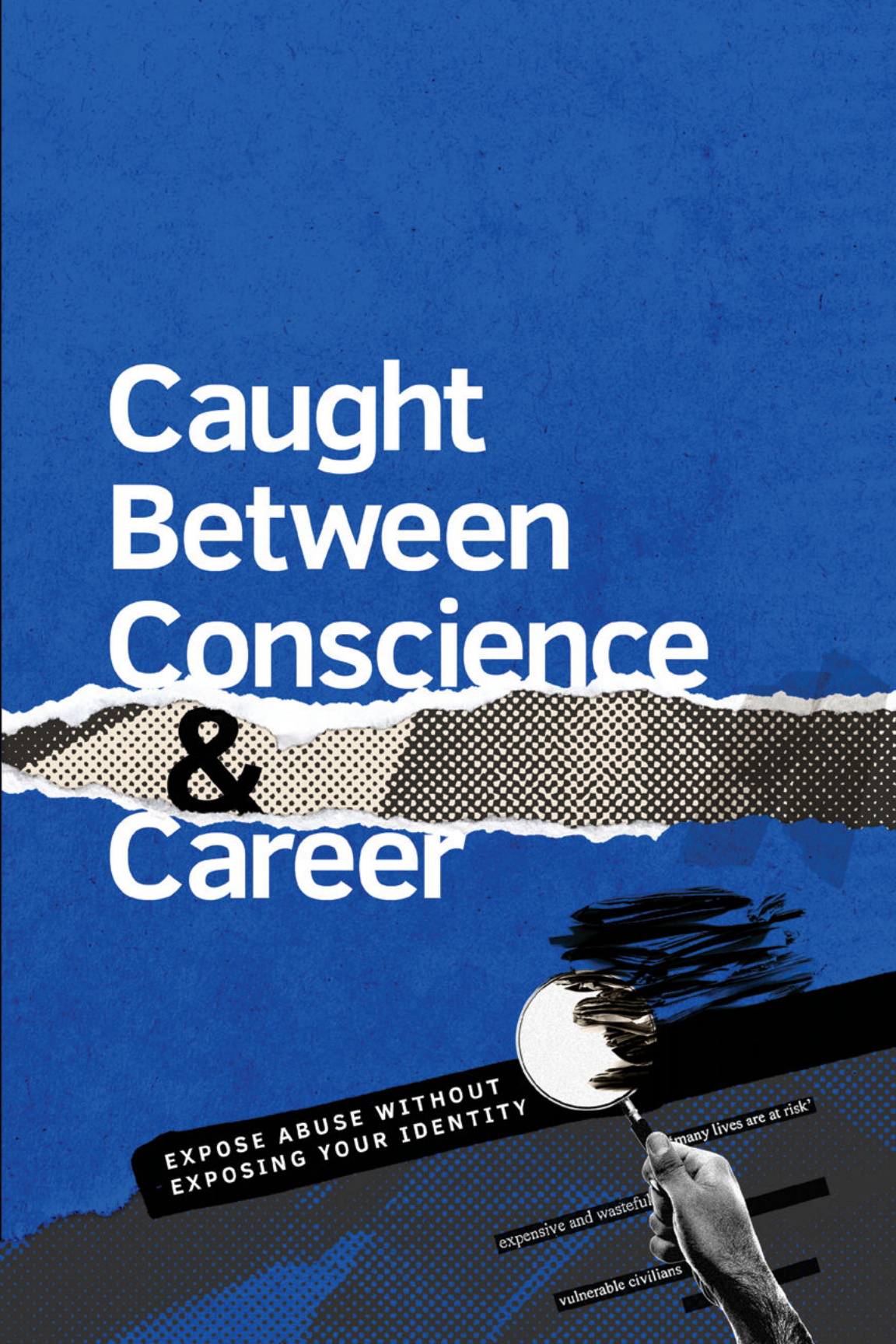
Caught Between Conscience & Career



Acknowledgements

A collaboration of the Project On Government Oversight, Government Accountability Project, and Public Employees for Environmental Responsibility, this survival guide updates the language and lessons from the 2001 book, *The Art of Anonymous Activism: Serving the Public While Surviving Public Service*.

This new edition was made possible thanks to the work of:

EDITOR
Nick Schwellenbach

CONTRIBUTING AUTHORS
Tom Devine
Rebecca Jones
Andrea Peterson
Mandy Smithberger
Timothy Whitehouse

ADVISORS
Kevin Bell
Danielle Brian
Paula Dinerstein
Samantha Feinstein
Dana Gold
Doug Hartnett
Liz Hempowicz
Irvin McCullough
Nicholas Pacifico
Jeff Ruch

COPY-EDITING AND FACT-CHECKING
Danni Downing
Neil Gordon
David Janovsky
Mia Steinle

ASSISTANCE AND RESEARCH
Lane Corrigan
Daniel Van Schooten

DESIGN AND ILLUSTRATION
Rachel Freedman
Leslie Garvey

MARKETING AND OUTREACH
Jordan Bollmann
Abby Evans
Timothy Farnsworth
Andrew Harman
CJ Ostrosky
Pam Rutter

Special thanks to Tom Devine, Jeff Ruch, and the late Beth Daley, who were the main authors of the first edition of this book, and to Frank Serpico, who authored its foreword. And thanks to Andrew Bakaj, David Bralow, Kel McClanahan, Kathleen McClellan, Dan Meyer, Fabio Pietrosanti, Jesselyn Radack, Trevor Timm, Mark Zaid, and Jason Zuckerman for sharing your expertise and experience.

This project was made possible thanks to funding support from Bauman Foundation, CS Fund, Democracy Fund, The Frankel Foundation, Fund for Constitutional Government, Stewart R. Mott Foundation, and Val Schaffner.

Caught Between Conscience & Career

EXPOSE ABUSE WITHOUT EXPOSING YOUR IDENTITY

POGO
PROJECT ON GOVERNMENT OVERSIGHT

GOVERNMENT ACCOUNTABILITY PROJECT

PEER

Contents


(5,678,692)
(-416,880)
many lives are at risk'
expensive and wasteful
vulnerable civilians
800,554
50,000
(50,000)
"The way to right wrongs is to turn the light of truth upon them."
IDA B. WELLS-BARNETT
INVESTIGATIVE JOURNALIST

Introduction

LEGAL DISCLAIMER

The material in this guide is provided for informational purposes only. Nothing in this publication should be construed as legal advice. **Before you act on any of the material in this guide, the authors STRONGLY urge you to seek legal counsel.**

At government agencies, financial institutions, government contractors, and other powerful organizations, once-lonely voices speaking out against wrongdoing are increasingly being joined by others, and together they are beginning to raise a crescendo that can no longer be ignored or silenced. Institutions that break the law, commit fraud, or harm public health, safety, or security have good reason to fear whistleblowing by conscientious employees. Whistleblowers who "commit the truth"[1] can prompt significant reforms, hold institutions accountable, and shine a light on agency abuses and illegal practices by sparking Congressional hearings, newspaper stories, and prominent television coverage.

Many things have changed since the days of the brown envelope slipped

under the door by an anonymous source. Now, the internet and the proliferation of online platforms have expanded the means by which whistleblowers can disclose information and the number of people that information can reach, increasing the potential to make a difference.

Yet many things have stayed the same, particularly the risk that whistleblowers will face retaliation. Further, while the information revolution has expanded whistleblowers' potential audience, technological advances have also made it harder than ever before to dissent anonymously. In this edition of our book, we've considered these new vulnerabilities and other technological developments.

For the purposes of this book, we define "whistleblowers" as individuals who work inside organizations, either in the government or private sector, and who disclose and challenge abuses of power or other failings by their organization that betray the public trust. The whistleblowers can raise concerns purely internally or through disclosures to law enforcement, Congress, other official channels, or the public.

Some people use the term "whistleblower" colloquially to refer to journalists, activists, or others who raise concerns about an organization from the outside. While these individuals often are vital to exposing misconduct, and also sometimes face retaliation from those who are threatened or angered, they are a subset within the universe of "whistleblowers," and not whom we spotlight in this book.

Moreover, the lessons we present in this book are primarily for whistleblowers working in the federal government, specifically the executive branch. However, the same lessons can be valuable for local and state government whistleblowers, private-sector whistleblowers, and anyone else who wants to bring wrongdoing to light while protecting themselves.

We do not define "whistleblowers" solely as the federal government employees who have legal rights against employer retaliation. Indeed, missing, limited, or ineffective legal protections are major themes in this book. Whistleblower-protection laws have significant loopholes.[2] Further, agencies responsible for turning paper rights into reality do not always have the staffing, resources, or even desire to vigorously enforce the laws, or get it right when they do.[3]

Unfortunately, the public can see whistleblowing through a partisan, ideological, or agenda-driven lens, rather than through one focused on the disclosure's truth or benefit to society.[4] The latter should be what the public

and the government care about. Even if a whistleblower is wrong about the specifics, their disclosures may still warn of valid threats, or an investigation into their concerns may still expose related misconduct.

Deciding to blow the whistle—disclosing information about breaches of public trust through internal channels, publicly, or as an anonymous source—is a professional crossroad after which the employee's career will never be the same. Laudatory press coverage and movie portrayals can sometimes cast whistleblowing in a glamorous light.

Individuals like analyst Daniel Ellsberg, who leaked the Pentagon Papers; FBI agent Coleen Rowley, who blew the whistle on the FBI's failures leading up to 9/11; Enron executive Sherron Watkins, who brought to light the company's rampant fraud; and scientist Jeffrey Wigand, who exposed dangerous lies by the tobacco industry, are viewed by many as truth-tellers who were successful.[5] But beyond the limelight, these public figures and others who choose to follow their conscience often experience a darker reality.

Retaliation against whistleblowers is widespread and poses a significant barrier to the accountability and transparency of government and corporate conduct. According to government surveys of federal workers in 2010, "approximately one-third of the individuals who felt they had been identified as a source of a report of wrongdoing also perceived either threats or acts of reprisal, or both."[6] An updated 2017 employee survey found that, despite passage of the landmark Whistleblower Protection Enhancement Act of 2012, about 30 percent of government employees say they fear retaliation if they report wrongdoing.[7]

Retaliation against private-sector whistleblowers is also troubling. Despite the enactment of new whistleblower rights following the financial meltdown caused by the home-mortgage crisis of 2007, instances of reprisal against employees for reporting wrongdoing have *doubled* from 22 to 44 percent since 2013, with 72 percent of employees who were retaliated against saying it happened within three weeks of making a disclosure.[8] Research shows that the legitimate fears of reprisal and futility—that speaking up will not change anything—continue to be the dominant reasons employees in all sectors stay silent despite witnessing wrongdoing in organizations.[9]

Federal whistleblower law prohibits managers from taking personnel actions against employees who make any lawful disclosure of information they reasonably believe is evidence of "any violation of any law, rule, or

regulation; or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health and safety."[10] But skepticism and fears of reprisal are justified, because although these protections exist on paper, only a small fraction of employees who filed retaliation claims prevail through the legal process.[11]

Fortunately, legal rights for whistleblowers are steadily getting stronger, and the chances of winning protection have improved. After a thirteen-year campaign by the Make It Safe Coalition, of which our organizations are members,[12] Congress unanimously passed the Whistleblower Protection Enhancement Act of 2012. That legislative makeover of whistleblower rights reversed more than a decade of hostile court rulings, restored access to an appeals process, outlawed agency gag orders, and offered reinforced protection against scientific censorship.[13]

Confusion about whistleblower rights—by employees and managers alike—is widespread.

Similarly, since the 1990s, Congress has passed numerous whistleblower laws providing much of the private sector—including government contractors—with rights enforced through jury trials.[14] Congress's votes to approve the Whistleblower Protection Enhancement Act and the expansions of corporate whistleblower rights represent an impressive legislative mandate for employee speech rights. This edition of our book keeps pace with new legal developments, and the chapter on the law has been expanded to discuss legal protections for federal contractor, FBI, intelligence community, and military whistleblowers.

Unfortunately, confusion about and lack of awareness of whistleblower rights by employees and managers alike are widespread.[15] And disclosures by employees may anger bosses who face scrutiny as a result.

In sum, whistleblowing continues to be dangerous, and the risk of retaliation remains.

For instance, during the Obama Administration, whistleblower retaliation at the Department of Veterans Affairs made national headlines when the Office of Special Counsel reported a massive surge in whistleblower-retaliation complaints, some from employees who disclosed secret waiting lists that revealed the difficulty many veterans faced in accessing health care at Veterans Affairs medical centers.[16]

In another instance, several agents from the Bureau of Alcohol, Tobacco,

Firearms and Explosives asserted that the Bureau retaliated against them for disclosing that a U.S. government operation allowed the sale of thousands of guns that made their way to drug cartels in Mexico.[17] The Bureau settled three of the whistleblowers' retaliation cases.[18] In the Department of Defense, Army Special Forces Lieutenant Colonel Jason Amerine had his security clearance suspended after he disclosed to Congress how dysfunctional the government's hostage negotiation and recovery process was.[19] And after Army intelligence analyst Chelsea Manning leaked massive amounts of military and State Department information to WikiLeaks, President Obama commented that Manning "broke the law" before Manning even went to trial before a military judge. Media commentators noted that President Obama may have used "unlawful command influence" because, as the commander-in-chief, he was the judge's ultimate boss.[20] These are just a handful of examples.

