Working with Whistleblowers

A Guide for Public Interest Organizations

GAP

GOVERNMENT ACCOUNTABILITY PROJECT

Truth be told.

Government Accountability Project
1612 K Street NW, Suite 1100
Washington, DC 20006
202.457.0034

www.whistleblower.org

The Government Accountability Project thanks the following organizations for their support in developing this resource:

Defending Rights & Dissent

Financial Accountability & Corporate Transparency

Fund for Constitutional Government

Greenpeace USA

Jubilee USA Network

Levin Center at Wayne Law

News Media for Open Government

Open the Government

Project On Government Oversight

Public Citizen

Taxpayers for Common Sense

Special thanks to:

Justice Catalyst

Working with Whistleblowers

A Guide for Public Interest Organizations

CONTENTS

Whistleblowing & Your Organization

Whistleblowers—employees who discover and expose serious wrongdoing—are vital for public interest organizations fighting to advance social, economic and environmental justice. Information provided by whistleblowers, when used effectively, has tremendous power to hold institutions and leaders accountable.

Escalating concerns about scientific censorship, obstruction of public access to information, and government dysfunction have prompted new support for whistleblowers among advocacy organizations. Disclosures made by whistleblowers have exposed serious problems and prompted significant reforms across a wide range of issues, including public health dangers, food safety risks, science censorship, fraud and waste, environmental violations, racial injustice and national security threats.

Whistleblowers have made important contributions in almost every area of public interest concern. But rather than being valued by their employers, they are often vilified, risking workplace retaliation, character assassination, mistreatment by colleagues, demotion and termination. Some even face civil suits and criminal prosecution. The power of truth is significant, but so are the risks to whistleblowers.

It is essential for organizations working with whistleblowers to do so wisely. The legal landscape of whistleblowing is complicated and the risk of retaliation is high. Understand that information often cannot be separated from the person providing it. Word will spread when a public interest group abandons whistleblowers or exposes them to retaliation. Not only will that group lose that flow of information, others may as well. Organizations have a responsibility to protect whistleblowers by understanding risks and using best practices.

The Government Accountability Project (GAP) is the nation's leading whistleblower protection and advocacy organization, having represented or advised over 8,000 whistleblowers since 1977. GAP serves as an important lifeline for whistleblowers, helping them hold government and corporate institutions accountable by verifying their concerns and presenting problems to public officials, advocacy groups and journalists, and seeking justice if they suffer reprisal. In addition, GAP has drafted, spearheaded the campaigns to pass or helped defend all the federal whistleblower protection laws that exist today, and have established best practice standards for domestic and international whistleblower policies.

Solidarity with other public interest organizations is critical to amplifying the importance of whistleblowers' disclosures and demanding reform. For example, GAP collaborated with local and national environmental advocacy organizations that received information from whistleblowers in the wake of the 2010 BP Deepwater Horizon oil spill. Similarly, GAP works within coalitions that include food safety, public health and animal welfare organizations to protect whistleblowers and urge reform of unsafe food inspection and animal cruelty practices. GAP also collaborates with environmental and science advocacy groups to promote integrity in climate science and policy, and with human and civil rights organizations to support national security whistleblowers. Finally, GAP partners with a diverse group of public interest organizations across the political spectrum to maintain and expand whistleblower protection laws.

This guide is a tool for organizations working with, or considering working with, whistleblowers. It offers practical guidance on how to protect and support employees who want to address malfeasance while ensuring they are not inadvertently exposed to retaliation.

An advocacy group's collaboration with a whistleblower can be the highest stakes, most stressful partnership in that whistleblower's professional life. Your organization must earn the trust of the whistleblower. Whistleblowing partnerships done right can substantially amplify your organization's mission. We hope this guide helps your organization weigh the pros and cons of working with whistleblowers and helps protect the organization and the whistleblower in the process.[1]

1 Disclaimer: This guide is for informational purposes only and does not constitute legal advice.

What is a Whistleblower?

Whistleblowers are those who witness wrongdoing in the workplace and decide to speak up rather than stay silent to expose serious violations of public trust.

Legally, a common definition of a whistleblower is someone, typically an employee, who discloses information, either internally (to managers, organizational hotlines, etc.) or externally (to lawmakers, regulators, the media, watchdog organizations, etc.), that he or she reasonably believes evidences:

- a violation of law, rule or regulation;
- gross mismanagement;
- a gross waste of funds;
- abuse of authority; or
- a substantial and specific danger to public health or safety.

This definition captures two key points about whistleblowers. First, whistleblowers typically are current or former employees with direct, credible information about wrongdoing that they became aware of while on the job. Second, the concerns are serious and their disclosure promotes legal compliance or protects the public interest.

The Truth About Whistleblowers: Tackling Misperceptions

Despite the important role whistleblowers have played in exposing and correcting abuses of power, the term "whistleblower" often has negative connotations and common misperceptions. Here are some truths:

TRUTH #1: Almost all whistleblowers report concerns internally first.

Most employees who witness wrongdoing in the workplace stay silent. The first reason for silence is cynicism, or the belief that disclosure will not make a difference. The second reason is fear of retaliation. Of those who do decide to speak up, over 95% of them try to solve the problem internally first.[2]

While many believe that whistleblowers are employees who choose to go outside of the organization to raise a concern, most whistleblowers are loyal to their employers and believe that raising concerns within their workplace will address the problem. Typically, they do not anticipate their management will view them as the central problem rather than the concerns they report. Often, they seek external support only after the employer fails to address the real issue or attacks the messenger.

Employees who raise serious concerns internally to managers or through other internal channels are considered whistleblowers under nearly all whistleblower protection laws.

Because whistleblowers often report concerns internally first, and/or because the information to which they have access is tied to their work responsibilities, they likely have left metaphorical fingerprints on the matter. Unless third parties that publish information are very careful, employers can discover who blew the whistle.

For this reason, promises of anonymity may be difficult to keep. We discuss issues involved with maintaining anonymity, including pros, cons, and strategies, later in this Guide.

