. Further, following such procedures may provide unlawful actors an opportunity to cover their tracks. Finally, this condition does not consider that current whistleblowing protocols favor the bureaucracy over the leaker. While an alternative is to report evidence of wrongdoing to Congress, there is a risk that such information could be distorted and used for political gain.

   Moving forward, whistleblowers may be justified in leaking information directly to the press if they have considered all options and can reasonably defend their decision. Further, it is worth noting that the method of the leaks is less important than the scope. The release of classified documents must be limited to those that pertain to the alleged wrongdoing.

5. **Individual must be willing to disclose his identity.** Finally, a whistleblower must be willing to disclose his identity, thereby allowing the public to discern and scrutinize his motivations. Maintaining anonymity can make it extremely difficult for the public to determine whose interests are being served by the disclosure and if there are other factors or political motivations at play. As such, justification must be based on a whistleblower's willingness to reveal his identity and defend his motivations.

5+1. **The leaks should serve the public interest in a way that would not have happened otherwise.** While Sagar's five conditions create a strong set of guidelines, future justification for intelligence leaks should also consider whether the leaks served the public interest in a way that would not have happened otherwise. At issue here is the idea that leaks should only be used as a fail-safe mechanism in the event that current oversight protocols are rendered ineffective. Over-reliance on leaks as a method of oversight would weaken the current classification system and fundamentally alter how the United States creates foreign policy.

Justification for future leaks should not only be required to meet the five conditions discussed above, but should also be predicated on the fact that the leaking of classified documents was the only remaining option available to provide oversight in the interest of the public.

# 3 Issues that Require Further Consideration

In addition to developing a framework for justification, there are a number of factors that could influence an investigation's outcome and the fate of the source. Though an in-depth discussion of these issues is beyond the scope of this memo, we believe the following issues deserve further investigation.

- **Selecting the forum for deliberation.** Our current system provides several avenues for determining justification, including civil and criminal courts, congressional hearings, military tribunals, and investigative committees. However, some of these may be more appropriate than others, and consistency is important to developing confidence in the system. We must consider the ability of each to make decisions free from undue political or agency influence, as well as their respect for the constitutional right to due process.

- **Strengthening whistleblower protections.** In 2012, President Obama issued a policy directive to strengthen whistleblower protection laws for members of the intelligence community and, by extension, to government contractors [Oba12]. While it is in the intelligence community's best interest to have strict rules in place to protect national security, these whistleblower laws only cover actions that follow a prescribed

protocol. As discussed above, they do not allow disclosure of information beyond an individual's chain of command or to an Inspector General. This raises concerns about the efficacy of reporting potential agency wrongdoing to an agency representative.

- **Changes to classification system.** In addition to the concerns about information asymmetry raised by Sagar, the current classification system has illuminated concerns regarding the ability of Congress to effectively handle oversight of intelligence activities. Only members with the highest security clearances have access to sensitive information, which presents issues of transparency and accountability. In addition, the confidentiality of previously unreleased but relevant information may make it difficult to have an impartial civilian trial. Though the Ellsberg case was tried in federal court [Arn73], it remains to be seen whether our current classification system would allow open discussion of the facts of the case.

- **Developing a consistent internal policy on disclosures.** Presidential administrations have sent contradictory messages regarding release of confidential material. We must consider the current acceptability of an unofficial policy of "instant declassification," which allows insiders to release information deemed favorable to the administration without concern for prosecution [Els13]. Currently the Attorney General has the freedom to decide which leaks to pursue. In particular, the Obama administration has taken a hard stance against leaks it has not authorized, calling for government agencies to develop policies against "insider threats" [Oba11].

# 4 Case Study: Edward Snowden

Edward Snowden, an NSA contractor working for Booz Allen Hamilton, is responsible for the most recent intelligence leaks in the United States. By the current estimates, he is believed to have obtained 15,000 or more Australian intelligence files [SM13]; at least 58,000 British intelligence files [BBC13]; and roughly 1.7 million US intelligence files [SW14]. The series of global surveillance disclosures based on these files, which started from June 2013 and has continued to this date, are considered by many to be the most significant intelligence leaks in the US history.

