Working with Whistleblowers

A Guide for Journalists

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

CONTENTS

Working with Whistleblowers

A Guide for Journalists

Information shared by whistleblowers—employees who discover and disclose evidence of serious abuses of public trust—can take down a corrupt CEO or corporation, drive significant legislative and agency reforms, save lives from contaminated food, prevent nuclear accidents, and prompt the impeachment of a President.

As concerns about corruption, wrongdoing and serious threats to public health, safety and the environment increase, so does our dependence on whistleblowers' willingness to speak up as a mechanism to promote accountability.

The power of whistleblowers to hold institutions and leaders accountable very often depends on the critical work of journalists, who verify whistleblowers' disclosures and then bring them to the public. The partnership between whistleblowers and journalists is essential to a functioning democracy.

Journalists and legitimate media outlets are under unprecedented attack even as their role as watchdogs empowering the public with information is more important than ever. Similarly, whistleblowers who reveal serious wrongdoing committed by their employers have always faced the risk of professional and personal reprisal, but never more so than in today's political environment. The need for both whistleblowers and journalists has escalated, but so has their vulnerability.

Whistleblowers who may reach out to journalists with information generally aren't activists. Rather, they are typically employees who have tried to raise concerns with their management and were frustrated by the response and/or harassed.

They care deeply about wanting to address the problems they have discovered and are uniquely credible as inside sources. Because of their unique knowledge, however, they pose a unique threat to their employers and are especially vulnerable to reprisal.

Competition among media outlets for inside sources' information is fierce. But maximizing the effectiveness of a whistleblower's disclosures while minimizing their risk can be complicated. Journalists need to understand not only the value of a whistleblower's information but also the unique challenges and risks faced by sources who are employees. A relationship with a journalist can be the highest stakes and most stressful partnership in a whistleblower's professional life. Earned trust lays the foundation for this partnership to work. Word will quickly spread about a journalist or news outlet that uses and abandons whistleblowers, that exposes them to retaliation, or that fails to provide solidarity when harassment occurs. Then the flow of information will dry up.

The Government Accountability Project (GAP) has represented and advised over 8,000 whistleblowers since 1977. GAP is a lifeline for employees of conscience. We verify and present their concerns to public officials, NGOs, and journalists and seek legal justice for them when they suffer retaliation. GAP has unique expertise navigating the dangers confronting whistleblowers—over the past four decades, we have drafted, led the campaigns to pass or helped defend all the federal whistleblower protection laws that exist today.

GAP partners with media outlets and investigative journalists to promote accountability based on disclosures by whistleblowers who seek our assistance. This guide seeks to empower and protect journalists and their whistleblower sources by sharing critical information to them both—from the gaps to the common ground in their goals, responsibilities and challenges.

We are excited to work with any reporter who needs help navigating the legal terrain associated with whistleblowers. We recognize the importance of exclusivity for a journalist working on a story. If you come to GAP with a whistleblower, we

will maintain your exclusivity. We will be cautious and get your consent before speaking to anyone about the case because we are aware that stories can come out in many ways. We would keep you in the decision making loop about any outside moves, like speaking to congressional staff or filing a lawsuit.

By offering information critical to understanding the complex issues involved with an employee's decision to disclose evidence of serious wrongdoing, abuses of authority and threats to the public interest, we hope to help journalists have whistleblowers' backs, rather than unwittingly exposing them to further retaliation. While by no means comprehensive, we hope this guide not only generates support for the important function whistleblowers play in advancing civil society, but also awakens awareness for the special care required when utilizing whistleblowers' information.

Whistleblowing 101: A Short Primer

What is a Whistleblower?

In common terms, whistleblowers are individuals, typically employees, who use free speech rights to expose abuses of power that betray the public trust. Under the Whistleblower Protection Act (WPA), the primary law that protects **non-intelligence federal employees**, they are defined as employees who disclose information, either internally (to managers, organizational hotlines, etc.) or externally (to lawmakers, regulators, the media, watchdog organizations, etc.), that they reasonably believe evidences:

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

For classified information or information that is specifically barred from release by statute, the WPA only shields disclosures made to the U.S. Office of Special Counsel, the agency Inspector General, or an employee designated by the agency chief to receive them.

Federal employees covered by the WPA also have the right:

- to report censorship related to scientific research or analysis that would result in one of the five types of misconduct described above; and
- to refuse to obey an order that would require the individual to violate a law.[1]

1 See Whistleblower Protection Act of 1989, 5 U.S.C. § 2302(b)(8) & (b)(9); Whistleblower Protection Enhancement Act of 2012, § 110(b)(1).