2 See Ethics Resource Center, "Inside the Mind of a Whistleblower: A Supplemental Report of the 2011 National Business Ethics Survey" (2012). http://www.ethics.org/nbes/files/reportingFinal.pdf.

TRUTH #2: Whistleblowers are typically motivated by a sense of civic or legal duty influenced by the seriousness of the misconduct or degree of harm.

Contrary to popular belief, it's not about the money. Some whistleblower laws, like the False Claims Act and the Dodd-Frank Act, offer whistleblowers a percentage of the portion of money recovered as an incentive for reporting. These laws have been extraordinarily successful in encouraging reports of fraud. Yet it's rare that a whistleblower receives a monetary reward, and most non-financial whistleblower protection laws do not have award provisions. Where whistleblowers are awarded a share of the government's recovery, it's often small comfort for the pains they have suffered for following their conscience.

In GAP's experience, most employees who feel compelled to speak out about wrongdoing explain that they had to act to be true to themselves. As one explained, "I have to keep looking at myself in the mirror."

TRUTH #3: Disclosing evidence of wrongdoing is not a crime. It is a legally protected right.

The aggressive prosecution by the Obama and Trump Administrations of intelligence employees who released classified information to report serious abuses, such as Edward Snowden, Chelsea Manning and Reality Winner,[3] has fueled a widespread belief that whistleblowing is a crime.

Intelligence community (IC) whistleblowers are unique, as they have very few legal protections and immense vulnerabilities. In the above cases, the whistleblowers chose to commit a crime—revealing classified information—in order to report more significant crimes. Most whistleblowers, however, are not forced to risk breaking the law by disclosing classified information to expose wrongdoing. ***Only a small percentage of whistleblowers work in the intelligence community.***

Further, in forty years at GAP, intelligence community whistleblowers always have been able to make their point by summarizing misconduct without releasing classified information. However, sometimes taking the risk is unavoidable to make a difference.

3 E.g., Edward Snowden's, Thomas Drake's, Bill Binney's, Thomas Tamm's and others' disclosures of the NSA's warrantless mass surveillance of U.S. citizens, as well as John Kiriakou's disclosures of the government's official use of waterboarding in interrogations, were all met with investigations and/or charges under the Espionage Act, which offers no public interest defense. Chelsea Manning's sentence was only recently commuted after serving almost seven years in jail. These high-profile cases shape public perception about whistleblowing, sowing the potential misconception that whistleblowing is a crime in all contexts.

Because agencies often engage in classified lies, sometimes the only way to expose them is through classified documents.

As a rule, unless public release is barred by statute, whistleblowers who disclose evidence of illegality and other wrongdoing are engaging in legally-protected activity.[4] Most whistleblowers disclose information about financial fraud, public health or consumer safety threats, environmental dangers, or other misconduct—information that is not classified. They are not operating in the national security context at all, and they have legal rights to encourage reports of wrongdoing. In fact, since 1978 in the United States, there has been a unanimous, bipartisan legislative mandate for every whistleblower law enacted to encourage disclosures of serious concerns.

Prosecutions of IC whistleblowers combined with aggressive "anti-leak" rhetoric fuels the misperception that whistleblowing is rogue rather than legal activity. This confusion is then exploited and exacerbated by new attempts to suppress employee speech, including gag orders, non-disclosure agreements, bans on using certain words in government documents, and mandatory "anti-leak" and "insider threat" trainings. Aimed to prevent "unauthorized disclosures" even when those disclosures are not classified (indeed, most whistleblowing to external sources is inherently "unauthorized"), these efforts create a dangerous chilling effect on employees who are often unclear about or hesitant to exercise their legal rights to blow the whistle.

4 Some whistleblower protection provisions, particularly those that protect state and municipal employees, may require employees to follow certain internal disclosure paths before reporting concerns externally in order to qualify for legal protection. Other laws may only protect external reports. Because each whistleblower protection law is different, discussed later on page 11, this is why legal advice sought in advance of disclosure is most valuable.

Whistleblowers Who Made a Difference

PUBLIC HEALTH

FDA safety researcher **Dr. David Graham** demonstrated that the painkiller Vioxx had caused heart attacks with a 30% to 40% fatality rate. After the FDA tried to suppress his findings, Dr. Graham shared his concerns with Congress, ultimately resulting in Vioxx being pulled from the shelves.

SCIENCE CENSORSHIP

Rick Piltz, who served as a senior associate in the U.S. Global Change Research Program, exposed the George W. Bush Administration's improper editing and censorship of science program reports on global warming intended for the public and Congress. His disclosures, reported on the front page of the *New York Times*, prompted the resignation of the offending official, a former top oil lobbyist, and helped expand whistleblower protections to federal employees who report scientific censorship.

FOOD SAFETY

Former Peanut Corporation of America (PCA) employee **Kenneth Kendrick** exposed the company's egregious health violations at PCA's Texas facility after a deadly salmonella outbreak in 2008 from tainted peanuts. Kendrick's disclosures prompted one of the largest food recalls in U.S. history and drove passage of the Food Safety Modernization Act.

RACIAL DISCRIMINATION

Cathy Harris was a senior inspector for the U.S. Customs Service who disclosed discriminatory racial profiling of black and brown female travelers as drug carriers, including numerous incidents of such women being body-cavity-searched, illegally detained or restrained for several days. Her disclosures were made public in March 1999 by a Fox 5 investigative news team, prompting a complete overhaul in Customs policies and practices.

BANK FRAUD

Numerous bank employees, including Citigroup whistleblowers **Eileen Foster** and **Richard Bowen** and Countrywide whistleblower **Michael Winston**, uncovered fraudulent mortgage-loan practices that fueled the financial meltdown in 2008. Their disclosures helped drive sweeping bank reforms and a new whistleblower program at the Securities and Exchange Commission to encourage tips, prevent reprisals, ensure reforms, and punish reckless activity.