The Trump Administration has also sent chilling signals to whistleblowers. In response to a press question about State Department officials who used the agency's dissent channel to register concerns with the first version of President Trump's travel ban, then-White House press secretary Sean Spicer said, "they should either get with the program or they can go."[21] After an anonymous author who claimed to be a senior Administration official wrote a *New York Times* op-ed critical of the White House, the President called for investigation to find the author.[22]

The retaliation even applies to high-level officials who have left government: President Trump yanked the security clearance of former CIA Director John Brennan specifically for criticizing him, and threatened the clearances of other former intelligence leaders who dissent.[23] As with past White Houses, the Trump Administration has also seen numerous allegations of whistleblower retaliation against rank-and-file employees.[24] Although the numbers peaked with the surge of Veterans Affairs complaints at the end of the Obama Administration, the Office of Special Counsel continues to receive historically high levels of complaints about prohibited personnel practices from federal employees.[25]

Even though both Presidents strengthened legal protections for whistleblowers—and deserve credit for that—these statements and developments during both Administrations may make lower-level employees think twice about speaking up when they witness misconduct, and certainly about identifying themselves.

Most frightening, government employees who disclose information to the press are encountering criminal investigations and prosecutions, illustrated by record levels of prosecutions of government employees under the Espionage Act. President Obama's Justice Department used the law to prosecute more government officials who had made disclosures to the press than all past Administrations combined.[26] Under President Trump, the Justice Department ramped up leak investigations, tripling the number during the first year of the Administration, according to then-Attorney General Jeff Sessions.[27] A top Justice Department official stated in June 2018, "The Attorney General has stated that investigations and prosecutions of unauthorized disclosure of controlled information are a priority of the Department of Justice."[28] As of February 2019, four of the six prosecutions of employees for disclosing classified or otherwise sensitive information to the press during the Trump Administration involved "disclosures related to Trump, the circle of people around him, and the Trump-Russia inquiry," according to *The Intercept*.[29]

Another alarming fact is that due process and legal remedies available for many types of whistleblowers are woefully inadequate. For instance, unlike corporate and government contract workers, federal employees cannot seek justice against whistleblower retaliation through jury trials in courts.[30]

Perhaps the starkest choice government employees may confront is if they should overlook violations of law or obey a direct order to violate the law. The government employee is faced with an unpalatable choice of possible discipline for insubordination or potential liability for knowingly sanctioning violations of law. While federal civil service protections make it illegal to retaliate for refusing to violate a law, rule, or regulation,[31] the lack of credible due process means in practice that law-abiding public servants still proceed at their own risk.

This bleak reality means that those seeking to expose and resolve problems caused by corruption, political pressure, unaccountable bureaucracies, incompetence, or illegal actions within government agencies and by powerful corporations should do so in ways that are less risky for their careers, if possible.

Caught Between Conscience and Career is intended to help employees encountering these difficult ethical issues in their workplaces and to empower them to make the best choices. It is a survival guide for whistleblowers. It walks through the difficulties that may be encountered when blowing the whistle, the path of disclosing information without disclosing your identity, how to securely communicate electronically, the pros and cons

of different official government channels for disclosure, tips for working with the press, and a primer on legal protections.

The most important point is that it is possible to fight wrongdoing from within without sacrificing your career.

There is a desperate need for conscientious employees to serve as the public's eyes and ears about what is happening within powerful organizations. The vitality of the United States' democracy, the long-term viability of its economy, and public health, safety, and security depend upon truth-tellers to shine light on corruption and malfeasance.

There is a vibrant community of concerned citizen-activists who seek to aid those patriots who struggle to serve the public good.

Three organizations with many decades of experience supporting whistleblowers have contributed to this guide—the Government Accountability Project, Project On Government Oversight (POGO), and Public Employees for Environmental Responsibility (PEER). We can help you bring serious problems in the federal government and the private sector to light by providing assistance in exposing wrongdoing; assistance in conducting policy advocacy and media campaigns to remedy identified problems; and investigative research. The Government Accountability Project and PEER provide legal assistance and representation to whistleblowers as well. Collectively, we have helped countless conscientious employees do the right thing while still minimizing the risk to their careers.

If you blow the whistle, first learning the lessons of others who suffered can make all the difference in your own efforts. We hope this guide—reissued with new and revamped information for the 30th anniversary of the Whistleblower Protection Act—will be an effective course in how to "commit the truth," a phrase coined by the late, legendary Pentagon whistleblower Ernie Fitzgerald.[32]

TOM DEVINE
Legal Director, Government Accountability Project

DANIELLE BRIAN
Executive Director, Project On Government Oversight

TIMOTHY WHITEHOUSE
Executive Director, Public Employees for Environmental Responsibility

"If you're going to sin, sin against God, not the bureaucracy. God will forgive you but the bureaucracy won't."

ATTRIBUTED TO
ADMIRAL HYMAN G. RICKOVER

CHAPTER 1

Blowing the Whistle May be Hazardous to Your Professional Health

In the spring of 2014, whistleblowers at the Department of Veterans Affairs (VA) came forward and told the press horrific stories of how veterans were not receiving the medical care they needed. This sparked a deluge of disclosures by others across the VA that led to front-page stories, cable news investigative exposés, and Congressional hearings. Veterans Affairs Secretary Eric Shinseki and others resigned in the immediate wake of the scandal.[1]

But many of the whistleblowers who raised concerns also faced retaliation from the federal government. The Government Accountability Office issued a report in the summer of 2018 that found VA whistleblowers were "10 times more likely [than VA employees who don't blow the whistle]…to receive disciplinary action within a year of reporting misconduct."[2]

Too often, the more successful whistleblowers are at making a difference, the more threatening they become to those whose actions cannot withstand

scrutiny. Their successes can motivate retaliation if they are identified. And for those who think that blowing the whistle publicly is glamorous or a path to recognition, think again. Many whistleblowers suffer in obscurity, frustrated by burned career bridges, blackballed in their line of work, and never achieving the validation they sought. For every success story, there are an untold number of stories of professional martyrdom. The prominent, lionized exceptions stand as beacons of false hope for thousands.

Few paths are more professionally treacherous than challenging abuses by your own employer.

Whistleblowing is always dangerous, but embarking on that path without preparation and thoughtful consideration of the consequences can be a recipe for disaster.

For those contemplating (or maybe unable to avoid) being identified as a whistleblower, we sketch out some considerations and potential negative consequences in the following pages. Sometimes whistleblowers avoid worst-case scenarios, but you shouldn't expect to do the same: it is better to be prepared and be pleasantly surprised.

Downsides Are Apparent

It takes individuals to deliver the truth about wrongdoing and sometimes the only individuals in a position to do so work within the very organizations committing wrongdoing. But few paths are more professionally treacherous than challenging abuses by your own employer. If you are thinking of publicly opposing an action by your agency or openly reporting wrongdoing in the workplace, here are some considerations to think about before acting.

1 IT IS NOT A FAIR FIGHT

One person against a government agency is inherently a David-versus-Goliath struggle. The organization holds most of the cards. People who speak out loudly and publicly against their organization can face repercussions in their jobs. Not all of these repercussions are immediately obvious. Some whistleblowers are given lateral transfers to isolated or unpopular offices.[3] Some organizations relentlessly create a hostile workplace where they are socially ostracized.[4] Some are scrutinized by

management that seems to be looking for problems.[5] Still other whistleblowers find that they are passed over for promotions.[6]

The tactics for harassing whistleblowers are manifold. For example, an organization can:

- **Set an employee up for failure.** Usually, this means giving the employee impossible assignments and then firing or demoting them for non-performance.[7]

- **Blacklist the employee so that they cannot find gainful employment in their chosen field.** That employee then serves as an example to scare off others from the same fate.[8]

- **Conduct a retaliatory investigation[9] and charge the employee with an offense as minor as stealing pens.[10]** Smears of alleged misconduct similar to what the whistleblower is challenging are common, potentially to undermine the whistleblower's credibility and make them look like a hypocrite. Significantly, federal whistleblower law does not allow employees to challenge retaliatory investigations until there is a subsequent personnel action.[11] Whistleblower protections only create protections from adverse employment-related actions, such as terminations and demotions, and do not shield against criminal prosecutions. That means they have no anti-retaliation rights against this not-uncommon tactic. The criminal charges whistleblowers have faced have ranged from theft or misappropriation of government property to violations of the Espionage Act.[12]

- **Discredit or humiliate the whistleblower by questioning their mental health, professional competence, reliability, or honesty.** One tactic is to order the employee to undergo a psychiatric examination. Often the agency can hide behind privacy laws to hint that there is a problem with the employee that the agency is not at liberty to disclose.[13]

2 IT OFTEN MISSES THE POINT

When agency employees go public with tales of malfeasance or other information of public concern, the media spotlight may focus on the

personality at the expense of the issue. Whistleblowers may find that they become the story.

There are a number of problems with this.

Government agencies often find it easier to distract from their misconduct by attacking the messenger than addressing the message. Rather than face the problems brought to light, managers may simply try to focus attention on the "disgruntled" employee."[14] The conscientious worker is then portrayed as vengeful, dishonest, and self-serving. Women can face misogynistic accusations and racial minorities can face racist allegations.[15]

This allows the agency to turn the tables and put the employee, or their motives, on trial: Is the whistleblower a good employee? Does the whistleblower have a hidden agenda like revenge or ambition? In many instances, the whistleblower's work record is irrelevant to the issue at hand, but it can occupy center stage in terms of public attention.

In instances where the employee is fighting to obtain a remedy for retaliation, the case turns on questions of employment law (see Chapter 6) such as: Was the termination lawful? Is there a legitimate reason for the transfer? Did the agency abuse its discretion? The concern the employee raised becomes a subsidiary issue in a reprisal case. This means whistleblowers must fight on two fronts—to defend themselves, and to convince government authorities to address the problems they raised.

3 IT OFTEN TAKES THE BEST AND BRIGHTEST OUT OF THE ORGANIZATION

Good professionals are often casualties of whistleblower conflicts. Even vindicated whistleblowers leave agencies as a matter of survival, or are too disheartened to continue in their chosen career.[16] Usually, it is not realistic for an employee to work for a boss they just battled. In those instances when a whistleblower can obtain a transfer for a fresh start in the organization or industry, the whistleblower's reputation will likely follow. At a minimum, agency managers will likely shy away from giving whistleblowers sensitive or potentially controversial assignments—in other words, the most significant work where integrity counts the most.

If a whistleblower files a legal complaint and if it results in a positive outcome, agencies often pay them to leave as the case's final resolution. But conscientious employees who take career risks to address

problems are precisely the people who best serve the public, and are the employees we need to keep in government agencies.

The human dimension to these risks should not be overlooked. Being a whistleblower is stressful.[17] Whistleblowers have reported impacts on personal relationships, ranging from friendships to marriages.[18] Less obvious but no less real is the strain from "mind-game" retaliation. As employees are transferred to less-interesting projects or have their responsibilities removed, boredom and frustration can set in. Supervisors may overly nitpick at an employee's work product. Once-friendly colleagues may suddenly ostracize a whistleblower as word gets around that they are on management's bad side.

CHECK YOUR PARACHUTES BEFORE YOU LEAP
Tips for Whistleblowers

Notwithstanding the above, you may choose to blow the whistle. As we explain in later chapters, often employees do not even think they are engaging in dissent, believing they are just doing their jobs. But then they wake up one day to find that they somehow made the transition from valued worker to Public Enemy Number One. In other instances, the employee is in a situation where they have nothing to lose by fighting.

When that moment of realization or decision arrives, pause for a moment to review the following survival tips that apply to whistleblowers who choose not to act anonymously.

1 CONSULT YOUR LOVED ONES

Blowing the whistle can impact your entire family. Before taking any irreversible steps, talk to your spouse, significant other, family, or close friends—the support group you will need in the coming days, months, or years—about your decision to blow the whistle. If they are not with you, you may want to rethink this path.[19]

2 CHECK FOR SKELETONS IN YOUR CLOSET

Any personal vulnerability or peccadillo can be used against you by your agency. If there is something in your past you do not want to see on the front page of the newspaper or shared with the world on social

media, reconsider blowing the whistle. One practical step is to make a copy of the complete contents of your personnel file as insurance that your employer cannot later slip new but backdated "dirt" into it.

3 DOCUMENT, DOCUMENT, DOCUMENT, BUT BE CAREFUL

Keep copious records and a daily diary of relevant information to memorialize conversations and developments. Forward or print relevant work emails and maintain copies of records in case you are cut off from evidence in your workplace that can assist you in proving your allegations. Your chances of success will likely depend on how powerful a paper trail you produce.

Be warned, however. Proving your charges with institutional records can be extremely dangerous. It can mean criminal prosecutions for unlawfully copying or removing government records. There have even been cases where federal employees have been threatened with prosecution for sharing non-classified information.[20] See Chapter 2 to learn more about the risks of disclosing classified information. Corporations aggressively file multi-million dollar "SLAPP suits"[21] or seek criminal prosecution against employees for allegedly stealing company property, even if it is evidence of the organization's criminal misconduct.

Depending on the potential legal liabilities involved, whistleblowers should store their copies of evidence in a secure, independent location away from their homes, preferably through an attorney where confidentiality is generally protected by attorney-client privilege.

If there is any doubt, a safer tactic may be hiding copies of paper records on the organization's premises in a location that will not draw attention, such as archives or some other innocuous location. Copies of electronic records can be stored under misleading folder names or in locations that are unlikely to be discovered (see Chapters 2 and 3 for more discussion of the risks of moving agency records). That way the whistleblower can be a navigator for law enforcement authorities, instructing them on what records to seek, and then where to find them if an employer denies their existence.[22]

4 DON'T USE YOUR EMPLOYER'S RESOURCES

Avoid using your employer's resources for making a disclosure or filing a retaliation claim.