While the Whistleblower Protection Act does not apply to all employees (more on the legal landscape is discussed below), its definition of what constitutes a whistleblower captures two key points. First, a whistleblower typically is a current or former employee with direct and credible information about wrongdoing. Second, the concern is serious and its disclosure promotes legal compliance or protects the public interest.

The Majority of Whistleblowers Report Internally First

After discovering wrongdoing, more than 95% of whistleblowers first try to solve the problem internally.[2] Many whistleblowers are loyal to their employer and believe raising concerns will address the problem. Often they seek external support only after an employer fails to address the problem or attacks the messenger.

Cynicism, or lack of belief that challenging misconduct will make a difference, overwhelmingly is the primary reason why would-be whistleblowers remain silent observers. Fear of retaliation is second, but a distant second. This means whistleblowers are sizing up your trustworthiness when deciding whether to share their knowledge with you.

In many cases, both strategically to sustain the flow of information and defensively to avoid harassment, it is of primary importance to whistleblowers that your communications with them remain undiscovered.

Because whistleblowers often report internally, and/or because the information is tied to their work, they have likely left fingerprints on the issue. If reporters are not

2 See Ethics Resource Center, "Inside the Mind of a Whistleblower: A Supplemental Report of the 2011 National Business Ethics Survey" (2012). http://www.corporatecomplianceinsights.com/wp-content/uploads/2012/05/inside-the-mind-of-a-whistleblower-NBES.pdf

careful handling evidence, employers might discover who blew the whistle. Even a FOIA request that is too specific might set off alarms.

The Risk of Reprisal & the Complicated Legal Landscape

No matter how right they are about wrongdoing, corruption, and public safety threats, as a rule employees who speak out suffer reprisal rather than thanks for identifying serious problems. It may begin with a retaliatory investigation, then be followed by isolation, gag orders, cancellation of meaningful duties, reassignment to undesirable job assignments, public humiliation, surveillance, management efforts to recruit complaints by peers, poor performance appraisals, threats, harassment, denials of promotions, psychiatric exams, termination, violence, law suits, criminal investigations, or efforts to seek prosecution.

Despite the standard legal definition of a whistleblower, no single law protects employees who disclose evidence of serious wrongdoing. Instead, a patchwork of more than 60 federal statutes and numerous state and local laws protect and provide redress for whistleblowers, While there may be legal protection available for your source, he or she could also fall through the cracks.

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

- **The nature of the information exposed.** Most corporate whistleblower protections are essentially witness protection provisions, with the many federal environmental, financial, transportation safety, food safety or occupational safety laws containing anti-reprisal provisions to protect employees who report possible or actual violations of those laws in order to promote compliance and enforcement. Others are like the federal WPA that protect reports of nearly any significant abuse of authority with consequences for the public.

- **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, or a state or municipal employee. Available protections also differ depending on which state the whistleblower lives or works.
- **If the information is classified.** Whistleblowers have no legal protection to publicly release classified information. Indeed, it is a criminal offense for which they could be prosecuted. 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.
- **The type of reprisal experienced.** Poor performance appraisals, job reassignment, demotion, psychological exam, security clearance revocation, termination: the forms of harassment are limited only by the imagination, and the federal WPA only protects against some reprisals. 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.
- **How and to whom the disclosure was made.** Whether protection exists can depend on whether the whistleblower disclosed concerns as part of his or her job duties; on personal initiative; internally to co-workers, supervisors, union representatives, ethics officers, ombudspersons; or externally to Congress, an Inspector General, an oversight agency, a watchdog organization, or the media. The order of to whom a whistleblower reports concerns can also matter depending on the available legal protections.
- **When the employee became aware of the reprisal.** Statutes of limitations differ widely, ranging from 30 days to three years or none.
- **Where the disclosure was made.** Local and state protections vary significantly, and may or may not be preempted by a federal remedy.

In addition, laws protecting whistleblowers have different remedies, different procedural steps and different avenues for enforcement. Even if a whistleblower

has protection, cases can take many years to resolve. Some laws provide temporary relief in some circumstances where the government has verified the reprisal; other laws do not, and as such encourage employers to delay resolution.

