

Speaking up from within the government

A practical guide to navigating speaking to reporters or the public while protecting yourself and respecting the law.

Whistleblowing: What and Why

A common **misconception** is that disclosing information is only legally protected when a public employee tells a specific entity—like Congress or a watchdog agency—about wrongdoing. Not so. With some exceptions, federal law protects federal employees who disclose—**including to the public or press**—information they reasonably believe is:

- A violation of any law, rule, or regulation
- An abuse of authority
- A gross waste of funds
- A substantial and specific danger to public health or safety
- Gross mismanagement

Some of the most important things the public has ever learned about its own government came to light only because a public servant decided to come forward. A few examples of what would have stayed secret:

- **A decades-long government experiment on Black men** — Public Health Service investigator Peter Buxtun repeatedly warned his agency that it was withholding syphilis treatment from patients without their consent. Ignored internally, he went to the press. The Tuskegee study ended, and federal research ethics were transformed.
- **A TSA plan to pull air marshals off long flights to save on hotel costs** — Air marshal Robert MacLean contacted a reporter after being rebuffed internally. The TSA reversed course, and the Supreme Court held that MacLean was protected by whistleblower law.
- **Warrantless mass surveillance of American communications** — AT&T technician Mark Klein revealed information, including to the press, showing the company was cooperating with the NSA to intercept and monitor Americans' internet traffic and other communications data.
- **Falsified air quality data after September 11** — EPA chemist Cate Jenkins disclosed testing indicating the Ground Zero air was likely toxic, even as the agency called the air safe. Thousands of first responders have received compensation for injuries.

The Rules: Respecting Legal Barriers to Disclosure

Federal law protects your job in many circumstances when making a protected disclosure. However, depending on what information you want to share, speaking up may create risks—including criminal prosecution, civil liability, and job-related consequences.

Before you disclose, ask yourself:

- **Is this information classified or related to national defense?**
 - Federal law makes it a crime to knowingly disclose classified and certain other unclassified national security-related information to an unauthorized recipient—including a reporter.
- **Does a specific statute (law) prohibit me from disclosing this information?**
 - Some laws, like the Privacy Act, have serious penalties for disclosing certain information. Some agencies have specific laws protecting specific information.
- **Is this information covered by a legal privilege?**
 - Information can be protected by attorney-client privilege, grand jury secrecy rules, the rules of professional conduct (for attorneys), or other privileges.
- **Does sharing this information violate your agency's policies or procedures for speaking externally?**
 - Many agencies have policies that mandate certain procedures before speaking to the press in certain contexts, which have been enforced aggressively lately.
 - You have a right to blow the whistle, but your agency still may try to retaliate with a disciplinary action, and that can be onerous even if you ultimately prevail.

If the answer to any of these is “yes,” or you are uncertain, there may be serious consequences to speaking up. Consult an attorney before acting.

The Whistleblower Protection Act: what it does and doesn't cover

The Whistleblower Protection Act (WPA), 5 U.S.C. § 2302, protects many¹ federal employees from **employment-related** retaliation for disclosures—including to the press—if the employee reasonably believes the information reveals a violation of law, gross mismanagement, gross waste, abuse of authority, or a substantial danger to public health or safety.

¹ In the Whistleblower Protection Act, a number of agencies in the intelligence community are explicitly excluded from the law's protections. That means that if you work at the FBI, CIA, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, National Reconnaissance Office, or an agency determined by the president to be conducting foreign intelligence or counterintelligence activities, you are likely not protected by the WPA. A complex patchwork of laws and executive orders governs employees in these agencies; consulting with an attorney before speaking out is very strongly encouraged.

What the WPA does

- ✓ Protects you from adverse personnel actions for covered disclosures
- ✓ Applies to disclosures to the press, Congress, and designated agencies
- ✓ Covers most federal employees

What the WPA does NOT do

- ✗ Authorize the disclosure of classified information or other info protected by law
- ✗ Shield you from criminal prosecution (e.g., under the Espionage Act)
- ✗ Cover employees of certain intelligence community agencies

The bottom line: **the WPA may protect your job, but it does not protect you from all legal consequences.**

Before you speak up: assessing goals and risks

You're a government employee who wants to speak publicly about something that you're seeing at work. Before you give a speech at your local town council meeting or call a reporter, assess what level of risk you're comfortable with, as that can guide how you speak up.

What level of risk?

There are ways to mitigate each of these risks, but before thinking about mitigation strategies, decide what consequences you can tolerate (and prepare for them).

- **Discipline on the job:** Some public employees who've spoken publicly about issues related to their work have been placed on administrative leave and investigated by their agency.
- **Job loss:** The risk of being fired for speaking out publicly is likely higher now than ever.
- **Doxxing and other risks of speaking publicly:** Unfortunately, some people who've spoken out against what they see as abuses of power have become targets of online harassment, doxxing, or other threats.
- **Criminal liability:** Laws against disclosing certain information—for example, classified information—could expose you to serious charges.

What level of anonymity?

One way to account for your own risk tolerance is to decide on what level of anonymity you want. You have options:

- **Fully anonymous:** You want to make sure nothing you say is associated with you in any way.
- **Not anonymous:** You believe attaching your name to your disclosure is important and are ready to accept the risks.
- **Not publicly named:** You understand that people within your office may learn you spoke up, but you want to keep your name out of the press—and off the Internet.