Detailed discussions about the nature of these leaks are outside the scope of this work but to assist future referencing, we have assigned them to five categories below and provide some examples for each:

- **Cellphone Data:** Collection of Verizon subscribers' metadata [Gre13], Chinese citizen's text messages[Lam13], German citizens metadata [LPS13b], Breaking cell phone encryption [TS13], piggybacking on smartphone applications [Bal14]; and programs such as Boundless Informant [GG13a], MYSTIC [GS14]

- **Browsing Data:** Tracking Chinese citizens [Lam13], and German citizens [LPS13b]; Attacking TOR network [JBG13a]; and programs such as PRISM [GG13b], Boundless Informant [GG13a], EvilOlive [GA13a], ShellTrumpet [GA13a], Stellar Wind [GA13b], MUSCULAR [GS13]

- **Cyberwar Operations:** Presidential Policy Directive 20 [GG13c], Spying on Chinese government and company Huawei [De 14], Wikileaks [GG14], and hacktivists [MSG13]

- **Internet Infrastructure:** Attacks targeting Tsinghua University [Lam13], and System administrators [RG14], weakening encryption standards [JBG13b]; and programs such as Tempora [EMB13b].

- **Diplomats and Foreign Leaders:** Intercepting communication at 2009 G20 summit [EMB13a], and climate negotiations [KS14] ;surveilliance on E.U. embassies [LPS13a],United Nations [LPS13c], and IAEA [LPS13c]

While this categorization is imperfect, it provides us with the general framework to look at Snowden revelations in the light of the six characteristics discussed in the previous section.

## 4.1 Were Snowden leaks justified?

1. **Reveal Wrongdoing** At the current moment, there is little doubt that gross wrongdoing has been committed by the NSA and other security agencies such as GCHQ. The disproportionate amount of data collection on both US and foreign citizens around the world, targeting websites such as Wikileaks [GG14], and reports of data collection abuses within the NSA [Gor13] have led to considerable condemnation.

A ruling by US district judge has concluded that NSA's surveillance program "may be unconstitutional". [JW13] Snowden and his proponents have called this ruling "vindictive [RA13]."

2. **Based on Evidence** While some analysts have described several of Snowden's claims as "overblown", [DBD13] given the top secret documents released by journalists and government reactions to these reports, there is no doubt regarding the authenticity of these documents.

3. **Proportionate Burden** Although Snowden's revelations easily clear the first two criteria, it is hard to argue about the burden they have caused on national security. Opponents of Snowden have said that these leaks have "slowed the effort to protect the country against cyberattacks [San14]." Moreover, Snowden's leaks about US activities in China have been called "a grave threat to US national security [Bol13]." However, his supporters have called the usefulness of the NSA Mass Surveillance program into question [PB14] and argued that programs such as PRISM and phone metadata minimally contribute to terrorism investigations [Isi13]. The same argument cannot be made for cyber attacks and espionage programs revealed by the Snowden leaks, such as those categorized under cyberwar operations and diplomatic espionage.

4. **Least Drastic Means** Just like proportionality, whether or not Snowdens revelations were the least drastic way of bringing NSA overreach to the publics attention is subject to much discussion. While theoretically there are governmental channels for whistleblowers to go through, previous experiences such as Thomas Drake, William Binney, and J. Kirk Wiebe [EP13] have shown the inefficiencies of these paths. While Snowden's revelations have forced the long-delayed discussion on cyber privacy onto the agenda, The magnitude of revelations, especially those involving cyberwar operations or espionage activity against foreign leaders, and possible repercussions it has on United States foreign relations might prove damaging in the future.

5. **Reveal Identifiability** The fifth characteristic of a justified leak is that the leaker must reveal their identity. The series of global surveillance disclosures based on Snowden documents began on June 5th, 2013 [Gre13]. Edward Snowden's identity was disclosed 4 days after

that in an exclusive interview with the Guardian [GGP13]. In this interview, he described his motives as "...to inform the public as to that which is done in their name and that which is done against them." While there have been suggestions that Snowden have provided intelligence to Russia [SS14], these claims have been vigorously denied by Snowden [May14] and no proof has been provided to support this claim. [Ger14] Given these information, we believe Snowden leaks meet the identifiability requirement.