The legal landscape's complexity makes it difficult for employees, and even lawyers inexperienced with helping whistleblowers, to assess the risks and benefits of various disclosure strategies. That is why both whistleblowers and journalists should consult a lawyer with expertise in whistleblowing before releasing information. It can be professionally fatal not to know the lay of this land.

Will Lawyers Kill the Story?

When a whistleblower starts consulting with a lawyer, sometimes they stop talking to journalists. Lawyers have to act in their client's best interest to reduce risk, and whistleblowing is risky business. Lawyers also validly need to control developments in cases for which they are responsible, and some lawyers view the media as a wild card. For example, evidence involved with litigation released prematurely by the press could affect trial or settlement strategies or identify the whistleblower. Being duty-bound to protect their client's interests, many lawyers may warn clients not to speak with the media in order to minimize the risks associated with working with those whose interests differ from or conflict with their clients'.

However, the lawyer works for the whistleblower, not vice versa. The whistleblower's professional life is on the line, not the lawyer's. This means the proper boundary for a lawyer's role is recommendations, not orders or threats to withdraw from the case upon failure to follow advice.

How should journalists balance the conflict of wanting to publish a potentially ground-breaking story while knowing that the whistleblower source may be best served by consulting with a lawyer first? Journalists should not hope their source avoids getting proper outside legal advice, or worse, discourage them from doing so. Instead, they should research and match-make potential whistleblowers with the right lawyers – those who support responsible whistleblowing but know where

all the traps are. 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.

There are also occasions when blowing the whistle publicly may be the best recourse for the employee's security. For example, if employees have already raised concerns internally, they are uniquely vulnerable, so blowing the whistle externally and loudly rather than retreating might be both the safest and legally strongest course of action. Depending on the circumstances, "half-way" whistleblowing can easily leave the whistleblower with the worst of all worlds, isolated and unemployed, without having made a positive difference. However, only lawyers with a thorough understanding of the law will be able recognize when to implement that strategy.

GAP is unique in that we not only know how to blow the whistle safely, but our mission often relies on effective partnerships with NGOs, journalists, and agency and congressional staff. We have lawyers on staff or we partner with other attorneys to ensure whistleblowers have the benefit of attorney-client privilege, a heightened level of protected confidentiality. This can help whistleblowers work with journalists at less risk to themselves.

Other organizations, such as the Project on Government Oversight (POGO), ExposeFacts, and Public Employees for Environmental Responsibility (PEER) have similar expertise and are interested in working with whistleblowers to seek reform.[3]

3 See Resources, p.30, for more information about these organizations.

Reach out to us; it won't kill the story. Because the risk of reprisal for whistleblowers is high and the legal landscape is complex, both journalists and sources would be well served to consult or coordinate with GAP or other lawyers versed in whistleblower law before acting on information supplied by an employee source. Lawyers can be important resources, serving as useful partners in their understanding of the facts and implications of the issues while also maintaining your exclusivity and nurturing your relationship with the whistleblower.

Whistleblowing Is (Usually) Not a Crime

Intelligence Employees v. All the Rest

The aggressive prosecution by the past two Administrations of intelligence employees whose disclosures of classified information exposed government illegality and abuse of authority[4] has fueled a widespread narrative and belief that whistleblowing is a crime. However, outside of the intelligence community, internal and external whistleblowing generally is protected activity on a legal pedestal.[5] Since 1978 in the U.S., there has been a unanimous, bipartisan legislative mandate for every whistleblower law enacted to encourage rather than discourage disclosures of serious concerns.

Intelligence community whistleblowers are unique. Available whistleblower protections mandate internal disclosures while banning external communications, and generally have very weak due process rights. **But most whistleblowers 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.**

4 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. Whistleblower Chelsea Manning's sentence was commuted after serving almost seven years in jail. These high-profile cases shape public perception about whistleblowing generally, sowing the potential misconception that whistleblowing is a crime even when it does not involve the release of classified information. While it should not be a crime to report a crime publicly, a powerful intelligence bureaucracy and the Department of Justice have a different position on this point.

5 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. Because each whistleblower protection law is different as discussed earlier, this is why legal advice sought in advance of disclosure is most valuable.

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. 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, financial fraud, environmental violations, or public health and safety threats are engaging in *legally-protected activity*, not committing crimes by reporting evidence of crimes or other wrongdoing. Employers responsible for the wrongdoing and those who engage in reprisal are the ones risking investigations and enforcement actions.