ILLEGAL SURVEILLANCE

Whistleblowers **Thomas Drake**, **William Binney** and **J. Kirk Wiebe** reported to Congress and the Inspector General the National Security Agency's gross waste in choosing to purchase Trailblazer, a multi-billion dollar surveillance software program that did not protect against warrantless searches, over ThinThread, a $3 million dollar in-house developed program that was more effective and constitutionally protective. Their whistleblowing preceded Edward Snowden's disclosures of the NSA's mass surveillance of American citizens' electronic communications, leading to government reforms as well as new private sector protections of consumer privacy rights.

ENVIRONMENTAL PROTECTION

PhD engineer **Walt Tamosaitis** exposed waste, fraud and technical problems at the Hanford Nuclear Site's Waste Treatment Plant that could have resulted in a Fukushima-like nuclear explosion in the Pacific Northwest. Tamosaitis's concerns were validated by agency and media investigations and resulted in recovery of $125 million for taxpayers, new whistleblower protections for federal contractors, and a halt to plant construction pending resolution of safety issues.

NATIONAL SECURITY

Two years after the 9/11 terrorist attacks, agent **Robert MacLean's** disclosures of reductions in Federal Air Marshal coverage on commercial flights in the midst of intelligence warnings of an imminent hijacking attempt restored in-flight staffing to appropriate levels.

How to Work with Whistleblowers

Many advocacy organizations and activists are interested in the information whistleblowers offer but are not in the business of representing whistleblowers or providing advice about their rights, risks and options for disclosure. Whether your organization is actively soliciting information from whistleblowers, or if an employee approaches your organization with evidence of serious wrongdoing, keep the following tips in mind.

Understand the Risk of Reprisal

No matter how right they are about wrongdoing, corruption, and public safety threats, employees who speak out often suffer reprisals rather than thanks. Allies that support whistleblowers—including journalists and advocacy organizations—are also vulnerable to retaliation.

Reprisals against whistleblowers can take a range of forms, including:

- **retaliatory investigations**
- **gag orders**
- **removal of duties or resources**
- **reassignment**
- **public humiliation**
- **surveillance**
- **management efforts to recruit complaints by peers**
- **poor performance appraisals**
- **threats**
- **harassment**
- **denials of promotions**
- **psychiatric exams**
- **termination**
- **violence**
- **lawsuits for defamation, misappropriation of private property, breach of contract, such as non-disclosure agreements**
- **criminal investigations**
- **efforts to prosecute**

Other examples of aggressive tactics used to deter whistleblowing by retaliating against not only employees who report wrongdoing, but also the journalists or advocacy groups that support them, include:

- Pronouncements by the Department of Justice to escalate prosecutions of national security whistleblowers and threats to force journalists to reveal their sources.
- "Ag-Gag" legislation introduced in several states that criminalizes the publication of photo and video documentation of conditions at industrial agricultural facilities (although courts have found some of these laws unconstitutional).
- Corporate employers seek, and occasionally secure, criminal prosecution of employee whistleblowers and organizations for "theft" of company property even though it reveals the company's crime.
- Companies may file multi-million dollar "SLAPP suits"[5] against whistleblowers for violations of non-disclosure agreements, or against non-profit organizations for alleged defamation.
- Government agencies increasingly are referring employees for criminal investigations and prosecutions in non-intelligence contexts when they engage in protected whistleblowing activity.

It is important not to underestimate the risk of aggressive reprisal strategies that an employer can take against an employee who has exposed its wrongdoing. Not only can these destroy a whistleblower, but they can chill others in that organization or industry from disclosing concerns in the future.

Appreciate the Legal Landscape: It's Complicated

Understanding that whistleblower law is complicated can help protect your source.

No single law protects whistleblowers from reprisal. Instead, a patchwork of First Amendment rights, more than 60 federal laws and statutes, and numerous state and local laws offer whistleblowers protections and avenues for disclosure. In addition, laws protecting whistleblowers have different remedies, different procedural steps and different paths for enforcement.

5 SLAPP (Strategic Lawsuit Against Public Participation) suits, though illegal in some states, are used to censor and intimidate critics through a burdensome lawsuit.

Figuring out what legal protection might be available to a specific whistleblower depends on several factors:

- **What is the nature of the information?** Numerous federal environmental, financial, transportation safety, food safety or occupational safety laws contain anti-reprisal provisions to protect employees who report possible or actual violations of those laws. Others are like the federal Whistleblower Protection Act (WPA), which allows most federal employees to challenge nearly any significant abuse of authority with consequences for the public.[6] Whether protection exists can depend on whether the issue or problem the whistleblower is disclosing relates to an area that is subject to regulations and rises to a level of severity to demonstrate a violation, abuse or threat of harm.
- **Who is disclosing the information?** Different protections apply depending on whether the whistleblower is a federal employee, a federal contractor, a corporate employee in a publicly traded versus a privately held company, an intelligence/national security employee, a state or municipal employee, a citizen of another country or an employee of an international organization.
- **Is the information classified?** In the United States, whistleblowers have no legal protection to publicly release classified information. Indeed, it is a criminal offense for which they could be prosecuted.[7] Similarly, there is no protection to publicly share information whose confidentiality is specifically protected by a statute, such as the Trade Secrets Act or the Privacy Act.[8]
- **What kind of reprisal has the employee experienced?** Different laws protect against differing kinds of retaliation taken in response to whistleblowing. The federal WPA outlines specific prohibited personnel actions[9] that cannot be taken in retaliation for

6 The Whistleblower Protection Act (WPA), amended by the Whistleblower Protection Enhancement Act (WPEA), is the primary law that protects non-intelligence federal employee whistleblowers. Employers may not retaliate against employees who disclose information they reasonably believe evidences a violation of law, rule or regulation; gross mismanagement; a gross waste of funds; abuse of power; a substantial and specific danger to public health or safety; or censorship related to scientific research or analysis that would result in one of the five types of misconduct described above. Additionally, federal employees also have the right to refuse to obey an order that would require the individual to violate a law. See Whistleblower Protection Act of 1989, 5 U.S.C. § 2302(b)(8) & (b)(9); Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112-199, § 110(b).