Your work phone, computer, copier, and any other institutional resources all belong to the agency, and it is likely that if you use those resources to make a disclosure or file a retaliation claim, identifying information will be in management's hands soon after you blow the whistle.[23]

Time is also an institutional resource. Depending on the circumstances, you could end up enabling your organization to make the argument that you committed time fraud, misappropriated agency time or resources, or simply are a poor performer.[24] Unless you have specific approval, such as through a union collective bargaining agreement, you also may not be able to use work time to prepare a defense for yourself in a retaliation case.

Even off the clock, you also should make it clear that you do not speak for the agency—especially if you are communicating concerns to the press.

CHECK TO SEE WHO, IF ANYONE, WILL SUPPORT YOUR ACCOUNT

Solidarity is important for your ability to make a difference and survive professionally. Do not wait to be cut off by your agency.

Without exposing yourself as a threat to the organization, gauge the level of support among your co-workers for the concerns you might raise. See if others share your concerns.

This is important for quality control, not just for your sense of solidarity. They may have knowledge to which you were not privy, and that could change your mind or modify or expand your concerns. Get a sense of whether key people will back up your account. If you can't count on others to later testify as supporting witnesses, you may be well advised to wait before challenging misconduct. Try to stay on good terms with administrative staff who may be in a position to know of impending agency actions.

Seek out potential allies before your situation heats up, and work through intermediaries when possible. Enlist the assistance of sympathetic interest groups, elected officials, or journalists. The strength of your support coalition is often key to making the legal rights you have on paper work for you in reality.

CONSULT AN ATTORNEY EARLY

Do not wait until you are in the "career emergency room" before

seeking professional help. As with preventative medicine, getting a little legal advice up front can protect against the need for extensive intervention later. Be careful to find an attorney who respects your goals as a whistleblower, and who is willing to safeguard your evidence. Many attorneys see their duty as preventing you from incurring the liability you are willing to risk but that you should be prepared for. This will be an intimate professional partnership, so make sure you trust and are compatible with your lawyer. One reason some whistleblowers hire attorneys is because they can make disclosures on behalf of an anonymous client, legally shielded by attorney-client privilege.[25]

7 CHOOSE YOUR BATTLEGROUND CAREFULLY

If possible, pick a time and set of circumstances where you will have the most impact with your disclosure. The timing of your disclosure, particularly to the press, is a serious strategic decision that can affect the chances your disclosure will receive attention. Timing can also affect whether you face retaliation. Press coverage can cut both ways: it could shield you from immediate retaliation while you remain in the media spotlight, but it could also anger your management more than if your disclosures were more discreet.

If you do decide to disclose your evidence to the press, it may be wise to release your evidence incrementally rather than all at once. This can spark repeated stories that sustain the spotlight, and provide a chance to call the bluffs of overly broad institutional denials. See Chapter 5 for an extended discussion of working with the press.

8 HAVE A WELL-THOUGHT-OUT PLAN

Those who are abusing their power must be reacting to you, not vice versa. Otherwise, you will get overwhelmed by the agency's superior resources, access to information, and political clout, and its presumed institutional credibility.

Be clear-headed about precisely what you expect to accomplish and how. Do not premise your actions on the vague notion that the truth will prevail. Plan out a step-by-step scenario of what documents should be released when, and how your organization's responses will be perceived by key audiences such as the press or government

oversight bodies. As part of your advance work, get information into the hands of key potential organizational and political allies, and earn their commitment to reinforce your disclosure. Try to prepare for your management's counter-moves by anticipating agency reactions to your charges and by mapping out the response to those moves. The tenor of this first exchange may determine if the immediate battle with your organization will be quick or drawn-out.

DEVELOP AN EXIT STRATEGY

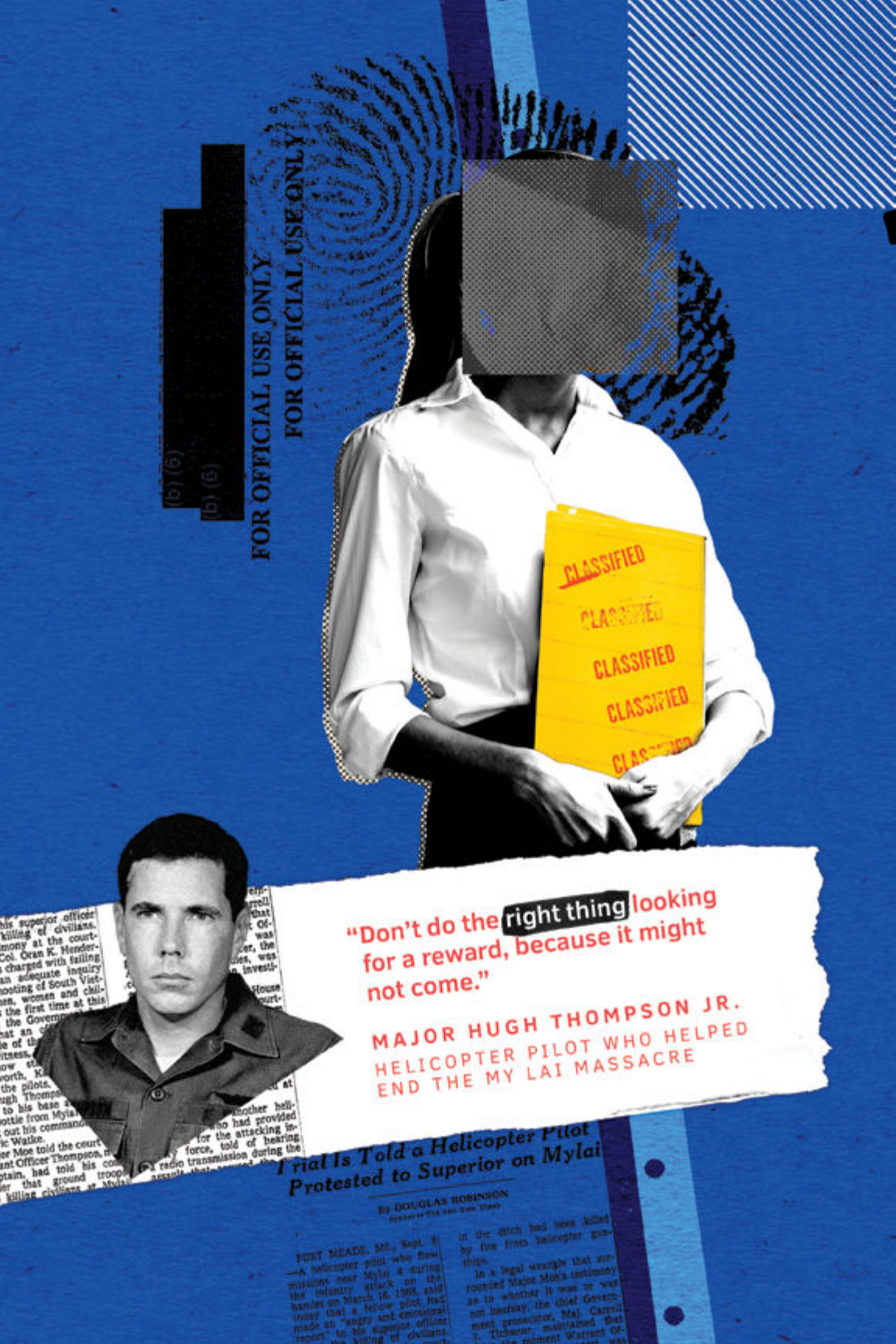
Map out where your actions will leave you a year from now, two years from now, five years, and further on. Plan out the route you want to take and how you reasonably expect your professional path to proceed. There is little doubt that you are about to embark upon a journey that will have a significant impact on your professional and personal life, and you should be prepared with a realistic roadmap of how you might get where you want to go in your career. However, you should also have contingency plans since once you make a disclosure, particularly if it becomes public, your career and life may change in unexpected ways.

OFTEN THE BETTER WAY

Delivering the Message, Not the Messenger

Throwing away your entire career, particularly if there are other ways to air the problem, can be imprudent and counterproductive. In addition, bureaucracies prefer to focus on the "disgruntled employee" rather than the substance of the problem. The longer you can keep the spotlight on the issue and not on you, the greater the chance the problem will be addressed, the longer you will maintain access to evidence necessary to prove your concerns, and the greater the chance you can keep your job and avoid retaliation.

As discussed in the next chapter, you can bring agency troubles to light by focusing on the message without making yourself the target of management's anger. The best way to do this is by providing powerful evidence to those who can expose the wrongdoing and take action without leaving an obvious trail for managers to trace back to you.


FOR OFFICIAL USE ONLY
FOR OFFICIAL USE ONLY
(b) (6)
(b) (6)
CLASSIFIED
CLASSIFIED
CLASSIFIED
CLASSIFIED
"Don't do the right thing looking for a reward, because it might not come."
MAJOR HUGH THOMPSON JR.
HELICOPTER PILOT WHO HELPED END THE MY LAI MASSACRE
Trial Is Told a Helicopter Pilot Protested to Superior on Mylai
By DOUGLAS ROBINSON

CHAPTER 2

Deliver the Message, Not the Messenger

One way you can spur change at your agency is by releasing information about wrongdoing while staying under the radar.

In order to be anonymous, you must shield all of the identifying information that can be traced back to you, not just your name, from public disclosure and from your management. Your desire to remain anonymous may force you to make some high-stakes choices on what information to disclose.

In some instances, the evidence that reveals agency misconduct also inherently reveals the whistleblower source, such as a sensitive memo with an extremely limited circulation or an email sent to only a few recipients. In other words, when few people know the truth, the facts can be the equivalent of your signature. In these cases, you could suffer career damage if your agency learns that you were the employee who released the information.

Unless the information you're disclosing has titanic significance, risking your career in order to expose one act of misconduct is hard to justify.

The key then is to stay undercover and work on your own time with others, such as an advocacy group or journalist, to share the critical information in a way that leaves no fingerprints (or as few as reasonably possible). Strict

confidentiality procedures coupled with ready legal assistance can help maximize your protection.

In short, anonymity prevents retaliation. Anonymity does not necessarily mean that reporters, advocacy partners, or Congressional staffers you choose to work with will not know your identity. In this book, we generally use "anonymous" to refer to whether your agency or the public knows you are a whistleblower.

Anonymity does not necessarily mean that reporters, advocacy partners, or Congressional staffers you choose to work with will not know your identity.

Being anonymous also allows you to keep your job and to access a sustained flow of information from your agency. If you are able to maintain your anonymity, you may get advance access to any organizational strategy to deny or cover up your anonymous disclosures. This insider role is especially powerful if you are the organization's expert on the topic and your knowledge is needed to craft the response.

Needless to say, being on the organization's damage control team can be especially advantageous in keeping a controversy alive—you can expose deliberate misstatements your agency makes to the press or to Congress. This can keep authorities or the public a step ahead of government attempts to perpetrate a cover-up. By contrast, once you're exposed as a threat, the flow of information to you will dry up.

Techniques that have been effective at shielding identities and getting the truth out for past whistleblowers include working with advocacy partners, using the Freedom of Information Act to get documents released, and working through collective action to shield individual whistleblowers.

Whether you're working with journalists, advocacy groups, or Congressional staff, you should pin down specific confidentiality commitments before exposing yourself to risks. Some groups less sensitive to the plight of whistleblowers may choose to risk exposing your identity for what they believe is the greater good. Congressional staff may not realize they are exposing you when they demand answers from agencies by asking questions that sound like the points you are known to have made internally. Because of the great risks that come with whistleblowing, it is important to make a plan with a trustworthy advocacy group or publishing partner to prevent your exposure.

Sometimes developing and implementing such a plan takes weeks, months, or even years. Considering the alternatives, however, the wait and effort in planning are well worth it.

Working with Advocacy Partners

Having external allies and public opinion on your side can help you safely and effectively bring the truth to light. Advocacy partners can be a networking lifeline to neutralize workplace isolation, whether you are a secret source for disclosures and thus cannot talk to anyone at work about what you are doing, or you become ostracized because management identified you as the source. An outside group can help provide you with resources, connections, and assistance in developing a constituency for the truth about abuses of power your agency is hiding. This outside affiliation can be key to effectively utilizing your limited time outside of work.

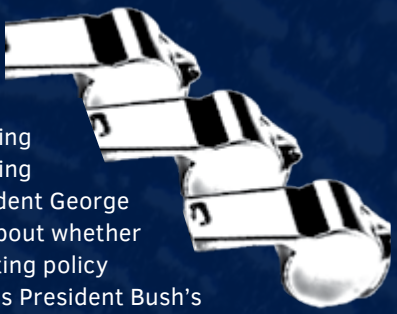
An advocacy partner may be a union, nonprofit organization, or professional society.[1] Whatever you choose, it is essential that you trust that the partner shares your goals and priorities, including minimizing negative consequences to you, so that your concerns and welfare are not subordinate to a pre-set agenda. An advocacy partner can work with you, your attorney, reporters, or any other players relevant to getting the truth out, such as Congressional committees.

It is essential that you trust that the partner shares your goals and priorities, including minimizing negative consequences to you.

The advocacy partner can act as both a shield to protect your identity and a conduit for your information to get to the outside world so that your concerns become known and hopefully acted-upon. This partner may also be able to identify allies within your organization.