Risks of Criminal and Civil Liability Outside of the Context of Classified Information

Unfortunately, public prosecutions of national security whistleblowers have emboldened new efforts to criminalize whistleblowing in non-intelligence contexts. "Ag-Gag" legislation exists in some states that criminalizes the publication of photo and video documentation at industrial agricultural facilities, though courts have found some of these laws unconstitutional. Corporate employers seek, and occasionally secure, criminal prosecution of employee whistleblowers for "theft" of company property which proves the company's crime. Firms on occasion threaten to or even file multi-million dollar "SLAPP" suits[6] against whistleblowers for violations of non-disclosure agreements or alleged defamation. Government agencies are increasingly referring employees for criminal investigations and prosecutions when they engage in protected whistleblowing activity. The consequences of these aggressive harassment strategies can be far more destructive, and effective, at terrifying employees into silence than conventional

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

employment reprisals like termination. When exposed, those inappropriate referrals can and should spark a backlash on the employer.[7]

While assertions by employers that evidence of the wrongdoing was wrongfully acquired have weak merit, knowing the potential vulnerabilities of your whistleblowing partner to such allegations should prompt you to counsel caution. You should encourage them to engage trustworthy counsel and help them to shield their actions, plans and strategies with an attorney-client privilege, an even stronger confidentiality protection that a reporter's privilege. You can also counsel whistleblowers on how to prove their point without "stealing" corporate records. For example, the whistleblower can keep an index of critical documents, take a screen shot of records that remain in the office, or hide incriminating documents and electronic records in a camouflaged (misnamed) file in their work computer so that they are not lost if their employer tries to destroy evidence, and can be shown to law enforcement later.

Whistleblower laws generally protect the right of employees to report serious misconduct, even when the employees are ultimately mistaken about their concerns as long as there was a reasonable basis for their assertions. It is important, however, not to underestimate the risk of aggressive reprisal strategies in the form of threatening lawsuits filed by a defensive employer 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.

Is it Leaking or Whistleblowing?

Frequent conflation of the terms "leaker" and "whistleblower," typically invoked in relation to anonymous disclosures of classified or confidential information, sows

7 Retaliatory investigations and prosecutions are not a new form of reprisal. For in-depth case studies of retaliatory criminal investigations, view GAP's 2010 report, "Whistleblower Witch-Hunts: The Smokescreen Syndrome."
https://www.whistleblower.org/sites/default/files/WWHfinal.pdf

confusion about what these terms actually mean. While there is some overlap, they have distinct identities. A "leaker" is the anonymous source for unauthorized disclosure of any information. A "whistleblower" makes a public interest disclosure, and may be either anonymous or public.

The term "whistleblower" means someone who is disclosing information about breaches of the public trust and is objectively significant for exposing those violations. This is reflected in the legal standards for protected whistleblowing activity—disclosures an employee reasonably believes evidence illegality, gross waste or mismanagement, abuse of power, or a substantial and specific danger to health, safety or the environment. Whistleblowing inherently means the disclosure serves to protect the public interest and promote public safety and accountability about illegality and other breaches of public trust.

Employees with serious concerns, particularly those who work in the intelligence community where evidence of wrongdoing may be classified, are sometimes driven to **blow the whistle anonymously** to the press. These disclosures are typically described as "leaks" by the officials responsible for the exposed misconduct, and are often met with aggressive "leak investigations" and prosecutions.

Characterizing the source responsible for disclosing evidence of serious wrongdoing as a "leaker" is often a deliberate move to delegitimize both the source and the information. While the term "whistleblower" has historically had pejorative associations, the terms "leaker," "leaking," and "leaks" have even greater negative connotations. To qualify as a whistleblower, a disclosure must credibly raise serious concerns affecting the public interest. Leaked information may be interesting to the public, but it does not necessarily expose illegality, gross wrongdoing or imminent threats of harm. Leaks, frequently politically motivated or offered to curry favor with journalists, may involve sensitive information but do not rise to the level of seriousness of a protected whistleblower disclosure.

These distinctions matter. Most whistleblowers have the right to make disclosures they reasonably believe show violations of a law, rule or regulation, abuse of

authority, gross mismanagement, gross waste of funds, or a substantial and specific danger to public health and safety. Intelligence agency whistleblowers, because of the national security implications of potential disclosures, need to follow specific internal procedures to report their concerns. While these procedures and protections are inadequate, the law recognizes the disclosures as legally-protected, not misconduct.