5+1. **Serving Public Interest** The effect of the Snowden revelations on policy making is undeniable. The judicial action to review NSA surveillance practices [Rus13], President Obama's call for NSA reforms [NM14], and talk of possible legislation which cut back on NSA's questionable practices [McC14] would probably not have happened without those revelations. These reports have also brought the issue of privacy and anonymity to the front of public discussions which can translate to meaningful steps on improving social rights and incorporation of privacy norms in the cyberspace.

# 5 Conclusion

Overall, Snowdens revelations regarding the collection of cellphone, browsing data, and attacks against the Internet infrastructure meet the criteria mentioned above, and as such, we find that the leaks were justified. However, his disclosure of programs categorized under cyber war operations and diplomacy, which are separate from the revelations regarding metadata, do not meet all necessary conditions for justification. As there are no norms or international laws regarding cyber espionage, the programs revealed by Snowden do not technically qualify as wrongdoing; further, the scope of the document release violates the "least drastic means" criteria.

As this memo focuses on justification, we make no attempt to prescribe a method for handling cases once this has been decided. However, future research may wish to address a few of the additional issues we have highlighted above in the hopes of ensuring fair, consistent policies for treating those accused of releasing sensitive information.

# References


[Arn73] Martin Arnold. Pentagon papers charges are dismissed; judge byrne frees ellsberg and russo, assails "improper government conduct". *The New York Times*, May 1973.

[Bal14] James Ball. Angry birds and 'leaky' phone apps targeted by nsa and gchq for user data. *The Guardian*, January 2014.

[BBC13] BBC News. David miranda row: Seized files 'endanger agents'. August 2013.

[Bol13] John Bolton. Edward snowden's leaks are a grave threat to us national security. June 2013.

[DBD13] Ken Dilanian and Washington Bureau Barbara Demick. Analyst overstated claims on nsa leaks, experts say. *Los Angeles Times*, June 2013.

[De 14] De Spiegel. Targeting huawei: NSA spied on chinese government and networking firm. March 2014.

[Els13] Jennifer K. Elsea. he protection of classified information: The legal framework. *Congressional Research Service*, January 2013.

[EMB13a] Nick Hopkins Julian Borger Ewen MacAskill, Nick Davies and James Ball. GCHQ intercepted foreign politicians' communications at g20 summits. *The Guardian*, June 2013.

[EMB13b] Nick Hopkins Nick Davies Ewen MacAskill, Julian Borger and James Ball. GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*, June 2013.

[EP13] Peter Eisler and Susan Page. 3 NSA veterans speak out on whistle-blower: We told you so. *USA Today*, June 2013.

[GA13a] Glenn Greenwald and Spencer Ackerman. How the NSA is still harvesting your online data. *The Guardian*, June 2013.

[GA13b] Glenn Greenwald and Spencer Ackerman. NSA collected us email records in bulk for more than two years under obama. *The Guardian*, June 2013.

[Ger14] Josh Gerstein. Feinstein sees no evidence snowden spying for russia. *Politico*, January 2014.

[GG13a] Ewen MacAskill Glenn Greenwald. Boundless informant: the NSA's secret tool to track global surveillance data. *The Guardian*, June 2013.

[GG13b] Ewen MacAskill Glenn Greenwald. NSA prism program taps in to user data of apple, google and others. *The Guardian*, June 2013.

[GG13c] Ewen MacAskill Glenn Greenwald. Obama orders us to draw up overseas target list for cyber-attacks. *The Guardian*, June 2013.

[GG14] Glenn Greenwald and Ryan Gallagher. Snowden documents reveal covert surveillance and pressure tactics aimed at wikileaks and its supporters. *The Intercept*, February 2014.

[GGP13] Ewen MacAskill Glenn Greenwald and Laura Poitras. Edward snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, June 2013.

[Gor13] Siobahn Gorman. NSA officers spy on love interests. *The Wall Street Journal*, August 2013.

[Gre13] Glenn Greenwald. NSA collecting phone records of millions of verizon customers daily. *The Guardian*, June 2013.

[GS13] Barton Gellman and Ashkan Soltani. NSA infiltrates links to yahoo, google data centers worldwide, snowden documents say. *The Washington Post*, October 2013.