Take the classic example of a leaked document. A document detailing disconcerting information the public should know about has been broadly circulated within an organization.[2] An employee who wants to make sure this document enters the public domain could try to contact a reporter directly, or could entrust it to an advocacy partner.[3] The partner could negotiate terms for its use with the reporter, organize others to comment about it on the record, and publicly follow up by pushing the agency to respond.[4]

LEAVING NO FINGERPRINTS



As an oil-industry favorite with a history of pro-drilling advocacy, Gale Norton faced skeptical Senators during her confirmation hearings in 2000 to serve as President George W. Bush's first Interior secretary.[5] She was grilled about whether she could set aside her personal views when evaluating policy decisions, particularly on high-profile issues, such as President Bush's proposal to drill for oil in the Arctic National Wildlife Refuge. To allay those concerns, Norton unequivocally pledged to relay "the best scientific evaluation of the environmental consequences" from oil development in the Refuge.[6] She lied.

After her confirmation, Alaska Senator Frank Murkowski wrote to Norton requesting her department's assessment of the effects of oil drilling on the Porcupine caribou herd in the Refuge. Norton directed Murkowski's questions to the Fish and Wildlife Service, an agency within the Interior Department that oversees the Refuge. The Fish and Wildlife Service reported its conclusions back to Norton but the conclusions did not suit her—so she doctored the responses.[7]

Fish and Wildlife Service employees contacted Public Employees for Environmental Responsibility and provided the group with the paper trail consisting of two letters: one from the Service to Norton, and the other from Norton back to Murkowski. The contrast between the letters is stark. Norton made substantive changes to the scientific findings. All of Norton's changes were designed to minimize the impacts of the projected drilling activity.[8]

An exposé in *The Washington Post* ran on the very day Norton was giving a keynote speech at the Society for Environmental Journalists conference in Portland, Oregon.[9]

Norton admitted that "we did make a mistake," but ascribed discrepancies to an error made when copying information.[10] A spokesman for Norton also admitted they had set aside the Fish and Wildlife Service's scientific findings, claiming she was relying on other"peer-reviewed" data.[11] In fact, the data she used was from a non-peer-reviewed study by an academic who often worked for oil companies and who acknowledged oil giant BP Exploration for providing "encouragement, funding and useful comments" on his research.[12]

This episode helped sink the effort to open the Refuge for drilling during the George W. Bush Administration.[13] Moreover, the sources of the original documents were never revealed.

The episode gained new relevance during the Trump Administration with the nomination of a former Norton political aide, David Bernhardt, to be deputy Interior. Bernhardt's legislative affairs office had sent Norton's misleading letter to Congress.[14] When Hawaii Senator Mazie Hirono asked in a May 2017 hearing about Bernhardt's contribution to Norton's misleading letter, he responded with little more than that his "office had engagement at each stage and ultimately transmitted" Norton's letter to Congress.[15] He subsequently was confirmed as deputy secretary. As of this book's publication, he was on a verge of a promotion. In early 2019, President Trump nominated him to be Interior secretary.

It could use the whistleblower's evidence as the basis for a public campaign that amplifies the whistleblower's revelations by posting documents online, issuing press releases and investigative reports, or placing relevant opinion pieces in news outlets.

In other words, it helps to have friends. But remember, each advocacy organization has its own agenda. Even if your interests appear to be aligned, the organization has no formal obligation to be loyal to you. Thus, you may want to establish a formal attorney-client relationship with an attorney at an advocacy organization.[16] An attorney-client relationship means that the attorney must work with your best interests in mind. The relationship is covered by the attorney-client privilege,[17] which generally requires the attorney not to disclose certain information you share with them.[18]

The privilege generally shields information from being released, but can be challenged in court if there is some factual basis showing that an attorney gave advice related to committing a future crime.[19] Given that the federal government has prosecuted employees for disclosing classified and other restricted information, it is important for the whistleblower to discuss the extent of his or her personal liability and the potential liability of the attorney regarding the dissemination of leaked information.

You should be careful not to disclose any restricted information to the attorney until the attorney advises you regarding liability; as noted below, there are many scenarios in which a disclosure is protected only if it is made to certain recipients, which often does not include private attorneys.

Not all advocacy organizations will legally represent whistleblowers, though. Further, there can be conflicts between the group's interests and the whistleblower's. When that happens, one party or the other must waive its rights, and the advocacy organization may not want to hamper its options. So, another course is to seek out your own attorney who can act as an intermediary between you and an advocacy organization. The attorney can shield your identity, serve as a go-between for communications, and make sure your interests are not sacrificed.

Make sure you are comfortable with how little control you may have once you hand over information.

If you share information with an advocacy group or others anonymously and without legal representation, those communications are inherently less controlled. Unless you obtain an advance agreement on conditions for the

KEEPING THE GENERALS FROM GETTING TOO COMFORTABLE

After the 9/11 terrorist attacks, U.S. counterterrorism spending surged, ostensibly to keep Americans safe.[20] Not all of that money was used that way. An example of how counterterrorism funds were being diverted came to light in 2008.

A source inside the federal government provided the Project On Government Oversight with documents showing that the Air Force was building "world class" accommodations on military aircraft for senior military leaders. These accommodations were called "Senior Leader In-Transit Comfort Capsules," and were designed to be "aesthetically pleasing and furnished to reflect the rank of the senior leaders using the capsule," according to the documents.[21] These comfort capsules featured leather chairs, flat screen monitors "of at least 37 inches," and automatically adjusting ambient lighting. One Air Force general ordered the wood to be replaced with cherry, and the brown leather to be ripped out and replaced with Air-Force blue. The millions of dollars needed for the project came out of counterterrorism funding.[22]

POGO worked with *The Washington Post* to break the story.[23] A flurry of other media coverage followed, including a *New York Times* editorial and a segment on The Colbert Report.[24] Senators John Warner, John McCain, and Claire McCaskill all questioned the program.[25] The Air Force scaled back its plans.[26]

material you provide, the organization has a blank check to use the information however it wants, without regard to or even knowledge of the consequences for you the whistleblower. So make sure you are comfortable with your partners and how little control you may have once you hand over information.

You may not need counsel, but at a minimum you should have an explicit conversation with the advocacy partner about your concerns, and you should feel that you're dealing with honest brokers whom you can trust with your professional life. In this situation, it may be difficult to stay anonymous to the advocacy organization's staff, who may want to know who they're talking to (this does not mean they will reveal your identity externally; the

same goes for reporters, Congress, and official oversight offices). Even if you feel you can negotiate on your own with the advocacy organization, it may add a layer of comfort to have an attorney who's working for you be part of the process. They may point out considerations you have not thought of.

There are some additional cautionary notes to consider before you hand over documents to an advocacy group. See Chapter 3 for details on how to minimize your digital fingerprints when moving evidence from your agency to an advocacy partner or anyone else.

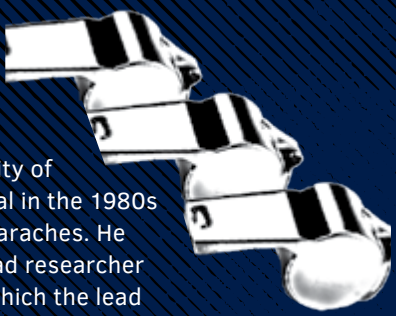
Some whistleblowers, ideally using secure methods, email pertinent documents from their agency to their personal email account or a private digital drop box, ostensibly to be able to work at home but simultaneously to preserve copies of "smoking gun" documents in case the agency later deletes the originals. Before doing so, check to make sure there are not restrictions on emailing or otherwise moving the government documents you need.[27] Also, it can be very dangerous to possess the documents at home, where you are vulnerable to the authorities ransacking your house. You need to be especially careful with how you handle classified information (see the section below on the risks of classified information) or information that the law specifically prohibits public release of,[28] such as material covered by the Privacy Act or medical-patient privacy protections.[29] Remember, as noted earlier, your agency can see how you use government resources such as government computers, networks, printers, copy machines, or email accounts, so emailing yourself files or printing them at work means your agency may be able to identify you.

If you are not careful, your agency could target you for improperly taking possession of restricted information.

If you are not careful, your agency could target you for improperly taking possession of restricted information.[30] From the standpoint of your legal liability, a safer way to prevent destruction of documents is to secure them within the workplace, mixing them in with archives about different topics or electronically filing them under a misleading, innocuous title. Even this is not foolproof. Your agency may have rules on how government information must be secured even if the information does not leave the workplace, so you should consider that as well.

If you decide that removing evidence is necessary, you may want to consider hiring your own lawyer and asking them if they can maintain the files,

AMPLIFYING INSIDER VOICES



Dr. Erdem Cantekin was a researcher at the University of Pittsburgh working on a federally funded clinical trial in the 1980s evaluating the efficacy of antibiotics on children's earaches. He became alarmed when he realized that the trial's lead researcher was misrepresenting the results of the research—which the lead researcher began doing after he personally received honoraria and $262,000 in funding for travel expenses from drug companies making the antibiotics. While Cantekin's data showed no advantage to the use of antibiotics over that of a placebo, the lead researcher presented the data to support of the use of these antibiotics.[31]

When Cantekin raised his concerns, his university tried to suppress him. This eventually sparked a Congressional investigation and examinations by the National Institutes of Health (NIH), which had provided over $17 million to fund the research. One NIH review found the lead researcher had "analyzed the data from NIH-funded research in a manner biased toward the effectiveness of the antibiotics he had evaluated with public monies."[32]

Cantekin's disclosures also triggered a decades-long series of retaliatory measures by the University of Pittsburgh, including the removal of his research responsibilities and a salary freeze at its 1986 level.[33]

In the 1990s, Cantekin began working with the Project On Government Oversight (POGO) to help expose the misinformation spread by drug companies who reap billions of dollars in antibiotic sales. Together, Cantekin and POGO released a report in 1994 that convinced an agency within the Department of Health and Human Services to change its guidelines: the new recommendation was for pediatricians to include "watchful waiting" as an alternative to prescribing antibiotics for children's earaches.[34]

and if attorney-client privilege would shield the files. Please note there's a caveat: attorneys cannot legally receive all restricted information that potentially is provided to them, such as classified documents.[35] You can also seek an attorney's advice on the safest way to get your information to an advocacy group or others. Another way to get documents in the hands of an advocacy partner is to help the partner craft a Freedom of Information Act request to your agency (see "Liberating Agency Documents with the

Freedom of Information Act" on page 36 for more).

Smoking guns and proof of cover-ups make a difference. By working with an advocacy partner, you can inform the public of the existence of incriminating documents or other evidence of malfeasance. Public awareness is often the key to holding government entities accountable for malfeasance.

Handing over evidence is only one of the ways you can work with advocacy partners. Another is educating them on the complicated bureaucratic issues, abuses of power, or violations of law that you have witnessed. While these problems can seem arcane to the general public, they often have profound impacts on public policy, and an advocacy group may be able to translate your specialized knowledge in a way that the public can easily understand.

Another option for educating the public is to submit a public comment in a federal rule-making process, as long as you do so outside of work time and using non-governmental equipment. But some offices are so politicized that many employees dare not participate in that process. And unless your comment has information protected by whistleblower laws, federal employee speech outside of the workplace on issues related to their job falls into a gray zone of First Amendment protections—meaning that you can't rely on the Constitution to protect you from on-the-job repercussions (see Chapter 6 for a detailed discussion of legal protections).[36]

Another way you can get insider expertise out into the public domain is to publish white papers anonymously, with the help of an advocacy partner's edits to ensure the issue makes sense to the public and the media. A white paper provides a lay translation of technical terms and concepts, and provides context for the details of an organization's malfeasance or other actions that have a detrimental impact on the public. The result is a media- and public-friendly report that could only have come from an insider. These employee-written white papers have formed the basis of litigation, been the subject of legislative hearings, and helped shift the tide of policy.

Similarly, you can anonymously draft public comments, administrative appeals, document requests, or letters for signature by the advocacy group. You remain anonymous, of course. But the advocacy partner works with you to ensure that the facts are well documented. This includes citing publicly available materials and referring to—or even appending—reproduced copies of internal memos not easily available to the public (see Chapter 3 on how to minimize risks when using electronic communications and digital devices).

THE RISKS OF CLASSIFIED INFORMATION

If you transmit classified information to an advocacy group or anyone else not lawfully authorized to receive it, you risk felony prosecution under numerous laws,[37] including the Espionage Act.[38] Although you may send the information anonymously, there often is encrypted, invisible tracing information that can lead right back to you. The organization that receives the information may face legal risks as well, depending on the circumstances. Unless you are willing to eventually pay the price in potential criminal penalties, you should not try to send classified information to an advocacy partner or others not authorized to receive the information. At the very least, you should have a serious discussion with your intended recipient before revealing classified information to them.

In the Government Accountability Project's experience working with national security whistleblowers, the Project has never come across misconduct that cannot be credibly, effectively summarized in an unclassified manner. It may take classified information to prove a charge, but not to allege there is an abuse of power or other misconduct. As we discuss in this book, you may then be able to bury the incriminating documents in agency files where law enforcement authorities can find them if the institution denies their existence. The Government Accountability Project strongly advises whistleblowers against sending or providing it classified information because of the legal consequences.

An example of safely raising concerns about a classified program in an unclassified way involves John Tye, a former State Department official, who worked with attorney Mark Zaid to safely reveal the privacy and constitutional concerns created by surveillance authorized by Executive Order 12333 in a piece published by *The Washington Post* in 2014.[39] Tye had more leeway to speak publicly because he was a former official, but he also protected himself from potential prosecution. He and Zaid submitted a draft of the piece to "a pre-publication review by the State Department and the [National Security Agency] to ensure the op-ed did not contain classified information," according to *Vice*, a media outlet.[40] "They didn't redact a damn thing," Zaid told *Vice*. Soon after Tye's public disclosures, the Executive Branch's Privacy and Civil Liberties Oversight Board launched a review of the surveillance programs authorized by this executive order.[41]

A less-successful example can be seen in the case of John Reidy, a former CIA official, who worked with attorney Kel McClanahan in an attempt to safely reveal the existence of a "'catastrophic failure' in the spy agency's operations."[42] In that case, the CIA pushed back against every attempt Reidy and McClanahan made to follow the rules, at one point even refusing to grant McClanahan access to the relevant classified information in Reidy's appeal to the Inspector General of the Intelligence Community.[43] This meant that McClanahan was excluded from any interviews with government officials about Reidy's whistleblowing efforts. Even after investigative reporters in 2018 revealed details of the intelligence failure Reidy had blown the whistle about,[44] he remained unable to confirm any information either to the media or to his own lawyer.[45] Despite the disadvantages these restrictions imposed, Reidy remained insulated from more punitive measures, such as criminal prosecution.