7 Indeed, if an organization actively participated in a conspiracy to smuggle classified documents from a secure location, it too could face prosecution.

8 Most public interest organizations won't have reason to be approached with classified information in the first place. Still, it is important to understand that some prosecutors and high government officials believe that publicly disclosing classified information is a felony. Within the U.S., there is currently no public interest exception or defense available even to a whistleblower whose disclosures reveal illegality far more serious than release of classified information. Advocacy groups that work with intelligence community whistleblowers should understand that any advocacy based on classified information will likely result in the whistleblower's prosecution, no matter the precautions taken. Do not attempt to work with a whistleblower from the intelligence community without sound legal advice.

9 Prohibited personnel actions include disciplinary action, transfer or reassignment, poor performance evaluation, change in pay, benefits, awards, or training, ordering a psychiatric exam, change in duties, responsibilities, or working conditions, gag orders or non-disclosure agreements that do not include an exception for whistleblower rights and protections under the WPA or WPEA, or threatening an employee with any of the above. 5 U.S.C. § 2302(a)(2)(A).

protected whistleblowing activity. Most federal corporate whistleblower laws protect against any discrimination sufficiently severe to create a chilling effect on the exercise of associated rights, a broader standard, while some state common law rights protect only against wrongful discharge but not reprisal short of termination.

- **To whom and how was the disclosure made?** Whether protection exists might depend on whether the whistleblower disclosed concerns as part of their job duties or on personal initiative; whether they disclose internally to co-workers, supervisors, union representatives, ethics officers, ombudspersons; or whether they report externally to Congress, an Inspector General, an oversight agency, a watchdog organization, or the media. Certain laws may also mandate that the whistleblower report the concerns to specified parties in a prescribed order to receive protection.
- **When did the employee became aware of the reprisal?** Statutes of limitations differ widely, ranging from 30 days to three years or none.
- **Where was the disclosure made?** Local and state protections vary significantly and can sometimes preempt federal remedies or limit the choice of venue for appeals.

Organizations that do not offer direct legal assistance to whistleblowers should not attempt to conduct the legal analysis necessary to evaluate possible legal remedies for a source. However, understanding that the legal landscape is complicated should prompt organizations to prioritize consulting with experienced legal counsel, and to encourage the source to do the same to maximize protection and minimize risk.

Anonymity: Challenges & Consequences

If information provided by a whistleblower is going to be used in public, risk-free anonymity simply cannot be guaranteed. Because the vast majority of employees raise concerns internally first, or because the information can be connected to an employee's job duties and expertise, an employer may be able to quickly identify the likely source.

Many whistleblowers want to share information but remain anonymous. Some organizations have set up hotlines to receive tips from whistleblowers about misconduct, promising anonymity to those who call. But when a whistleblower decides to go to an external source to make a disclosure—e.g., an NGO or a journalist—his or her fingerprints are already on the

information. Management can frequently suss out the source once the issue is made public. Even if the employee didn't raise the concern internally first, it is often still relatively easy to figure out the source because the specificity of the disclosure can be traced to the job responsibilities and expertise of the employee.

Public Disclosure May Be Safer & More Effective

Remaining anonymous may also not be the best strategy for a whistleblower. For instance, trying to remain anonymous while the disclosure is public might make a legal case of reprisal more difficult, if not impossible, to establish. Under all whistleblower laws, an employee must show that the employer had knowledge of the whistleblowing. Going public, with the whistleblower serving as a human interest focal point for news stories, can sustain the whistleblower's viable legal rights.

Public disclosure can even preempt reprisal by putting the employer on notice that the employee is engaging in protected whistleblowing. When a whistleblower experiences solidarity with a team of allies—advocacy groups, journalists, champions in Congress, a lawyer—the credibility of the whistleblower and the seriousness of the disclosures are amplified and can defeat efforts to vilify the messenger.

Despite some of the benefits of a whistleblower standing publicly by his or her story, don't let factors like the need for a compelling spokesperson on an issue influence you to pressure a whistleblower to drop anonymity. Going public usually guarantees the whistleblower will burn professional bridges. If a scorched-earth, no-prisoners conflict did not already exist, that dynamic will become a near certainty. Consequently, many whistleblowers want to try to maintain anonymity. Ultimately, you have to respect their choices.

Anonymity & Your Organization

Despite the greater insulation and effectiveness that speaking out publicly often affords whistleblowers, many still request anonymity. Offering hotlines using secure communication technology, staffed by attorneys to receive information anonymously, may seem to address this concern. But promises of anonymity may be difficult to keep.

If the attorney takes information without offering legal advice to the employees about their rights and risks, this may fail to provide the employees with attorney-client privilege, which applies only when the client is seeking legal advice.[10] Thus the government can try to

10 It is not enough to have a lawyer, such as an organization's general counsel, present for discussions with a whistleblower source to invoke the confidentiality protections of the attorney-client privilege. If the whistleblower is not communicating with the intention of seeking legal advice, the privilege does not apply.

subpoena your organization to compel release of the names of your source, or corporations can file SLAPP defamation lawsuits in an attempt to get access to the whistleblower. Public interest organizations, including the Government Accountability Project, have successfully asserted freedom of association rights to protect the identities of their sources,[11] but there are no explicit legal protections governing source confidentiality for advocacy groups. Further, legal battles both distract from an organization's mission and are often expensive.

Worse, by not having attorneys experienced in representing whistleblowers closely monitoring the hotline, the employees who want to report problems they witness in the workplace may have a false sense of security and efficacy.

Offering a hotline for disclosures that fails to offer employees free legal counseling about their rights, risks, and possible strategies for effective disclosure may render them worse off for having called. It may also fuel the false idea that reporting misconduct is wrong or something to fear rather than a legal right and moral duty.

That said, many employees choose between self-censorship and exit rather than reporting witnessed misconduct, unaware of or unwilling to exercise their whistleblower rights. Hotlines that encourage disclosure may be an effective mechanism to support employees who want to report serious misconduct they have witnessed in the workplace, but these mechanisms should be set up with care and sensitivity to the unique and complex vulnerabilities of employee sources.