Different standards exist for **intelligence community contractors** like Edward Snowden or Reality Winner. While their avenues for disclosure are the same as intelligence community employees, with one exception their protections are virtually non-existent. They are protected under Part B of President Obama's Presidential Policy Directive-19, but that only prevents an employer from stripping away their security clearance. The double standard is particularly baffling, since the stakes are higher for contractor employees due to limited government oversight.

There are other problems plaguing justice in this arena. All leading experts argue that too many documents are classified. It is easy to classify documents and often impossible to declassify them. Frequently embarrassing and even illegal actions are buried through overclassification. Furthermore, favored government officials who illegally possess, store, and provide classified information to journalists are rarely punished, and if then only lightly. In contrast, whistleblowers are harshly punished, branded as "leakers," rendered unemployable and even prosecuted as spies with no available public interest defense. The Department of Justice, during one such trial, asserted that whistleblowers who disclose information via the press are worse than spies who sell classified information for money to just one country, because whistleblowers' disclosures may benefit every foreign adversary.

As a result of these legal weaknesses and double-standards, some intelligence whistleblowers choose civil disobedience whistleblowing by offering classified disclosures to the public. While employees who choose this route have no legal protections for making disclosures, and indeed can be criminally prosecuted without the right to invoke a public interest defense, they should still be considered

"anonymous whistleblowers" rather than "leakers" if the nature of the information meets the standard threshold for unrestricted whistleblowing disclosures.

Conflating "anonymous whistleblowing" with "leaking" can contribute to the chilling effect for all employees who might witness illegality and abuses on the job. Whistleblowers are already fighting an uphill battle to hold the powerful accountable, and being denigrated as a "leaker" erodes their ethical high ground as a "whistleblower."[8] Journalists can help advance support for whistleblowers through their language choices when reporting.

Classified Information

Disclosing classified information is a felony. 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. Pronouncements by the Department of Justice to escalate prosecutions of whistleblowers and threats to force journalists to reveal their sources or risk prison necessitate that both the whistleblower and the journalist should be exceedingly careful and aware of the risks involved.

A few key points about working with classified information are worth noting. First, under the statutory definition in the Intelligence Identities Protection Act, the information must be marked as classified or specifically designated as such orally to qualify as classified information. Second, whistleblowers are generally able to sanitize any classified knowledge by focusing on the consequences of the problem or pointing to relevant unclassified documents, so long as they do not disclose any classified information. Finally, under Executive Order 13556, agency "pseudo-classifications" such as "Controlled Unclassified Information," "Sensitive Security Information" or over 100 other agency secrecy categories do not restrict

8 *See* Dana Gold, "James Comey Is Not a Leaker. He is a whistleblower." Slate (June 9, 2017) http://www.slate.com/articles/news_and_politics/politics/2017/06/james_comey_is_not_a_leaker_he_is_a_whistleblower.html

a whistleblower's right to disclose it publicly. On paper, liability requires explicit notice of classified information's status. In practice, however, the government often ignores those distinctions. For example, it sought 35 years incarceration of NSA whistleblower Thomas Drake for mere possession of unmarked documents that were classified ***after the fact***.

Be aware, when an intelligence community whistleblower discloses information to a journalist, the employee is likely to be caught, no matter the precautions taken. There will be a leak investigation by the agency's internal threat team with sophisticated means to trace information. Further, employees and contractors with security clearances must go through a reinvestigation every 5 years. To maintain anonymity, the whistleblower either would need to be able to beat a polygraph or blow the whistle within 5 years of retirement and not renew the security clearance (which could be viewed as unusual and attract the attention of leak investigators). Even being placed under investigation is perilous. It creates the dilemma of an employee confessing to a felony leak, or engaging in felony false statements by denying it.

Asking a source directly for classified documents can also put a journalist at risk of prosecution. Directly soliciting a classified document itself isn't advised, for both you and your source's sake.

In addition, never give original documents, or anything else, to another government source or contractor while confirming your story. You may trust your other contact, but you should not take the risk—many agencies have implemented "insider threat" programs to deter and detect perceived threats to national security, including releases of classified information. These programs encourage employees to report suspicious activity. Be careful even describing the information and how you obtained it.

Because of these risks, journalists should not promise total anonymity, because they cannot guarantee it.