Good-faith efforts to avoid using

classified information can also lead to nightmare situations. Take the example of then-National Security Agency official Thomas Drake, who disclosed what he believed was unclassified information about a wasteful, ineffective intelligence program to the *Baltimore Sun* from 2006 through 2007.[46] Drake was charged with five felony counts of violating the Espionage Act for the "willful retention of national defense information" in his unauthorized possession. Three of the counts were connected to three documents found in his basement that he says he was supposed to keep because he was serving as a witness for a Pentagon Inspector General audit. The other two counts were for two documents in his email, one of which was marked "unclassified" and the other was declassified three months after he was indicted in 2010.[47] Drake eventually pleaded guilty to a single misdemeanor charge of computer misuse for using NSA's computer network to access information that he provided to someone not authorized to receive it.[48]

National security agencies also have a history of classifying documents after they are disclosed to the press, the public, or Congress.[49]

If the circumstances are such that you do decide to send classified information to an advocacy partner or others, tread extremely carefully. Given the serious potential legal consequences, including imprisonment, we recommend seeking advice from an experienced attorney who works for you before taking any action involving classified information. They can help you navigate this minefield and make informed choices.

It is highly unusual for advocacy organizations to have staff with security clearances that legally permit them to see classified information. They may not even have the option of destroying the disclosure, since they would be potentially destroying evidence of a crime. Some organizations want to avoid any potential liability that might result from receiving government secrets and might feel obligated to turn it in to the government, exposing the whistleblower to legal consequences if the data associated with the document can be traced back electronically or if there are other clues for the government's leak investigators. Other organizations may be more receptive, but may not have thought through how to minimize the risks to you or to themselves. Don't presume the advocacy partner or others you contact will be knowledgeable, sophisticated, or willing enough to shield your identity.

If you have classified information you want to disclose, an organization that is committed to protecting you would consider identifying a sympathetic member of the Senate or House intelligence committees, who is more likely to protect your identity and act on the evidence they can lawfully receive.[50] The organization could do this without coming into possession of the classified documents or information. Another alternative is for the advocacy partner to make its own unclassified summary of your disclosure to an Office of Inspector General or other authorized recipient without the classified information.

The next chapter will discuss how to shield identifying information as much as possible when communicating with others outside your agency about your concerns, whether or not classified information is involved. Though the risks vary depending on the disclosures you are contemplating and certain techniques can reduce the chances you will be identified, the path of whistleblowing—even anonymously—will always be professionally perilous.

Liberating Agency Documents with the Freedom of Information Act

The Freedom of Information Act (FOIA) is a tool that allows anyone to request records from federal agencies. Virtually all states also have some form of public records law.

For employees inside an agency, FOIA can be a tremendous tool for putting the agency on the record. The whistleblower can tutor advocacy partners about which records to seek, or even ghostwrite FOIA requests.

If you write documents as part of your job at an agency, you should try to minimize the chance these records can be withheld from public view under FOIA exemptions.[51] For example, since agencies often attempt to withhold records under the "deliberative process" exemption,[52] if you separate legal and policy analysis—which is the kind of information often covered by the deliberative process exemption—from factual information in your writing, it is harder for an agency to justify withholding a document or documents in full. For example, you could write a memo that includes a timeline of relevant facts in one section and legal analysis in another section.

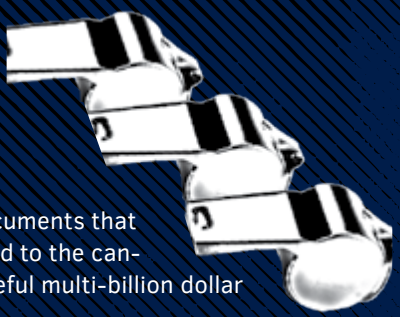
If you are receiving key records, you may consider circulating them as widely as possible without drawing unwanted attention to your action.[53] This wide circulation helps keep records available under FOIA from a multitude of sources.[54] It also makes it much harder for agencies to deny the existence of documents that have a high likelihood of turning up.

Email is another asset in the war to make government business public. Many managers write candid thoughts in emails that they would never put into formal correspondence, yet an email is just as much a public record as an old-fashioned memo is.[55] The ease with which emails can be forwarded makes email a powerful dissemination tool.

Email is another asset in the war to make government business public.

Anonymous whistleblowers can act as watchdogs for FOIA cover-ups. For example, during investigations of unsafe nuclear facilities, the Government Accountability Project worked with public employees to draft precisely targeted FOIA requests. These employees made copies of the records, and provided notice when documents were moved off-site, concealed, or destroyed.[56] Insiders have also blown the whistle to Congress on alleged abuses of the FOIA process.[57]

"ED" AND THE SUPERCONDUCTING SUPER COLLIDER



Working with the Project On Government Oversight (POGO), an anonymous whistleblower disclosed documents that ultimately generated major media attention and lead to the cancellation of the Department of Energy's (DOE) wasteful multi-billion dollar Superconducting Super Collider project in 1993.[58]

POGO only knew the whistleblower as "Ed," although that wasn't his real name. While they worked together, Ed mailed documents to POGO in plain envelopes and called the organization every other day at a certain time. Those phone calls proved to be crucial in ensuring that Ed could let POGO know what was happening, but also so that he could answer any questions the organization had about the documents he sent.

The Supercollider scandal reached a crescendo when Ed mailed POGO a draft DOE Inspector General report concluding that 40 percent of federal money spent on the project up to that point had been either wasted or misspent. Taxpayer money intended for the project had gone to pay $35,000 for a holiday party and $39,000 for coffee, among other items. Within weeks after Ed sent POGO the disclosures, the House of Representatives voted to kill the project.[59]

But no good deed goes unpunished. Then-Secretary of Energy Hazel O'Leary launched an investigation to identify the source, sending Inspector General agents with badges to POGO's office demanding to know the identity of the whistleblower. POGO provided no information to the agents, and Ed's true identity remained anonymous, even to POGO staff.[60]

Ironically, Ed's efforts exposing the multi-billion dollar waste ultimately led to him losing his job: the program was cancelled. He later called POGO to let them know that he was all right, had found a good new job, and was proud that he was behind the cancellation of this wasteful government contract.

It's important to keep in mind, however, that agency officials looking to find sources of leaks could use FOIA requests as clues to identify whistleblowers through the specificity of the requested document that could only be known by key employees. This appears to have happened with then-FBI agent Terry Albury, who pleaded guilty to providing classified information to *The Intercept*. Albury disclosed to reporters a pattern of surveillance by the FBI that posed risks to civil liberties, and backed that up with information from documents showing weaknesses in the Bureau's rules against racial and religious profiling.[61] *The Intercept* filed FOIA requests for documents Albury had disclosed to it, and the FBI matched those requests up with Albury's access to many of those documents.[62]

Harnessing the Collective Voice to Shield Individuals

Union organizers know that collective action provides both power and anonymity for members of groups. While bad managers can punish individual employees for simply bringing up problems, both retaliation and smears become more difficult to carry out when a group of employees speaks with one voice.

The larger the group, the more the power imbalance is neutralized. For example, the Government Accountability Project recruited the president of the Food Inspectors Union to publicly speak in congressional testimony for a number of whistleblowers, providing cover for those concerned about harassment—a way to launder the truth on the record.[63]

Use employee surveys to document or dramatize problems within organizations without putting individual employees in the spotlight.

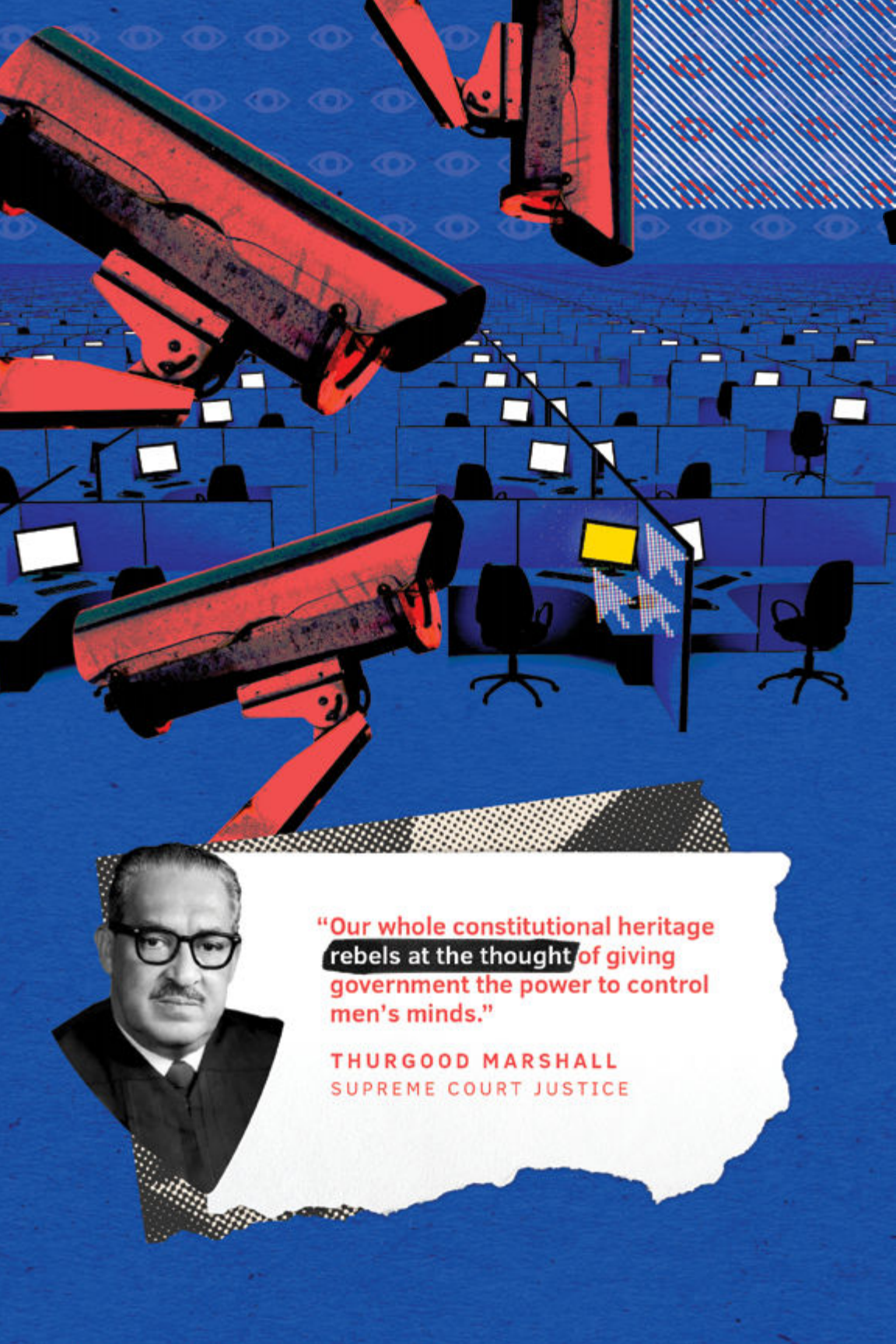
A way to put this principle into action is to use employee surveys to document or dramatize problems within organizations without putting individual employees in the spotlight. With the help of an advocacy partner, surveys can be worded with employee input to expose the most important problems facing the organization.[64]

Once the survey is finalized, an advocacy partner works with employees to distribute the questions, encourage participation, and compile the results.

The final product is a targeted audit of the organization's leadership, fashioned by the people who best know its strengths and weaknesses.

The results are then provided to survey participants, the organization's leaders, other decision-makers, and the media. Press amplification of survey results can help keep an organization's leaders accountable, as public scrutiny can pressure leaders to address the problems identified and to make needed changes.[65]

There are other benefits to conducting employee surveys. Aside from diagnosing problems within organizations and holding leaders accountable, surveys can show individual employees that they are not alone in their concerns, reducing the sense of isolation. Best of all, if the survey is credibly designed to protect the identity of its participants,[66] this can be accomplished without threatening the job security of any employees who participate.



"Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."

THURGOOD MARSHALL
SUPREME COURT JUSTICE

CHAPTER 3

Digital Security for Whistleblowers

Technology can be a valuable tool for blowing the whistle, but it can also make it easier to identify those who expose wrongdoing. While you may be able to share information with the click of a button, chances are that click will be tracked. Luckily, there are tools that can help you remain anonymous when reaching out to advocacy groups, journalists, or other potential allies online.

Digital security best practices are constantly evolving, as are detection technologies and techniques, so there are some general principles that are important to keep in mind while you decide whom and what to trust.

Think Before You Click

Always remember that digital security tools—including those reviewed later in this chapter—may mitigate risk, but they can't eliminate it. State and private actors have the ability to infiltrate many digital devices. No system is foolproof and it's possible that previously unknown security flaws or user error, either by the whistleblower or those they are in contact with, could expose the source of the information.