PRO TIPS

→ Never make an unqualified promise of absolute anonymity because you cannot guarantee it. There are ways to express a willingness to fight to protect the confidences of whistleblowers without promising what you cannot deliver.

→ Anonymous hotlines encouraging external whistleblowing should not only utilize secure communication practices, they should also offer informed legal advice or referrals to attorneys experienced in whistleblower law.

11 The Supreme Court in NAACP v. Alabama, 357 U.S. 449 (1958) held that absent a compelling government interest, an organization cannot be constitutionally compelled to identify the names of its members, agents, contributors, or recipients of contributions if it could be demonstrated that such disclosure would subject those identified to harassment or retaliation by virtue of their association. This precedent has been upheld successfully; U.S. v. Garde, 674 F. Supp. 604 (D.D.C. 1987), protected GAP's freedom of association rights by denying the Nuclear Regulatory Commission's subpoena seeking the identities and information of nuclear whistleblower who came to GAP about safety concerns, relying on promises of confidentiality for fear of reprisal.

Develop Trust

Often whistleblowers are bewildered and scared not only by the risks they have assumed, but by an alien world of strangers, new contexts and new rules with which they are unfamiliar. This usually is entirely new territory for people who do not think of themselves as whistleblowers and have no experience navigating the landscape of news, politics or advocacy tactics.

Below are some pointers for public interest groups to earn the trust of their sources by ensuring the paramount importance of their protection.

1. **Partner with a lawyer to protect the source if you plan to go public with information.** In addition to analyzing rights, risks and strategies to maximize effective and safe disclosure, a lawyer can help issue advance warnings to an employer of zero tolerance for retaliation. This can create a presumption of misconduct for any reprisal tactics and also potentially protect witnesses who might support the whistleblower's claims.

2. **Work with congressional staff who can support oversight efforts and help protect the source.** Being willing to think strategically about the most effective way to protect the employee and ensure that action is taken on the disclosure establishes solidarity and alignment of interests.

3. **Honor all commitments,** from scheduling to substantive, or provide advance notice if they must be adjusted.

4. **Be clear about confidentiality from the beginning,** including your commitment to maintaining it along with the true limits of your ability to guarantee it.

5. **Be clear about what protection you can provide,** and what you cannot, to prevent later charges of betrayal.

6. **Make whistleblowers' protection a visible priority** so they feel the relationship is a two-way street, rather than being mere "evidence objects" who will be discarded when no longer needed.

7. **Provide a safe environment** for interviews and communications.

8. **Engage in active listening during interviews.** Feeling heard is significant for whistleblowers to open up further.

9. **Engage in visible quality control.** Even if there will not be an affidavit attesting to concerns, have the whistleblower read and confirm that the report of interview is accurate. They must agree that they said what you say they did.

10. **Enfranchise the whistleblowers in the larger context by asking their opinions and brainstorming** with them. They may have more to offer than expected or previously realized.

11. If trust with the pioneer whistleblower has been established, **network to expand the scope of witnesses.** Sometimes a community will form around support for the investigation, which means you will almost certainly crack the case.

12. **Sustain the relationship.** Following through can earn a steady stream of new issues and updated evidence or cultivate a source of expertise for help with verification of other investigations in the future.

Information Security

If an employee has come to you with information about serious wrongdoing, public interest groups should exercise special care in communicating with the employee source to ensure that the employee retains the flexibility to consider all options in making choices about the best, and safest, ways to disclose information.

As discussed earlier, there might be benefits to a source being connected publicly with his or her disclosure. But there are many cases where protecting confidentiality is of utmost importance. Below are some best practices that can help protect communications with whistleblowers.[12]

Sources should not contact advocacy groups using work-related email accounts, computers, or telephones. Whistleblowers who are current employees should use non-work computers scanned for monitoring software or malware that could be used to record their activities. They also should consider using both secure operating systems that the individual controls and an anonymous web browser (such as Tor). Sources can also enhance their security by completely deleting communication histories and stripping metadata from messages and attachments, which will help minimize the risk of unintentionally sending information automatically embedded in digital documents. If electronic communication is necessary, secure encrypted communications tools should be used.[13]

In-person meetings may be preferable. Given modern technology, tracking an in-person meeting is often more difficult than tracking a digital connection, but it is not impossible. **When meeting in-person, parties should:**

- consider whether there are cameras that could record the meeting;
- leave their cell phones behind to avoid detection through location services on all smartphones;
- meet a source away from buildings to avoid security cameras or building visitor logs, if possible; and
- specify a meeting location where the source or the organization's staffer is not likely to be recognized. With these safety criteria in mind, the best location is the one picked by the whistleblower as most safe.

12 Special acknowledgements to our allies at the Project On Government Oversight for sharing their expertise on best practices regarding secure communications with employee sources.

13 Current tools used to protect communication privacy include Signal for calls and texts, encrypted email such as ProtonMail or Peerio, and SecureDrop to receive documents.

Be careful about how you ask for documents. It's always better to phrase a request as "How could I obtain documents to back up what you're saying?" rather than directly ask a source to provide actual documents. For classified documents, note that it might be illegal to instruct or directly aid a source in sharing classified information with someone who does not have the proper clearances or "need to know."

Handle electronic documents with care. Be careful about transmitting documents electronically, especially if they are going through a third party. Anything sent via email (e.g., Gmail), stored on Google Drive, or added to an internal calendar could be subject to a subpoena issued to the third-party service that may not be as committed to protecting the identities of its users. Sensitive information should always be sent via encrypted email and contained only on the organization's private computer networks.