Beyond using secure mechanisms for communication, such as snail-mail, Securedrop, Signal, Whatsapp, Tor and email encryption, working with an attorney can be useful to both the journalist and the whistleblower for exploring strategies to protect the whistleblower's identity to minimize the risk of prosecution. Under legal Rules of Professional Conduct, the attorney-client privilege is powerful protection allowing an attorney to speak confidentially with a client without being compelled to disclose those confidences. This allows an attorney to advise clients on how to avoid any violations of law in the proper exercise of their rights and to minimize risks for whistleblowers.

However, an attorney cannot counsel or assist a client in conduct that is potentially criminal. In other words, an attorney could not help a whistleblower to release classified documents, but an attorney could advise the whistleblower about risks and possible disclosure strategies to audiences that not only are legal but legally protected. Those include the U.S. Office of Special Counsel, the Intelligence community or relevant agency Office of Inspector General, and the Senate and House Permanent Select Subcommittees on Intelligence.

Journalists who work with intelligence whistleblowers should realize that any story based on classified information may result in the whistleblower's prosecution. The chances of reprisal are high, and even the most proficiently anonymous whistleblowers often can be traced based on work access or job duties. As a result, journalists should always encourage intelligence community whistleblowers to seek the counsel of an experienced lawyer with specialized expertise in whistleblowing and national security law and to report internally via approved channels.

How You Can Help Your Source

Journalists should not insert themselves into stories; you're not there to be a strategist or offer PR advice, nor can you be the whistleblower's lawyer. But by developing trust and demonstrating awareness of some of the unique considerations involved with whistleblowing, you can encourage reports of valuable information while maximizing your source's protection.

It's All About Trust

If the magic word in real estate is "location, location, location," for journalist-whistleblower working relationships it is "trust, trust, trust." Often whistleblowers are bewildered and scared not only by the risks they have assumed, but by an alien word of strangers, new contexts and new rules of which they are unfamiliar. This usually is an entirely new world for people who do not think of themselves as whistleblowers and have no experience navigating the world of news, politics or advocacy.

Below are some pointers for journalists to earn trust, rooted in GAP's experience:

1. **Honor all commitments,** from scheduling to substantive, or provide advance notice if they must be adjusted.
2. **Be clear about confidentiality** from the beginning, including your commitment to maintaining it along with the true limits of your ability to guarantee it.
3. **Be clear about what protection you can provide**, and what you cannot, to prevent later charges of betrayal.
4. **Partner with a lawyer to protect the source** if you plan to go public with information. A lawyer can help issue advance warnings to an employer of zero tolerance for retaliation, which will create a presumption of misconduct on associated charges and also potentially protect witnesses who might support the whistleblower's claims.

5. **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 abandoned after no longer needed.
6. **Provide a safe environment** for interviews and communications.
7. **Engage in active listening during interview.** Feeling heard is significant for whistleblowers to open up further.
8. **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.
9. **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.
10. **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 almost certainly will crack the case.
11. **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 for other investigations in the future.

Advice for Whistleblowers on Best Practices

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

1. **Before exposing themselves to risks, they should talk to a lawyer experienced in helping whistleblowers.** Part of the reason is so they can make an informed choice about taking those risks. If an employee drops out in the middle after realizing the price of dissent, wrongdoers will be stronger off. It would have been better to remain silent all

along. The other reason is to prevent whistleblowing accidents through first learning the rules of the road.

2. **They should consult their loved ones before taking the risk**. To a significant degree, they will be sharing the consequences. 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, but this is pain that whistleblowers may inflict upon themselves.
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 journalists to fully develop a story. If whistleblowers raise issues internally in a non-threatening manner, they can learn and share with journalists 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 such evidence in a safe place.** Authorities usually are not limited in access to your workplace but it is far more difficult to search a home. Since agencies have subpoenaed, searched and ransacked homes, the best choice is to secure the evidence with their attorney, where it is shielded by the 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. For example, maybe the whistleblower had accurate information but drew the wrong conclusions due to tunnel vision, or there was a new development that resolves the concern. Further, it is necessary to test 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 previously discussed such as taking cell phone pictures of subsequently "misfiled" records can secure documents that otherwise would be destroyed. This strategy can help prove the whistleblower's claims while limiting vulnerability to charges of theft of records.
8. **They should communicate with you through secure means,** including using Signal, Whatsapp, SecureDrop, or snail mail with no return address.
9. **Your source should not contact you during their work hours.** They should not use work equipment either, including their office phones, computers, or even paper. Otherwise, they can be fired for engaging in personal business with the employer's time and resources. Most employees do not even know about such risks.
10. **They should turn off location tracking in their phone before taking any pictures of documents, and they should strip any metadata** from documents before sending them. Journalists should work with professionals experienced in removing traceability.
11. **They should make sure several others possess the documents they provide to a reporter** to minimize the disclosures being traced back to them immediately.