The good news is that if you do your homework and are careful, some tools can help maintain the security of your conversations even if all your communications have been intercepted. Basic lessons to keep in mind are summarized below, with references for more advanced homework.

1 BASIC DIGITAL HYGIENE IS IMPORTANT

Almost everyone can benefit from doing a basic digital security review, even if they aren't looking into using online whistleblower tools. Taking precautions such as using multi-factor authentication to lock down online accounts and using strong unique passwords (or better yet, a password manager) can help reduce your exposure to online threats, such as criminal hackers, or government investigations seeking the source of leaked information.

SecurityPlanner.org, a tool from the University of Toronto's Citizen Lab, is an interactive guide that suggests ways you can protect yourself (and your data) online.[1] The Electronic Frontier Foundation's Surveillance Self-Defense guide is also a valuable tool that can help you to assess what digital risks you face and to find resources to offset those risks.[2] All of the tools and practices set out by these guides amount to a good baseline of security best practices, or "digital hygiene."

2 KNOW YOUR DIGITAL ACTIVITIES ARE BEING WATCHED AT WORK

Accessing and removing information from government systems can be as treacherous as transmitting it. Even the best encryption will not help if you already have exposed yourself as a threat. Monitoring software is widely reported to be used by employers, both in and outside the government.[3] The capabilities of such software varies, but it's safest to assume that anything you do on an employer's network or using their hardware, such as a work laptop or smartphone, can be tracked.

Be careful about what information you access at work. Many organizations consider high-tech leakers to be like hackers, and use highly advanced specialists to uncover both. Employers usually maintain logs, keep careful track of who has access to information, and monitor for unusual patterns of access.

For example, you could come under suspicion if logs show you were one of only a few people to print or email a document that later leaks. Similarly, you could draw scrutiny if you use work resources to access

information related to leaking or blowing the whistle, so it's best to do research on these issues outside the workplace not using work-issued devices, and to use some of the privacy protection tools we will discuss later in this chapter.

Be careful about what information you access at work.

In some cases it may be advisable to avoid removing data from networks directly. Some organizations automatically identify which machine accessed a file, and removing information through a flash drive, for instance, may look suspicious or even immediately trigger alarms. Consider if it's possible to instead take pictures of the screen with a separate device under your own control. Another approach is to transcribe the information word for word on paper.

As discussed in Chapter 1, it's important that you protect the information so investigators or journalists can later verify its authenticity. If the information is on paper, bury the original document in an archive or a file with a misleading name, or "misfile" it with documents on another topic. You may want to leave a physical copy of the information hidden somewhere secure inside the organization. Also note where the document is stored electronically and be prepared to describe the structure of your organization's systems to whomever you are working with to blow the whistle.

If possible without revealing your identity, save an electronic copy of the file to a location where it is unlikely to be found, to safeguard against later erasure of the original. If the information isn't time sensitive, create as long a time lag as possible between when you access the information and when you blow the whistle to reduce suspicions based on when people looked at it in the system.

3 KNOW YOUR DIGITAL ACTIVITIES ARE BEING WATCHED OUTSIDE OF WORK, TOO

Thanks to previous whistleblowers, including Edward Snowden, we know the government's vast digital surveillance capabilities include collecting information about Americans' communications.[4] Despite some transparency reforms, the classified nature of many surveillance programs makes it hard to gauge their scope.[5]

Many different entities, such as social networks, email providers, and the companies that actually provide internet access, also collect massive amounts of information about users in order to carry out their work and to fuel the online advertising market. This may include not only the content of communications, but also the "metadata"—such as what sites you visited or who you contacted and when. While the government may not have immediate access to your online activities, online-service providers may be legally compelled to turn over records in certain circumstances, such as during the course of a criminal investigation.

If you determine that whistleblowing is the right path for you, at a minimum never use your own or your employer's equipment to transmit information. Use a distant public computer at a library or internet café not likely to be associated with you. If you use a public Wi-Fi access point, avoid circumstances where you must log in or where you'll be in the view of cameras. Consider only doing research about your next steps while using some of the tools described later in this section, such as the Tor Browser or Tails.

4 DON'T LET YOUR DOCUMENTS BETRAY YOU

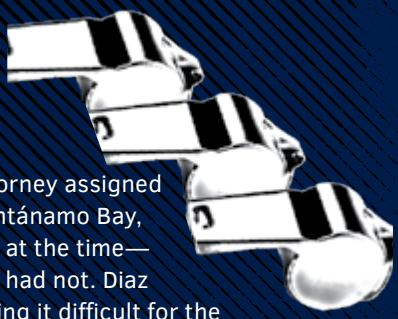
Carefully consider if documents can identify you as the source before you share them. How many people within the agency have access to them? Is there identifying information built into the text such as time-stamps, or tweaks to language or formatting unique to a certain version?

If you plan to share digital files, you should strip that information when possible. Tips on how to strip the info from file types such as Word documents, PDFs, and images are readily available online. Research on ways to cover your digital footprints is best done via Tails or Tor, tools that will be discussed later in this chapter, because searching for this type of information could throw suspicion on you if uncovered later during a leak investigation.

Carefully consider if documents can identify you as the source before you share them.

Scans of physical copies of documents may also include identifying information. For example, most printers leave tracking information in the form of dots not obvious to

GOING ANALOG CAN BE RISKY TOO



In 2005, Commander Matthew Diaz was a Navy attorney assigned to the U.S. naval base and detention center at Guantánamo Bay, Cuba. Over 550 men were held at Guantánamo Bay at the time—some who had committed terrorist acts, some who had not. Diaz was deeply troubled that the government was making it difficult for the detainees to have their day in court. One barrier was the secrecy surrounding the men's identities. Even though the Supreme Court had ruled six months earlier that the prisoners had a legal right to challenge their detention in court, the Pentagon insisted the detainees had no legal rights to counsel. And "keeping the names secret made it harder for volunteer lawyers to file petitions on the prisoners' behalf" to challenge their continued detention, according to *The New York Times*.[6]

Feeling a "moral obligation," as he put it, one night Diaz printed out a document filled with names and other information on the detainees, put the document inside a Valentine's Day card, and, several days later, mailed it to an attorney at the non-profit Center for Constitutional Rights based in New York City.[7] Unsure who had sent the document and what to do with it, the attorney reached out to a clerk for a federal judge presiding over a Guantanamo lawsuit. The court directed her to turn the records over to the Justice Department, and the FBI began to investigate.[8]

The *Times* reported that the FBI "had little difficulty narrowing the list of possible suspects. Diaz had printed the document from his own computer, bought the valentine at the base exchange and left his fingerprints on the list."[9] He was convicted in 2007 on charges of "passing classified information" with an "intention to harm the United States" and was sentenced to six months in prison.[10] Diaz also lost his license to practice law.[11]

A year after Diaz mailed the information to the Center for Constitutional Rights, the Associated Press obtained the names of the detained men through a Freedom of Information Act lawsuit.[12]

Diaz's story shows that an electronic trail can be left by devices we don't think about—in this case, printers. It also shows that analog methods, such as using the mail and printed documents, can also leave behind clues for law enforcement authorities. It shows that the lack of a dialogue between a whistleblower and the recipient of their information can lead to actions without the benefit of informed deliberation that put the whistleblower in legal jeopardy. It also shows that there can be legal alternatives for getting the information out.

the human eye. These should be scrubbed before the document is shared, if at all possible, through methods such as converting the document to black and white and making repeated printed copies that can distort the trackers.[13] However, be aware that most modern scanners and copiers also have internal memory that keeps a log of files they are used to produce, so use a device that is not linked to you.[14] And remember that even when taking those measures, watermarks and microdot tracers—like those that appear to have exposed Reality Winner—can be difficult to entirely remove.[15] For that reason, you may want to consider taking photos of physically printed documents or of information as it appears on your screen.

If you have managed to safely obtain a sensitive document, don't store digital copies on your personal computer or phone if possible. Also avoid cloud storage services like iCloud or Google Drive that can be linked to you. Instead, keep them isolated and encrypted on new, securely stored flash drives that have never been used on a computer that can be traced to you.

5 ENCRYPTION IS YOUR FRIEND

The best defense against digital snooping at this time is using technologies that incorporate strong encryption, both for communications and stored data. For communications, end-to-end encryption—encryption that applies throughout the process to help ensure that only the sender and receiver can read the contents—is currently the best tool to use. This method creates a protected digital connection between the parties of a communication who know the appropriate "key." Encrypted storage works similarly and can typically be unlocked using a passphrase key devised by the user.

However, it's important to note that the strength of the protections that encryption provides is typically based on how long it could take someone to "crack" the key by using computers to make automated guesses to unlock the data. That means that even if communications are secured with the strongest options currently available, future advances in computing may make something that would take years or decades to crack now easier to crack in the future.

Encryption can protect the content of different types of communications, including instant messages, email, and voice calls. Generally,

metadata, such as when and who you contact, may still be observable because this information is necessary to deliver messages. Some encrypted-communication products mitigate that risk by retaining minimal records or logs of such data. Check the tools section of this chapter for more information.

Be sure to verify the identity of contacts before sharing sensitive information. When visiting websites, make sure they are Hypertext Transfer Protocol Secure (HTTPS). Websites that don't have this are susceptible to cyberattacks that can be used to trick you into thinking you are sending information to a site you trust when you are actually sending it somewhere else. Private information sent via unsecured sites may also be vulnerable to snooping by other people connected to your same network.

Be sure to verify the identity of contacts before sharing sensitive information.

The Electronic Frontier Foundation offers a web browser extension to assist in preventing this problem.[16] The group's Privacy Badger tool, along with the browser plugin NoScript, can also help make your online experience more secure by blocking digital trackers and potentially insecure parts of websites.[17]

BE CAREFUL WHOM YOU TRUST

It's important to consider that using an encrypted communication method doesn't stop whomever you are communicating with from voluntarily (or accidentally) sharing things further. Reality Winner was exposed when *The Intercept* shared her documents with a government agency to verify their authenticity.

Consider: would the organization or journalist you're working with be willing to resist a subpoena to protect your identity?

Before sharing records with a journalist or organization, make sure the recipient will be satisfied to authenticate the record by using other information or by proof such as supporting witnesses, not by running the document past its

originating agency. Your communications may also be exposed if their (or your) devices are compromised, either through malicious hacking or a legal method, such as being forced to comply with a court order.

If you have safely accessed information, one option is to transmit that information through a tech-savvy lawyer who uses encryption best practices. In addition to the technological safeguards, you may be shielded by the attorney-client privilege if you pursue this route. However, that protection may not hold up in all situations, such as when facing Congressional inquiry.[18] A lawyer also may be able to negotiate an agreement with legally binding commitments before you turn over sensitive information to potential allies.

Research the security track records of individuals and organizations before you reach out to them. Do they use recommended encrypted communication services? Will they commit to stripping any identifying information from documents, and explain to you their process for doing so? What is their policy on responding to government demands for information, and how have they responded to past demands? Have they been the victims of hacks before? If so, what was the fallout? Have sources been compromised due to their digital security failures?

Once you've decided to reach out to an organization or journalist, carefully consider what you want the ground rules for your communications to be.

These questions and more will play into how much information you feel comfortable sharing with those you contact. Consider: would the organization or journalist you're working with be willing to resist a subpoena to protect your identity? If not, do you want them to know who you are?

Once you've decided to reach out to an organization or journalist, carefully consider what you want the ground rules for your communications to be. Ask for concrete definitions for terms like "on background" or "off the record," which organizations and journalists may interpret in different ways (see Chapter 5 for more on this).

7 USING DIGITAL TOOLS ISN'T ALWAYS THE BEST WAY

In some cases, in-person meetings may be less risky. When setting up a physical meeting, look for places without cameras and where neither you nor the person you are meeting have to sign in or are likely to be recognized. Examples include public parks, community centers, and trails.

And remember: most people now carry an incredibly sophisticated digital snooping device around with them—their smartphone. Location or other types of information tracked by devices such as cell phones (including older "feature phones"), smartwatches, or even other digitally connected devices like fitness trackers may be cross-referenced and used to help identify who a person has interacted with—*even if you turn off location tracking in your devices' settings*—so leave them at home if you set up an in-person meeting, and ask whomever you are meeting with to do the same.[19] Many smartphones also do not allow you to remove their batteries, leaving them vulnerable to potential attacks where the device may appear to be powered down, but actually is still surreptitiously collecting information. If compromised, your phone could even be turned into a video- or audio-recording bug.[20]

Cars can also be easily scanned and tracked through methods such as automated license plate readers; if you are using a vehicle associated with you to travel to a meeting, assume it can be tracked. Similarly, public transit that you pay for with a reloadable card, and apps like Uber and Lyft, collect information about your travels that could potentially be turned over to law enforcement during the course of an investigation. In some cases, going old-school and using foot- or pedal-power to get to a meeting may be the best option.

8 THE DIGITAL SECURITY LANDSCAPE IS CONSTANTLY CHANGING

The tools and best practices laid out in this guide are recommendations based on what is known at the time of publication. But the rapid pace of innovation in information security and the increasing sophistication of digital attacks mean things may be different by the time you are reading this. What is digitally secure now may not stay that way forever.

For example, encryption depends on the complexity of keys, but future developments in computing may make what are now considered secure keys easy to guess. Other surveillance technologies in

development or on the rise may later uncover actions taken now. Just imagine future investigators using facial recognition technology against security-camera archives to look for who may have met with a particular whistleblower advocacy group or journalist.

You should research recent security news about a tool before deciding to use it for sensitive communications.