[GS14] Barton Gellman and Ashkan Soltani. NSA surveillance program reaches into the past to retrieve, replay phone calls. *The Washington Post*, March 2014.

[Isi13] Michael Isikoff. NSA program stopped no terror attacks, says white house panel member. *NBC News*, December 2013.

[JBG13a] Bruce Schneier James Ball and Glenn Greenwald. NSA and GCHQ target tor network that protects anonymity of web users. *The Guardian*, October 2013.

[JBG13b] Julian Borger James Ball and Glenn Greenwald. Revealed: how us and uk spy agencies defeat internet privacy and security. *The Guardian*, September 2013.

[JW13] Kevin Johnson and Richard Wolf. Federal judge rules against nsa spying. *USA Today*, December 2013.

[KS14] Ryan Grim Kate Sheppard. Snowden docs: U.s. spied on negotiators at 2009 climate summit. *Huffington Post*, January 2014.

[Lam13] Lana Lam. Edward snowden: Us government has been hacking hong kong and china for years. *South China Morning Post*, June 2013.

[LPS13a] Fidelius Schmid Laura Poitras, Marcel Rosenbach and Holger Stark. Attacks from america: NSA spied on european union offices. *Der Spiegel*, June 2013.

[LPS13b] Fidelius Schmid Laura Poitras, Marcel Rosenbach and Holger Stark. Partner and target: NSA snoops on 500 million german data connections. *Der Spiegel*, June 2013.

[LPS13c] Marcel Rosenbach Laura Poitras and Holger Stark. Codename 'apalachee': How america spies on europe and the un. *Der Spiegel*, August 2013.

[May14] Jane Mayer. Snowden calls russian-spy story absurd in exclusive interview. *The New Yorker*, January 2014.

[McC14] Rick McCormick. Obama to propose legislation to end NSA's bulk phone-record collection. *The Verge*, March 2014.

[MSG13] Matthew Cole Mark Schone, Richard Esposito and Glenn Greenwald. War on anonymous: British spies attacked hackers, snowden docs show. *NBC News*, February 2013.

[NM14] Ellen Nakashima and Greg Miller. Obama calls for significant changes in collection of phone records of u.s. citizens. *Washington Post*, January 2014.

[Oba11] Barack H. Obama. Executive order 13587–structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information. *The White House*, October 2011.

[Oba12] Barack H. Obama. Presidential policy directive/ppd-19. October 2012.

[PB14] Emily Schneider Bailey Cahall Peter Bergen, David Sterman. Do NSA's bulk surveillance programs stop terrorists? *New America Foundation*, January 2014.

[RA13] Dan Roberts and Spencer Ackerman. Edward snowden says judge's ruling vindicates NSA surveillance disclosures. *The Guardian*, December 2013.

[RG14] Peter Maass Ryan Gallagher. Inside the NSAs secret efforts to hunt and hack system administrators. *The Intercept*, March 2014.

[Rus13] Russia Today. Citing snowden leaks, FISA court orders government to review secretive NSA surveillance rules. September 2013.

[Sag13] Raul Sagar. *Secrets and Leaks: The Dilemma of State Secrecy*. Princeton University Press, 2013.

[San14] David E. Sanger. NSA director says snowden leaks hamper efforts against cyberattacks. *The New York Times*, March 2014.

[Sav14] Charlie Savage. Obama to call for end to NSA's bulk data collection. *The New York Times*, March 2014.

[SM13] Cameron Stewart and Paul Maley. Edward snowden stole up to 20,000 aussie files. *The Australian*, December 2013.

[SS14] Eric Schmitt and David E. Sanger. Congressional leaders suggest earlier snowden link to russia. *The New Yorker*, January 2014.

[SW14] Chris Strohm and Del Quentin Wilber. Pentagon says snowden took most u.s. secrets ever: Rogers. *Bloomberg*, January 2014.

[Tat13] Julie Tate. Judge sentences bradley manning to 35 years. *The Washington Post*, August 2013.

[TS13] Craig Timberg and Ashkan Soltani. By cracking cellphone code, nsa has capacity for decoding private conversations. *The Washington Post*, December 2013.