Use Signal or encrypted email for communication and document exchange. Encrypting emails makes it so the content is only readable by you and the recipient. If encrypted properly and without compromise (i.e., free from malware that allows spying on your or the whistleblower's computer activities), the government will only be able to see the metadata of the email (e.g., the header information containing details about the email recipient and sender, the date and the subject line), but the content of the message will remain encrypted and unreadable. Signal is a mobile and web app that provides end-to-end encryption. Using Signal provides the same benefits as encrypting email, but is more user-friendly because it works like text messaging. Signal also allows for attached documents. If you are using Signal, be sure to secure your phone with a pin or passphrase. You can also set a password for the Signal app itself and set messages to expire after a certain time period. Consider moving the Signal app to be next to your other text messaging apps to encourage more frequent use.

Store sensitive documents securely. Ideally, sensitive paper documents should be stored in a secured office, safe or locked file cabinet. Electronic documents can be encrypted and stored on a flash drive that can then also be stored in the secured physical location after deleting unencrypted copies stored elsewhere. Be careful about storing sensitive documents on personal laptops. Sensitive documents should not be left on desks unless in use.

Be cautious about original documents. Do not post the originals online, where identifying features could be discovered. Printers leave nearly invisible identifying markings that can be used to track down the source of the disclosure. If you insist on posting sensitive documents, consider re-creating or re-typing your own version for use or disclosure.

Remove metadata from documents or photos posted online. Make sure to remove the metadata, such as the location a photo was taken, a watermark, or track changes. You can use tools like Document Inspector (which can remove metadata from Microsoft Office files) to remove much of this information. If you are redacting names or other information from a PDF by covering it with black bars, make sure you've actually permanently hidden the information. Export your file as a JPEG, then make it a PDF again, otherwise someone will be able to delete the redactions you made and see the information hidden under them. When hiding an image, doing it with a full black block will always be safer than blurring it.

Do not give original documents, or anything else, to another source while verifying your source's allegations. You may trust your other contact, but you should not take the risk—many agencies and businesses have implemented "insider threat" programs to deter and detect perceived threats to information security. These programs encourage employees to report suspicious activity. Be careful even describing the information and how you obtained it to avoid putting your verifying source in a position of choosing between loyalty to you or loyalty to their employer.

Protect your communication with your coworkers about your source. At times, the government and corporate sectors have spied on advocacy organizations to monitor their work and to find their information sources. Locking sensitive files in a dedicated room, locking computers, using encrypted tools to discuss sensitive issues or the source are all important best practices to implement in the workplace.

Install an app to remotely wipe your phone if it is lost or stolen by activating the Android Device Manager for Android devices and the Find My iPhone on iCloud.com for iOS devices.

Be careful about crossing international borders, particularly U.S. borders, with sensitive information on your phone and computer, including names and contacts.[14]

14 For more detailed information about protecting information when crossing international borders, *see* Esha Bhandari, Wessler & Yachot, "Can Border Agents Search Your Electronic Devices? It's Complicated," American Civil Liberties Union (March 14, 2017).

Protecting Whistleblowers, Protecting Your Organization

Work with Whistleblower Lawyers

If your organization is considering working with or acting on information provided by a whistleblower, it is wise to consult with a lawyer with whistleblower expertise before using material supplied by an employee source.

Advocacy organizations employ a wide range of strategies and tactics to achieve their missions, such as policy development and advocacy, grassroots and grasstops organizing, coalition building, media outreach, research and investigations, public education, trainings, statistical analysis, congressional and agency oversight, and litigation.

Information provided by a whistleblower can bolster many of these strategies to create change. For example, a disclosure by an employee about environmental dangers could prompt your organization to conduct its own investigation, urge an agency oversight or congressional hearing, organize local community members, or file a citizens' suit. Disclosures about fraud or corporate misconduct could drive a shareholder campaign, initiate a boycott, or create an opportunity to advance regulatory reforms. Serious evidence of wrongdoing provided by an insider can exponentially leverage opportunities for reform.

Always remember, though, that while the whistleblower came to you with the intention of having the information used so the problem identified might be addressed, what is in the whistleblower's best professional interest to minimize the risk of reprisal may conflict with various advocacy strategies.

For instance, you may want your source to publicize the disclosures in the media, but a journalist's interest is to secure and publish the story. Failing to carefully choose which journalist to work with—one ideally with a depth of knowledge to do justice to the whistleblower's disclosure and who has experience and sensitivity in working with whistleblowers—can have the consequence of recklessly exposing the whistleblower to retaliation.

For whistleblowers who have evidence of significant corporate fraud, disclosing information in a public way might prevent the opportunity for that whistleblower to file a lawsuit that could offer them the "insurance" of potentially receiving a percentage of the fraud recovered by an enforcement agency or to pursue their own private enforcement action.[15] Pursuing the path of litigation, particularly litigation that is protected by a degree of confidentiality, may have the attendant effect of precluding other forms of activism based on the whistleblower's disclosure, but it may be the safest path for the employee and the most effective for long-term reform.

Since most employees, as well as most public interest staffers (even lawyers), are not readily aware of the wide range of strategies and potential risks and benefits of choosing different advocacy tactics, being conscious of these potential conflicts will go a long way in promoting trust, preventing undesirable consequences, and choosing safe and effective strategies.

Lawyers can be important resources, serving as useful partners in developing an understanding of the facts and the implications of the issues without damaging your relationship with the whistleblower. **Experienced legal counsel will ensure both the whistleblower and your organization have full awareness of rights, risks and possible strategies to disclose information safely and effectively.** Additionally, communications with one's lawyer for the purpose of obtaining legal advice are shielded by the attorney-client

15 The False Claims Act, the Dodd-Frank Act, the Endangered Species Act and IRS regulations offer "bounties" to whistleblowers for being the first to report evidence of fraud, and some offer the option to bring a private enforcement action even if the government declines to pursue the claim.

privilege, the strongest confidentiality protection that exists.[16]

Referring an employee who wants to share information to an experienced attorney, and offering to work with the whistleblower and the lawyer to ensure that advocacy efforts are undertaken responsibly to both promote reform and protect the source, will help build trust with whistleblowers by demonstrating that your organization cares and is paying attention to their welfare. Advocacy groups who work with whistleblowers will be the good and bad advertisements for others who consider coming forward to share their knowledge. New potential whistleblowers might come forward if earlier whistleblowers are treated wisely and well.