The Current Toolkit

The Electronic Frontier Foundation's Surveillance Self-Defense guide maintains walk-throughs on how to set up and use many of the tools laid out below.[21] The Freedom of the Press Foundation, a non-profit with an emphasis on protecting public-interest journalism and whistleblowers, is also a valuable resource for information about current digital best practices.[22]

Note that in almost all cases, using a digital method will create some sort of data trail. However, the tools below can help minimize and hide that trail better than using ordinary communication methods.

1 ENCRYPTED EMAIL: PGP

The most commonly recommended way of encrypting email is called PGP and relies on public key encryption. This can be done using a laptop or desktop computer and involves installing special software to set up encryption keys for your email account and then connecting with another person who has gone through the same process. The Electronic Frontier Foundation has a good step-by-step guide for the process. (Note that, as with other tools discussed in this section, PGP has encountered security problems in the past.)[23]

This method is effective at securing the content of email messages, but still leaves metadata, including subject lines, the sender, the recipient, and the date of a message, exposed. If you have digital records on another device, such as pictures of documents that you've taken with a camera or smartphone, you'll need to securely transfer them to the computer you're using for your PGP encrypted email before you can send them on.

Consult current online resources like the Freedom of the Press Foundation or the Electronic Frontier Foundation for best practices to minimize your digital trail.

2 TEXTING, VOICE CALLING, AND DOCUMENT SHARING: SIGNAL

Signal is an app that provides end-to-end encrypted messaging and voice calls. It's more user-friendly than using public key encryption to protect emails, having an interface similar to most texting or instant-messenger services.

Signal can also be used to share digital documents. Before discussing sensitive topics, you should verify the security of the connection between yourself and the other person by comparing safety numbers via the app, a process explained on Signal's website.[24] The app also includes security features, such as the ability to set expiration times for messages, which can be used to minimize the digital trail left in the wake of blowing the whistle.

Signal is available for Android and Apple smartphones, as well as for desktop computers. Signal is open source and has undergone independent security audits.[25] However, the app has also had some security problems, particularly involving the desktop client. The smartphone apps have a longer security record and have had fewer reported security issues to date.[26]

One pitfall of using Signal is that the app, even when using the desktop variant, is inherently tied to a phone number. However, there are steps you can take to reduce the risk of being identified as the user behind a specific Signal account, such as setting up a burner phone[27] and using the device only in certain locations that aren't regularly associated with you. Be sure to erase your call history, which Signal otherwise will maintain locally on your device.

Court documents related to a 2016 subpoena of the app's developer, Open Whisper Systems, appear to show that the only information retained by Signal's systems were the date an account was created and the date an account last accessed Signal's servers.[28] However, without manual or automatic deletion of messages from your devices, the conversation could still be compromised if law enforcement gains physical access to your devices.

3 WEB BROWSING: TOR

Tor is a network that masks your online activities by encrypting your traffic and routing it through different servers, or "nodes," around the world to make it more difficult to track. It also allows you to access

special websites that end in .onion, such as those used by the SecureDrop system, another whistleblowing tool we will discuss later in this section. At the time of publication, the most accessible way to use this network is by downloading an internet browser called the Tor Browser, a version of Firefox with various security functions built into it.[29]

Although Tor is a vital tool for those seeking anonymity online, it has suffered security failures in the past,[30] and some experts believe traffic over the network may receive extra scrutiny from law enforcement or intelligence agencies.[31] Your privacy can also be compromised if you log in to services tied to your real identity during a Tor session when you are also using it to communicate with advocates or journalists.

4 GENERAL COMPUTER USE: TAILS

"The Amnesic Incognito Live System," or Tails, is a free operating system designed to provide users a private computing experience.[32] It can be run on most computers from a flash drive, and it automatically incorporates encryption and other privacy-protecting tools. For example, Tails automatically routes online activities performed while the operating system is in use through the Tor network and comes preloaded with the Tor Browser to secure your browsing from prying eyes.

It is important to note that these added protections generally cause Tails to run slower than other modern operating systems. Tails is an open source project that is continually being improved upon, so it is important to ensure you are running the most recent version. It's also worth reviewing the developer's warnings about issues Tails cannot protect against before using it.[33]

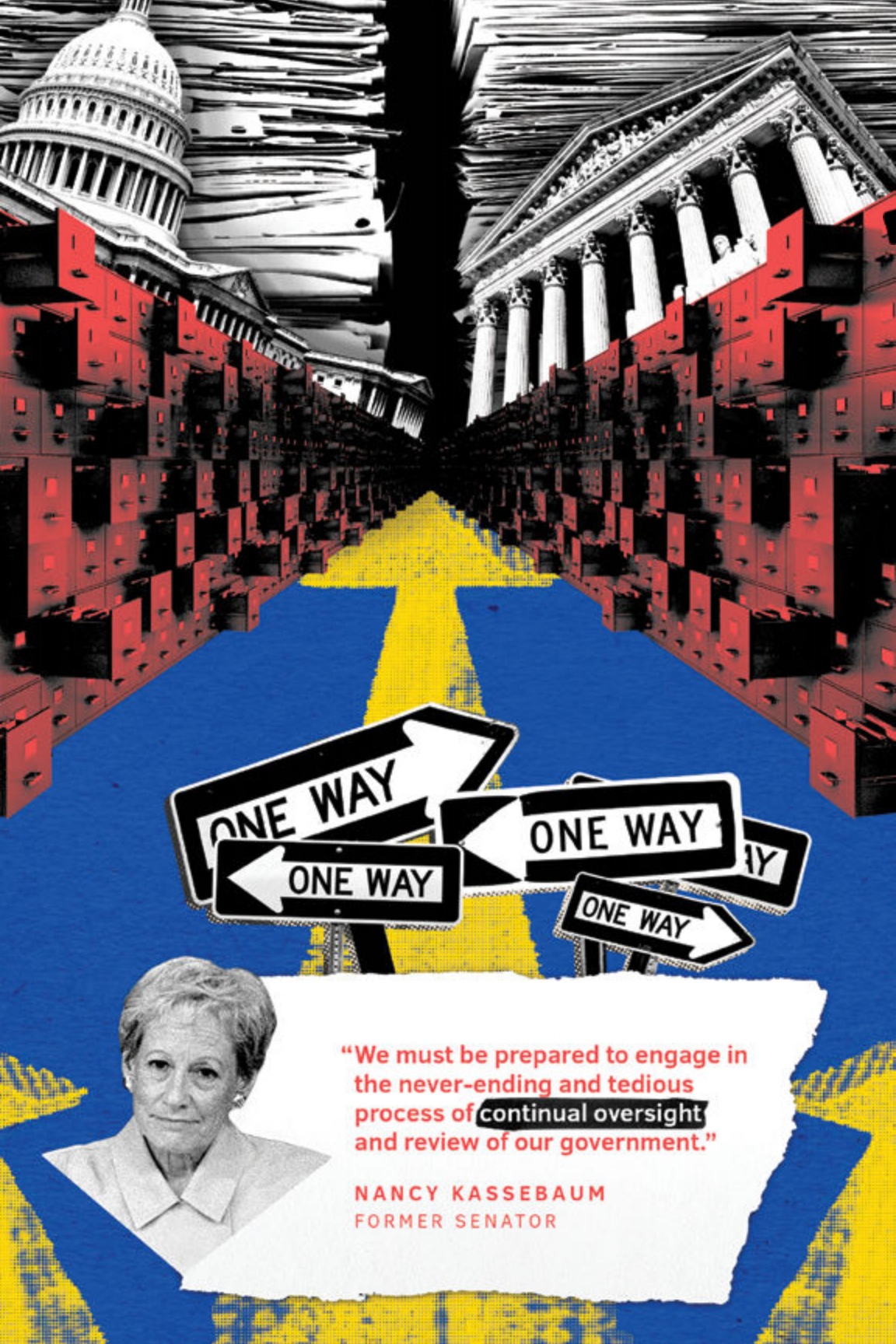
5 SHARING DIGITAL DOCUMENTS: SECUREDROP

SecureDrop is a system designed to facilitate anonymous communication between sources and non-governmental organizations or journalists and is generally considered the most secure digital method to contact a reporter or advocacy group.[34]

Nonprofits and media outlets generally run SecureDrop on their own in-house servers and only access the encrypted communications sent through the system on computers that are running the privacy-focused operating system Tails and that are not connected to the internet, which minimizes the potential for third parties to access

information shared via the system. SecureDrop also does not record many forms of potentially identifying information about submitters, such as the IP address or the type of operating system being used.

SecureDrop requires users to install and send information through the Tor Browser. The Freedom of the Press Foundation, which manages SecureDrop, recommends that whistleblowers who are sharing national security-related information go even further by using cash to purchase a new computer and connecting to the internet via public Wi-Fi that they don't normally use.[35]



"We must be prepared to engage in the never-ending and tedious process of continual oversight and review of our government."

NANCY KASSEBAUM
FORMER SENATOR

CHAPTER 4

OFFICIAL CHANNEL SWIMMING:

Starting and Monitoring Agency Investigations

One of the most treacherous situations for a public servant is navigating the bureaucracy of filing whistleblower disclosures. This chapter is focused on the official channels through which you can report wrongdoing. Note that filing a whistleblower disclosure is not the same thing as filing a complaint of whistleblower retaliation. The channels through which you can file a retaliation allegation are addressed in Chapter 6.

Many employees first disclose concerns to their supervisors. These employees may not intend to "blow the whistle"—they just want to let management know about a problem or have to disclose it to do their jobs properly.[1] The Whistleblower Protection Enhancement Act of 2012 protects disclosures of wrongdoing that federal employees make to supervisors or as part of their job duties (see Chapter 6 for a discussion of retaliation protections).[2] Still, if

a supervisor feels threatened by your disclosure, you could end up in their crosshairs. Conversely, failing to report a problem can also lead to difficulties, particularly if the problem becomes embarrassing and the agency starts looking for a scapegoat.

If reporting the problem to a supervisor resolves the matter, great. If it does not, and you need to go to oversight bodies outside the chain of command, the water becomes murkier. When you go outside of your immediate organization, especially when your concerns become public, it heightens the chance that your management will become angry with you.[3]

Because there is the potential for retaliation when you blow the whistle, especially if you decide to file a formal disclosure outside of the chain of command, you should seek legal advice from trustworthy counsel before taking any action (although there may not be time for this, especially if you are reporting an imminent health, safety, or security matter). Legal counsel will explain what protections are available to you and how to best take advantage of them, and can also help you work with offices that may investigate your disclosure.

If you want to swim in these official channels, the following should be taken as cautionary advice.

Inspectors General

Every major federal agency has an inspector general (IG). One of an IG's main roles is to investigate whistleblower disclosures of internal fraud, waste, abuse, and other types of misconduct. See Chapter 6 to learn more about their role in investigating whistleblower retaliation claims.

An IG office generally conducts investigations and audits. You can file a disclosure with an IG through its "hotline," which can usually be contacted through phone, email, or mail.[4] The scope of an IG review depends on the nature of the issue at hand and what type of staff is assigned to your inquiry.

One of the main roles of an inspector general is to investigate whistleblower disclosures of internal fraud, waste, abuse, and other types of misconduct.

Investigators tend to go narrow but deep, and focus on individuals' misconduct, such as violations of law, regulation, or policy. Investigations that find violations of criminal

laws can result in referrals for prosecutions, but whether to prosecute is a decision made by a Justice Department attorney.[5] Investigations can also lead to non-criminal, administrative penalties, such as termination.[6] Auditors look at program performance or financial management, and typically do not focus as much on individual wrongdoing.[7]

Under the Inspector General Act of 1978, IGs are supposed to be independent of the agencies they oversee. But reality doesn't always match that requirement. Some agency, commission, board, and legislative-branch IGs are appointed by the head of the organization they monitor, creating a structural conflict of interest.[8] And while IGs for most larger agencies are nominated by the president and confirmed by the Senate, giving them greater independence from their agency, those IGs still report to the head of the agency and serve at the pleasure of the president.[9] If an IG is upsetting the Administration's apple cart, they can be removed.[10]

Agency employees may view the IG as a kind of knight in shining armor—an outside, objective force charging up the hill to make all right in the agency world.[11] However, an IG office is a bureaucracy just like any other, and can have all the dysfunctions and limitations of any other workplace.[12] In fact, there have been numerous instances of whistleblower retaliation within IG offices against its own staff for raising issues.[13]

That said, there are dedicated IG staffers who fairly and aggressively work with whistleblowers.[14] An IG office also often works closely with prosecutors and Congress. Even if your plan to expose wrongdoing does not involve going to an IG, an IG may be involved at some point and you should understand the limits of these offices.

YOU SHOULD KNOW THAT INSPECTORS GENERAL:

1 HAVE NO CORRECTIVE ACTION POWER

An IG can identify a problem and then make findings and recommendations. The agency in question does not have to follow IG recommendations, even if the IG confirms your disclosures.[15]

2 DO NOT GUARANTEE CONFIDENTIALITY

The Inspector General Act of 1978 provides that an IG should keep its sources confidential unless it "determines such disclosure is unavoidable during the course of the investigation."[16] This leaves disclosure

of your identity up to the discretion of the IG (an action for which you have no recourse). It's not a theoretical possibility: IG investigators have identified whistleblowers to the whistleblower's management, which then led to management retaliating against the whistleblowers.[17]

Even if an IG does not disclose your identity, it may give away information to management or conduct its inquiry in a way that makes your identity patently obvious.[18] If you choose to remain anonymous, you should consider negotiating signed confidentiality agreements custom-fitted to your situation. In particular, the agreement should provide that, in consultation with you or counsel, the IG will not communicate any identifiable information that can be traced back to you. Further, you should lock in a commitment to provide you with advance notice if the IG decides that release of your identity truly is unavoidable.[19]

3 LACK DEADLINES

An IG can investigate (or ignore) your reports of wrongdoing at its leisure. The IG controls the investigation; you do not. Thus, an IG can take years to investigate a disclosure of wrongdoing. If it completes an investigation, an IG can still sit on the report, keeping it as a "draft" until it's no longer timely.[20] An IG is under no obligation to publicly release the investigative report (though audit reports are usually made public).