Speaking with the press

You know your goals, your risk tolerance, and your preferred level of anonymity. Now what?

Identifying a reporter & reaching out

Finding the right reporter matters as much as deciding to speak up in the first place. A few things to consider:

- ✓ **Choose someone who covers the issue.** Reporters who specialize in your agency or policy area will understand the significance of what you're telling them, ask better follow-up questions, and be better positioned to verify and report the information accurately. A story told to the wrong reporter may never run, or may be reported less accurately.
- ✓ **Look for reporters at outlets with strong legal support.** Many news outlets have lawyers who review stories before publication and can push back if the government threatens legal action. Generally speaking, larger outlets may be more likely to have these resources, but that is not universally true—so ask reporters before you disclose information.
- ✓ **Make contact on your own time.** Avoid making a disclosure when you are on the clock or physically at work. Do not use government time, resources, or devices—both for security reasons, and to avoid violating policies that govern use of government property and time.
- ✓ **Make contact safely.** If anonymity matters to you, do not reach out from an account that can be traced back to you. Many reporters who handle sensitive disclosures accept tips through encrypted messaging apps (e.g., Signal) or secure submission systems (e.g., SecureDrop). Check the reporter's or outlet's website for instructions.

The lingo: how to communicate with a reporter

Before you share anything substantive, you and the reporter should agree on the **ground rules** for how your conversation will be used. These terms are commonly used in journalism, but their precise meanings can vary—so it is worth **defining them explicitly at the start of every conversation**, even if you've spoken with the reporter before.

- ✓ **On the record:** Everything you say can be quoted and attributed to you by name. This carries the most risk but also the most credibility.
- ✓ **On deep background:** The information can inform the reporter's understanding and reporting, but it cannot be quoted or attributed in any form—not even a general descriptor. This can be a protective option, but it also limits how directly the reporter can use what you tell them.
- ✓ **On background:** The information can be reported and used in the story, but it will not be attributed to you by name. The reporter may describe you by a general
- ✓ **Off the record:** The information is shared

descriptor—for example, "a senior official" or "a person familiar with the matter." Confirm with the reporter exactly how they plan to describe you before agreeing to speak on background, because descriptors can sometimes narrow down the universe of possible sources.

solely to help the reporter understand a situation or point them in a productive direction. It cannot be used in the story at all. Note that "off the record" is not a guarantee of confidentiality if the reporter learns the same information from another source; in that case, they may be able to report it without reference to you.

One practical note: these ground rules must be established *before* you share information, not after. A reporter is not obligated to honor a retroactive request to go "off the record" about something you've already said. Avoid switching between these agreements to avoid confusion about what was or was not quotable in the span of a single conversation.

Behind the curtain: some practical tips about how reporting works

Understanding how the reporting process works—not just the conversation you have with a reporter, but everything that happens after—can help you prepare and protect yourself.

- ! **The reporter will likely seek corroboration.** Reporters generally cannot publish a story based solely on a single source. They will usually try to verify what you've told them by speaking with colleagues, reviewing documents, or consulting other sources. That means your coworkers may be contacted, and those conversations could indirectly reveal that someone inside your office spoke to the press—even if your name never appears. When setting ground rules, you can ask the reporter how your name, and information you provide, will be communicated to other sources.
- ! **The reporter will likely seek comment from your agency.** Before a story runs, it is standard journalistic practice to contact the relevant agency or official for comment or response. This will typically put the subject of the story on notice that a reporter is working on it—and potentially on notice that there is a source inside the agency. Plan for this, and discuss with the reporter in advance how and when they plan to reach out so there are no surprises.
- 🕒 **Consider the timing.** Once a story is in motion, events can move quickly. An agency may learn a story is coming and take preemptive action—including personnel actions against potential sources—before publication. Discuss with the reporter whether there is any flexibility in timing and what protections are in place.
- **You can set limits.** You do not have to answer every question a reporter asks. You can decline to address certain topics, correct misunderstandings without providing additional information, or end the conversation at any time. You can also ask for a correction if the published story gets something wrong. You are not obligated to share more than you intend, even if the reporter pushes. With the reporter's consent, you can also start the conversation "off the record" and then take certain points "on the record" later.

Before you begin, consider asking the reporter the following questions:

- How will you store documents or materials I share with you?
- Will you contact my agency for comment, and how will you describe your source in doing so?
- Are you working with any other sources on this story?
- Will you use my name, or information you learn from me, in conversation with other sources?
- What is your outlet's policy if the government seeks to identify your source through legal process?
- At what point will you notify me before the story is published?

Resources

If you are considering speaking up publicly about what you're witnessing at your federal job, you may wish to seek legal advice or other forms of support. In addition to speaking with a private attorney, the following organizations have expertise in whistleblowing:

- [Government Accountability Project](#) provides education and, in some cases, legal support
- [Whistleblower Aid](#) provides representation and support
- [Whistleblowers of America](#) supports whistleblowers who've been retaliated against
- [Project on Government Oversight \(POGO\)](#) provides resources and education
- [Justice Connection](#) provides DOJ employees with media support and connects them with attorneys

ABOUT US

Protect Democracy is a nonpartisan, nonprofit group working to prevent American democracy from declining into a more authoritarian form of government.