Does Your Source Need Anonymity?

Remaining anonymous is not always the best strategy for a whistleblower. If they have raised the concern internally or if the employer would know from the nature of the disclosure that the employee was the likely source. Trying to remain anonymous while the disclosure is public can make a legal case of reprisal more difficult, if not impossible. Under all whistleblower laws, an employee must show

that the employer had knowledge of their whistleblowing. Thus going public, with the whistleblower serving as a human interest focal point for news stories, can sustain whistleblower's viable legal rights.

Going public guarantees, however, that the whistleblower has burned professional bridges. If a scorched earth, no-prisoners conflict did not already exist, that dynamic is a near-certainty once the whistleblower goes public.

Often whistleblowers need or want anonymity since speaking out publicly may be illegal or invite retaliation. Be aware, even with strong efforts at protecting a whistleblower's identity, they are still at risk while an employer searches for the internal source. Work with the whistleblower so they are not releasing possibly traceable information. Specific information only the whistleblower had access to or could have known can be as much of a signature as their name.

If your source asks for anonymity, understand what that means for you. At minimum, it means choosing to make a human interest aspect of the story not about the whistleblower but about the risk or damage done to others by the wrongdoing your whistleblower exposes.

More significantly though, it means recognizing the legal limitations on your ability to maintain the confidentiality of your source. In many states, journalists are protected by **shield laws** or courts recognize a **reporter's privilege** to keep their sources and notes confidential when asked to reveal sources under demand of a subpoena. But there is no protection at the federal level, and like whistleblower laws, these are also a patchwork of protections that may differ state to state. If you are not protected by these laws and a judge orders you to name your source, you could end up in jail for contempt of court if you refuse.

Shield laws also may not protect you in a defamation lawsuit. Wealthy individuals and corporations may consider a SLAPP lawsuit (Strategic Lawsuit Against Public

Participation) to shut down reporting or attempt to force you to reveal your sources. Consult with a lawyer before you take on the story and work out details of any anonymity arrangement with your source at the beginning of the reporting project to make sure your responsibilities are clear. GAP is able to act as a broker of information in certain cases, which can help protect both the journalist and the source.

Some news organizations now require reporters to disclose their confidential sources to editors. One large organization mandates those disclosures be made via email, which creates a discoverable document should the confidentiality issue land in court. Be aware of your organization's policies before entering into such agreements. In some cases, the risk to whistleblower and/or journalist just might be too high.

Other Paths to Get the Information

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 access to information that could show wrongdoing by the government, tutoring you for the right Freedom of Information Act requests can gain access to those materials. If the agency denies their existence, the whistleblower can work discreetly with the FOIA officer to point out the disinformation and make the illegal cover-up backfire.

Even with this FOIA method, be careful. If you are too precise with your requests, you could tip off an agency that they've got a whistleblower and even who the whistleblower is.

Whistleblower sources can use an intermediary, such as an organization like GAP or POGO, which can either serve as a buffer between the source, the information, and a journalist, or as a middleman, providing the whistleblower's information to

a friendly Congressional[9] or agency staff member. Careful staff investigators can then work directly with the journalist, or can conduct investigations and issue subpoenas seeking a broad swath of documents related to the disclosure without revealing the source who prompted the inquiry.

Secure Communications & Information Security[10]

If an employee has come to you with information about serious wrongdoing, whether the information relates to human rights abuses, environmental threats or national security risks, journalists 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. Below are some best practices that can help protect communications with whistleblowers.

➔ Sources should avoid contacting journalists using government email accounts, computers, or telephones.

Whistleblowers 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 (like Tails) and an anonymous web browser (like 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, including Signal for calls, WhatsApp for texts, encrypted email such as ProtonMail or Peerio, and SecureDrop to receive documents.

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

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

➔ 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 1) consider whether there are cameras that could record the meeting, 2) leave their cell phones behind to avoid detection through location services on all smartphones, 3) if possible meet a source outside the building to avoid security cameras or building visitor logs, and 4) specify a meeting location where the source or the journalist 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.