PRO TIPS

- **Be transparent with whistleblowers about the fact that you are neither employment lawyers nor personal strategists.**
- **Be clear that you are a source of support and solidarity, but do not give whistleblowers false ideas about your power to protect them.**
- **Seek legal advice from attorneys with expertise in whistleblowing before using information publicly that was provided by whistleblowers, particularly if that information comes from a current employee. Advise whistleblowers to do the same.**

Procuring Counsel

Most lawyers do not have experience with whistleblower law and do not fully appreciate that clients have competing interests: job security but also public interest concerns. Lawyers should try to help the client weigh those competing interests rather than assuming job security is the employee's only, or even primary, priority. A list of organizations that either offer legal support to whistleblowers or have extensive experience working with whistleblowers and can offer referrals to experienced attorneys is located in the Resources section of this Guide.

16 Having outside advocates in meetings between whistleblowers and their counsel can break the attorney-client privilege, so precautions are mandatory.

Use Alternative Avenues to Investigate Disclosures

Freedom of Information Act (FOIA): You do not always have to put your source at risk to get the story. In fact, for public employees, you may not even need to bring the whistleblower into the story if there are internal documents that could do the same thing. If your source has information that could show wrongdoing by the government, tutoring you to craft the right FOIA requests can offer another route to gain access to those materials. If the agency denies their existence, the whistleblower can potentially work discreetly with the FOIA officer to point out the falsehood and make the illegal cover-up backfire.

PRO TIP

→ If you are too precise with your FOIA requests, you could tip off an agency that they've got a whistleblower, and even who the whistleblower is. Plus, what your whistleblower disclosed could perhaps show a general trend. Get more data rather than drilling down on something that could have only come from your whistleblower.

Use an intermediary: A whistleblower protection organization like GAP can serve as a buffer, working closely with advocate allies to leverage information provided by a source while offering legal protection to the whistleblower. Similarly, whistleblower protection organizations can serve as middlemen, providing the whistleblower's information to a friendly congressional[17] or agency staff member while offering legal protection from potential reprisal. Careful government investigators can then work directly with the advocacy group or journalist on the problem disclosed, or can conduct investigations and issue subpoenas seeking a broad swath of documents related to the disclosure without revealing the source of the inquiry.

17 Both the Senate and the House have Whistleblower Protection Caucuses made up of members who prioritize whistleblower protection.

Advise Whistleblowers on Best Practices

You can help your source mitigate risks by alerting them to a few basic best practices he or she should consider when deciding to blow the whistle:

1. **Before exposing themselves to risks, whistleblowers should talk to an experienced lawyer so as to make an informed choice about taking those risks.** Also, if an employee drops out in the middle after realizing the price of dissent, wrongdoers will be better off by being able to cover up evidence and chill future employees from blowing the whistle.
2. **They should consult with their loved ones, who will be sharing the consequences of the whistleblowing to a significant degree, before taking the risk.** If whistleblowers make the decision alone to take on the power structure, they may well end up alone. Loss of family is far worse than loss of job.
3. **They should continue to work within their system as long as possible without incurring suspicion.** It can backfire badly for a whistleblower to make aggressive internal allegations from a lonely perch of isolation. By contrast, without making charges, whistleblowers can be the insider eyes and ears that allow NGOs to stay one step ahead of their adversaries. If whistleblowers raise issues internally in a non-threatening manner, they can learn and share with NGOs the advance previews for cover-ups.
4. **They should create a contemporaneous paper trail or diary of everything that happens,** including when they raised complaints and issues, and whether they faced any retaliation.
5. **They should keep evidence in a safe place.** Authorities usually are not limited in access to the whistleblower's workplace, but home storage of documents can also be risky, potentially subjecting a whistleblower to a pretextual but seemingly valid discipline and harassment such as expanded retaliatory investigations. Since agencies have subpoenaed, searched and ransacked homes, the best choice is to secure the evidence with the whistleblower's attorney, where it is shielded by attorney-client privilege.
6. **Without giving themselves away, they should test the waters and organize support for themselves among their colleagues,** if possible. This is necessary for quality control. A second set of eyes can ensure the accuracy and legitimacy of the concern. Seeking support can also determine whether there is a sufficient solidarity base of supporting witnesses for the disclosure to have an impact. If the whistleblower is isolated, making allegations alone again could backfire by guaranteeing that those engaging in misconduct will weather the storm.
7. **If there are legitimate liability concerns attached to blowing the whistle, coach them on how to secure and protect evidence without removing it.** Tactics such as taking cell phone pictures on a personal (not work) phone can secure documents that otherwise would be destroyed. Whistleblowers can also reproduce memorized documents at home.

Keeping an index of critical documents is another strategy, as is hiding incriminating documents and electronic records in a camouflaged (misnamed) file in their work computer so that they are not lost and can be shown to law enforcement later if an employer tries to destroy evidence. These strategies can help prove the whistleblower's claims while limiting vulnerability to charges of theft of records. If there is uncertainty, do not keep records without a legal opinion confirming lawfulness.

8. **If maintaining anonymity is a priority, they should communicate with you through secure means,** including using Signal, SecureDrop, or snail mail with no return address.

9. **Your source should not contact you while they are at work.** A whistleblower should not use work equipment either, including office phones, computers, or even paper. Otherwise, he or she can be fired for engaging in personal business with the employer's time and resources.

10. **They should turn off location tracking in their phone before taking any pictures of documents, and strip any metadata from documents before sending them.** NGOs are well-advised to maintain a relationship or retainer with professionals experienced in removing traceability.

11. **Use an advocacy group as the beach head for a coalition.** Solidarity is the magic word for whistleblowers to make a difference and survive. It can be a fatal mistake for an employee, or a public interest organization, to try to do everything alone. Normally a hostile bureaucracy surrounds the isolated whistleblower. The most effective contribution an organization can make is to facilitate strategic matchmaking—getting the truth into so many hands that an awakened, informed majority of stakeholders surrounds the bureaucracy, reversing the balance of power.

With the whistleblower's support, prepare a joint strategy so the institution is on the defensive against the NGO-whistleblower team, rather than the whistleblower defending against attacks. When whistleblowers take on giant institutions, they only can prevail through guerilla warfare, with tactics that force bureaucracies to respond to them rather than vice versa. If the conflict is solely grounded in conventional legal warfare, the odds are nearly hopeless. The dissenting team will drown in the workload inherent when institutions pile it on in conventional litigation, which is their turf.

Conclusion

Public interest organizations are essential to a healthy civil society and robust democracy. Whistleblowers are invaluable partners who, through the power of information and transparency, can advance reform efforts for public good. Supporting whistleblowers, first through awareness of their important roles as truth-tellers in society, and second by using best practices that recognize the professional risk involved with reporting wrongdoing, will ultimately serve the interests of both the advocacy group and the whistleblower in their shared goals of advancing the public's interests.

Resources

Contact GAP

The Government Accountability Project (GAP) is the nation's leading whistleblower protection and advocacy organization. A non-partisan public-interest group, GAP litigates whistleblower cases, helps expose wrongdoing to the public, and actively promotes both government and corporate accountability. Our longstanding work with whistleblowers has involved fighting for accountability for decades in the areas of public health, food safety, national security, human rights, energy and the environment, finance and banking, and international institutions and expanding whistleblower protections domestically and internally.

GAP is available to offer legal and strategic advice and support to public interest organizations and their whistleblower sources, both government and corporate.

Contact us by email
info@whistleblower.org

Contact us by phone
202.457.0034

Other Whistleblower Support Organizations

ExposeFacts

https://whisper.exposefacts.org

ExposeFacts is a journalism organization that aims to shed light on concealed activities that are relevant to human rights, corporate malfeasance, the environment, civil liberties and war. They offer legal support to national security whistleblowers as well through their Whistleblower and Source Protection Program (WHISPeR).

Project On Government Oversight (POGO)

http://pogo.org

POGO is a nonpartisan, independent watchdog organization that promotes good government reforms by investigating and exposing corruption, misconduct and conflicts of interest. POGO frequently works with government whistleblowers to and other inside sources to document evidence of corruption, waste, fraud and abuse.

Public Employees for Environmental Responsibility (PEER)

https://www.peer.org

Public Employees for Environmental Responsibility (PEER) is a national alliance of local state and federal government scientists, land managers, environmental law enforcement

agents, field specialists and other resource professionals committed to responsible management of America's public resources.

Whistleblower Aid

www.whistlebloweraid.org

Whistleblower Aid is a new non-profit law firm that focuses on federal government whistleblowers, with special emphasis on helping employees expose wrongdoing without unlawfully releasing classified information.

Books/Articles on Whistleblowing

Devine, Tom and Tarek F. Maassarani. **The Corporate Whistleblower's Survival Guide: A Handbook for Committing the Truth**, Berrett-Koehler (2011)

GAP, POGO & PEER, **The Art of Anonymous Activism: Serving the Public While Surviving Public Service** (PDF), (2002) (updated version forthcoming)

Kohn, Stephen, **The New Whistleblower's Handbook: A Step-By-Step Guide To doing What's Right and Protecting Yourself**, Lyons Press; 3rd Ed. (2017)

McCutcheon, Chuck, **"Whistleblowers,"** CQ Researcher, 24.5 (Jan. 31, 2014)

Zuckerman, Jason and Eric Bachman, **The Whistleblower Protection Act: Empowering Federal Employees to Root Out Waste, Fraud and Abuse** (PDF), Zuckerman Law (2017)

Information Security

Freedom of the Press Foundation
Guides and Training
https://freedom.press/training/

Open Source News
Protecting Your Sources When Releasing Sensitive Documents
https://source.opennews.org/articles/how-protect-your-sources-when-releasing-sensitive-

Working with Whistleblowers Tip Sheet

1. **Do no harm.** Whistleblowers are uniquely vulnerable to reprisal. Because the legal landscape protecting whistleblowers is complicated, make source protection a priority.

2. **Contact a lawyer or organization experienced in helping whistleblowers.** Legal organizations and lawyers who understand the rights and risks of whistleblowing ensure the employee can make informed choices about how to proceed effectively and safely, while ensuring the employee has the benefit of the attorney-client privilege. GAP (www.whistleblower.org) offers pro bono case evaluation and can offer referrals to other legal organizations and lawyers.

3. **Don't promise what you can't deliver.** Many advocacy organizations (and whistleblowers) want to use information while keeping the source anonymous. But anonymity often can't be guaranteed because sources can be identified by earlier internal disclosures, the employee's job responsibilities or expertise. Also, because public interest groups cannot typically invoke the protection of attorney-client privilege, it may be difficult and expensive to refuse to comply with a subpoena seeking its sources. Don't over promise when it comes to protecting your source.

4. **Public disclosure might be more effective.** Disclosing information publicly can insulate the employee from retaliation by making it clear the employee is exercising his or her right to blow the whistle. It also helps strengthen a whistleblower's legal case if they do suffer reprisal, because it will be easier to show the employer was aware the employee reported serious concerns. Going public can also help the whistleblower build an advocacy campaign to prompt change.

5. **Advise whistleblowers on best practices.** Whistleblowers are not activists and are often unfamiliar with the world of news, politics or advocacy. Remind them to protect records and document the wrongdoing, their actions, and any retaliation. Help them do that in ways that will insulate them from charges of theft of records.

6. **Engage in secure communication with the whistleblower.** If the source is a current employee, he or she should not contact you while on the job or use office equipment, including work phones, computers or paper. Use Signal or other encrypted platforms for secure communication and document exchange. Meet in person in safe locations without cell phones to avoid tracking.

7. **Remember that a person is attached to the information**. Your support can make a world of difference.

www.whistleblower.org

202.457.0034

Working with Whistleblowers: A Guide for Public Interest Organizations