➔ Be careful about how you ask for documents. It is 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." For unclassified documents, it's also better to phrase a request as "How could I obtain documents to back up what you're saying?," rather than directly asking for them to provide documents.

➔ Handle electronic documents with care. Be careful about transmitting documents electronically, especially if it is going through a third-party. Anything that is sent via email (i.e. Gmail), stored on Google Drive, or added to an internal calendar, could be subject to a subpoena issued to the third party service which 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 journalist'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 provides end-to-end encryption yet is

more user-friendly because it works like instant or text messaging. When using Signal for sensitive conversations you should verify your safety numbers, which you can learn how to do here[11]. 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. Move the Signal app to be next to your other text messaging apps to encourage more frequent use.

➔ Use Secure Drop for the most sensitive communications and documents Journalists that actively communicate with whistleblower sources should consider employing SecureDrop to receive documents, a secure platform developed primarily to protect source communications with journalists. The information remains encrypted until it is transferred to an air-gapped computer that never connects to the Internet. SecureDrop is relatively pricey, requiring separate servers for hosting, and also somewhat complicated to use for even the most advanced whistleblowers, requiring a codename to access messages. Users must use the Tor Browser anonymous web browser to access SecureDrop safely. When a source uses SecureDrop, neither the receiving party nor any third parties will record their IP address or information about their browser, computer or operating system. SecureDrop is managed by the Freedom of the Press Foundation[12] which helps organizations with installation and training.

➔ 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 never to store sensitive documents on personal laptops. Sensitive documents should not be left on desks unless in use.

11 See https://support.signal.org/hc/en-us/articles/213134107-How-do-I-verify-the-person-I-m-chatting-with-is-who-they-say-they-are-

12 See https://securedrop.org

➔ 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 recreating your own version.

➔ Remove metadata from documents, PDFs or photos posted online. Make sure to remove the metadata, like 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 just 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 government source or contractor, while confirming your story. As mentioned earlier, many agencies have implemented "insider threat" programs to deter and detect perceived threats to national security, including releases of classified information. 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 over loyalty to their employer.

➔ Protect your communication with your coworkers about your source. At times, the government has obtained warrants to spy on reporters in an attempt to find their sources.

➔ **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** with sensitive information on your phone and computer, including names and contacts.[13]

Conclusion

Journalists and whistleblowers working together are essential to maintaining a robust democracy and holding institutions accountable through an informed citizenry. Supporting whistleblowers through best practices that recognize the professional risk involved with reporting wrongdoing will ultimately serve the best interests of both the employees and journalists in their shared goals of advancing the public's interests.

13 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). https://www.aclu.org/blog/free-future/can-border-agents-search-your-electronic-devices-its-complicated

Resources

Contact GAP

The Government Accountability Project (GAP) is happy to offer advice and support to journalists and their whistleblower sources.

by email

info@whistleblower.org

by phone

202.457.0034

Other Organizations

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.

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 some legal support to national security whistleblowers as well through their Whistleblower and Source Protection Program (WHISPeR).

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)
https://www.whistleblower.org/corporate-whistleblowers-survival-guide

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)
https://www.amazon.com/dp/1493028812/ref=cm_sw_r_cp_dp_T1_AYJBzb3EB0ZPE

McCutcheon, Chuck, "***Whistleblowers***," CQ Researcher, 24.5 (Jan. 31, 2014)
http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2014013100

Meyer, Dan and David Berenbaum, "***The Wasp's Nest: Intelligence Community Whistleblowing & Source Protection,***" 8 J. Nat'l Security L. & Pol'y 33 (2015)
http://jnslp.com/wp-content/uploads/2015/05/The-Wasp%E2%80%99s-Nest.pdf

POGO, GAP & PEER, ***The Art of Anonymous Activism: Serving the Public While Surviving Public Service*** (2002) (updated version forthcoming)
https://www.peer.org/assets/docs/The Art of Anonymous Activism.pdf

Shield Law Information

Reporters Committee for Freedom of the Press, **The Reporter's Privilege Compendium: An Introduction**
https://www.rcfp.org/browse-media-law-resources/guides/reporters-privilege/introduction

Reporters Committee for Freedom of the Press, **Shield laws and protection of sources by state**
https://www.rcfp.org/browse-media-law-resources/guides/reporters-privilege/shield-laws

Society of Professional Journalists, **Shield Law 101: Frequently Asked Questions**
https://www.spj.org/shieldlaw-faq.asp

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-

www.whistleblower.org

202.457.0034