4 AVOID CONTROVERSY

IGs sometimes seem to dwell on a $5,000 discrepancy while ignoring a $500 million issue with politically hot policy implications.[21]

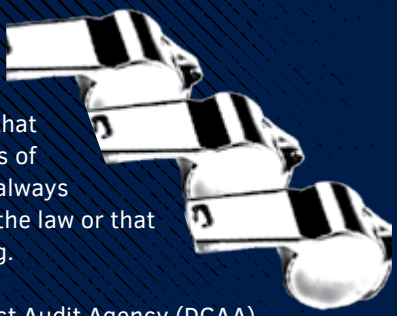
5 CAN TAKE ACTIONS THAT ARE USED AGAINST THE WHISTLEBLOWER

It's possible that your motivation for reporting will seemingly become the subject of an IG investigation.[22] It can seem that the IG wants to discredit your whistleblowing.[23]

Congress

You may believe that problems within your agency would be solved if only Congress knew about them. In reality, a Congressional solution on its own is the exception rather than the rule.

KEEPING CONFIDENCES



There are provisions of the Inspector General Act that instruct inspectors general to protect the identities of whistleblowers.[24] But inspectors general have not always acted in a way that is consistent with the intent of the law or that creates an environment that fosters whistleblowing.

Take the case of Diem-Thi Le, a Defense Contract Audit Agency (DCAA) auditor. In 2005, she made disclosures about flawed audits to the Defense Department's inspector general.

In April 2006, inspector general investigators sent Le's supervisor a letter seeking information on 10 audits that Le had confidentially alleged were flawed. Le had been involved in six out of 10 of those audits.

According to the Office of Special Counsel—which investigated her later claim of retaliation because she faced plummeting performance reviews after her disclosure—"no other non-supervisory auditor was involved in more than two of the 10 audits."[25] A DCAA supervisor, who was found to have retaliated against Le, told the Office of Special Counsel it was "relatively easy to connect the dots" and figure out Le was the whistleblower based on the audits the IG was scrutinizing.[26]

Another relevant case occurred in 2014. Massive numbers of Department of Veterans Affairs (VA) insiders began blowing the whistle against the agency, and hundreds of them contacted the Project On Government Oversight (POGO) confidentially with their disclosures.[27] Many expressed a fear of retaliation if their identities were revealed, even to the VA Inspector General.

In fact, the VA Inspector General issued a broad subpoena to POGO in May 2014 seeking "all records that POGO has received from current or former employees of the Department of Veterans Affairs, veterans, and other individuals or entities relating in any way to wait-times, access to care, and/or patient scheduling issues."[28]

POGO refused, arguing that the subpoena infringed on the organization's "freedom of speech, freedom of press, and freedom of association rights as they relate to all whistleblowers and sources."[29] Senator Ron Johnson agreed and called the subpoena "highly inappropriate" and a "potential abuse of power."[30]

The VA Inspector General dropped its subpoena and never received records from POGO.[31]

While Congress sometimes conducts investigations and investigative hearings, in many cases the bulk of the investigative work was done elsewhere, such as by an inspector general, the Government Accountability Office (GAO, an arm of Congress), or an agency.[32] The official purpose of the Congressional hearing is to create a public record that can inform and build a case for legislation,[33] but it can also be used to dramatize a situation and shape what the public thinks.[34] A quintessential use of this power was the 1994 House of Representatives hearing in which tobacco company CEOs were subpoenaed to testify under oath about their knowledge of the dangers of smoking.[35]

Congress is an unquestionably political entity. It is made up of hundreds of offices led by Representatives and Senators, each with their own stakeholders and political commitments, as well as dozens of committees with different, sometimes overlapping jurisdictions over the parts of the federal government. Capitol Hill is awash with activity and intrigue where short-attention-spans and one-page summaries are common because of overwhelming workloads and a lack of time.[36]

A 2010 federal survey shows that federal employees have far less faith that Congress will protect their identity than an inspector general or the Office of Special Counsel.

If you seek to wade into the swirling eddies of Congress, you face risks such as having your identity inadvertently exposed to your agency. A 2010 federal survey shows that federal employees have far less faith that Congress will protect their identity than an inspector general or the Office of Special Counsel, an independent agency empowered to receive whistleblower disclosures from most federal civilian employees.[37]

However, Members of Congress can be great allies, and sometimes you can appeal to legislators who want to act against bureaucratic breakdowns. Legislators have access to the media and can shine a national spotlight on problems. It can be far more difficult for your organization to retaliate against you if a Member of Congress supports you.[38] As a result, a legislative partnership can be invaluable—but it is a relationship that you must craft carefully.

The first way many public employees contact a Member of Congress is by writing a letter laying out a problem or issue in their agency. That can be a mistake. What sometimes happens with letters from public employees is that

the Congressional office sends a copy to the agency for a response.[39] The perpetrators of the misconduct may be the ones who prepare the agency answer, and they learn the identity of the "troublemaker" whistleblower within their midst. Before sending sensitive material to a Congressional office, you should do preliminary research and have informal discussions to pin down ground rules. Things to consider are:

- **Does the Member have a political stake in the matter?** The Member's relevant voting record could be telling, as could campaign contributions.
- **Is the Member a chairperson or ranking member of a committee or subcommittee with jurisdiction over the issue, or have they worked on the issue in another capacity?** If so, the Member may have staff who is knowledgeable and helpful.
- **Are you a constituent of the Member or close to someone who is a constituent?** Members tend to be more attentive to potential voters.
- **Does the Member have a history of working with and protecting whistleblowers?** Does the staff of that office have experience working with whistleblowers?

If you decide to approach a Member of Congress, you should:

- **Be truthful.** Members of Congress and their staff are under no obligation to work with anyone, unlike staff in oversight agencies in the executive branch specifically authorized by law to accept and review whistleblower disclosures.[40] They will quickly stop working with you if they learn you misrepresented facts.
- **Be concise in your presentation.** Their time is at a premium. You should be very clear about *precisely* what action you want taken, such as having a Member of Congress request that a watchdog agency such as GAO or an inspector general investigate your disclosure. (Members of Congress will rarely hold a hearing based on a whistleblower disclosure without official verification, so you generally should not ask for a hearing as an initial step.)
- **Realize that Congressional staff—not the Member of Congress—will be working on your case, but the Member of Congress will be the ultimate decision-maker.**

- **Do the work for staff whenever possible, such as researching documents and ghostwriting questions or communications.** In other words, "staff the staff." This may mean preparing a file for them on your issue. The file should have a one-to-two page talking-points memo that concisely states the key conclusions supported by the most powerful facts, so that a staffer can make the Member appear as an expert during the five-minute walk from office to hearing room. It also should contain any prior media coverage, and expressions of support or concern from stakeholders whom you have recruited. Staffers will be grateful, because whether or not they agree with you their highest priority is to make sure their boss doesn't appear ignorant or taken by surprise on something important to voters.
- **Be courteous and flexible rather than demanding, and, if the Member helps, express your thanks even if you don't get everything you had hoped for.** You should always strive to be helpful.

If a Member of Congress or, even better, a committee chairperson, takes up your cause it is potentially a huge asset. However, be aware that no individual Member has direct authority over the executive branch. Thus, even in the face of Congressional opposition, an executive agency can still proceed to engage in the concerning activity you have blown the whistle on. That means your best ally is often one with appropriations or oversight authority over the agency in question.

Office of Special Counsel

As discussed in greater detail in Chapter 6, the Office of Special Counsel (OSC) is the main place where federal civilian whistleblowers can lodge complaints of retaliation.[41] Perhaps less known is that OSC is a place where a civilian federal employee can go to blow the whistle on waste, fraud, abuse, or other kinds of misconduct.[42] That said, OSC is not an option for some types of federal-sector employees, such as FBI and military employees.[43]

In order to report a problem to OSC, you must do the following: first, file a disclosure with OSC detailing the wrongdoing. OSC then has 45 days to review your disclosure and determine whether further investigation is necessary (note that OSC often does not meet this 45-day deadline).[44] If OSC finds there is a "substantial likelihood that the information discloses a violation of

any law, rule, or regulation, or gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific danger to public health and safety," OSC must immediately inform the head of the appropriate agency of the matter. That agency head is required to conduct a proper investigation into the disclosed matter. Often, the agency head tasks the agency's inspector general to conduct the investigation. The agency head has 60 days (unless OSC grants an extension) to submit a written report outlining the findings.[45]

This report must include:

- A summary of the disclosure leading to the investigation
- A description of how the investigation was conducted
- A summary of all evidence found during the investigation
- A list of any real or apparent violations
- A description of any action either taken or planned to be taken in response to any violations[46]

Upon receiving the agency report, OSC is required to review it and determine if it contains the required information and whether the findings are reasonable. OSC has to transmit a copy of the agency report to you unless it referred the matter to the Justice Department as a potential criminal case. You have 15 days after receiving a copy of the agency report to submit comments on it to OSC. The Special Counsel then grades the report. If dissatisfied, the OSC either can direct the agency to provide more information, or simply flunk the effort.[47]

OSC transmits the agency report, your comments, and its own evaluation to the president, Congressional leadership, and the Congressional committee(s) with jurisdiction over the agency. OSC also makes these materials available to the public online.[48] If OSC does not receive the agency report within the allotted time including extensions, OSC is required to submit all available information to the president and the proper Congressional committee(s) along with a statement noting the agency failure to file its investigative report.[49]

The disclosure process has several strengths and weaknesses.

Strengths:

1 THE AGENCY IS FORCED TO DEAL WITH YOUR ALLEGATIONS.

An agency may try to ignore threatening whistleblowing disclosures as long as possible, simply not acknowledging their existence and hoping the issue will blow over. When OSC orders an investigation, the agency no longer has that choice.

2 THERE IS OVERSIGHT OF AGENCY INVESTIGATIONS.

Outside of the OSC process, when an agency acknowledges the existence of your concerns, it may respond with a quick report that rewrites or brushes aside hard issues and ignores significant evidence. This allows the agency to declare the issue was investigated and to let itself off the hook. Moreover, your contributions and evidence are often not recognized in the official record.

The OSC disclosure process, which gives you a formal opportunity to provide input on the investigation they spark, makes it harder for an agency to brush your disclosures aside. The law requires the agency to investigate your allegations and detail all material evidence it uncovered during its investigation in its report. The report also must include findings that take a stand on whether misconduct occurred, and what if anything the agency will do about it.[50] Your comments are officially made part of the record in full, and OSC makes an independent determination as to whether the resolution was responsible.[51]

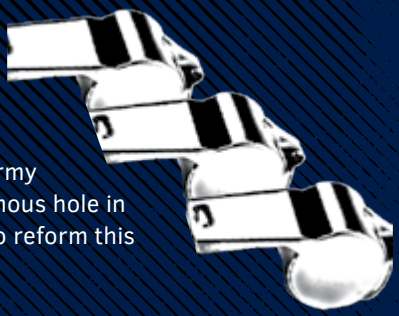
3 THE PROCESS CAN VINDICATE AND PROTECT THE EMPLOYEE.

If OSC makes the finding of "substantial likelihood," it is certifying that your allegations are credible.[52]

An OSC "substantial likelihood" finding provides a hook for the media to tell a story they may have otherwise ignored. Your story becomes less of an editorial risk to publish or broadcast once it has been validated to a certain extent by a government agency. The hook for several national nightly news stories on food safety, environmental threats, and national security breakdowns has been an OSC "substantial likelihood" finding.[53]

Also, it can be easier to successfully claim retaliation if agency management takes adverse employment actions against you in the wake

ONE PERSON CAN MAKE A DIFFERENCE



Dr. Donald Sweeney, a senior economist with the Army Corps of Engineers, single-handedly blew an enormous hole in the Corps' credibility and unleashed a movement to reform this powerful but little-publicized agency.[54]

In a disclosure he filed in 2000 with the Office of Special Counsel, Sweeney revealed a secret plan by Corps officers to manipulate cost-benefit studies in order to justify building a billion-dollar expanded lock system on the Upper Mississippi River.[55] This plan—which would have had far-reaching environmental impacts on one of the nation's most fragile ecosystems—indicated that the Corps' decisions were based on a desire to appease the barge industry.[56]

Sweeney's detailed disclosures, which included internal emails and memos, generated press coverage, Congressional inquiries, and raised questions about oversight and management of the Corps.[57]

Sweeney revealed memos from Corps officers that stated that the Corps would have "to get creative" in order to get funds for the Upper Mississippi project.[58] Another memo advised that if economic data failed to "capture the need for navigation improvements, then we have to find some other way to do it."[59]

The implications of the internal emails and memos Sweeney disclosed went well beyond the Upper Mississippi. The documents revealed an entire Corps planning process driven by a desire to please industry and its friends in Congress.[60]

Public Employees for Environmental Responsibility filed Dr. Sweeney's affidavit with the Office of Special Counsel, which found that his allegations of violations of law and gross waste of public funds had "a substantial likelihood" of validity and ordered then-Secretary of Defense William Cohen to immediately investigate the matter and to report the findings.[61] Investigators confirmed Dr. Sweeney's allegations, finding the Corps had cultivated "an atmosphere where objectivity in its analyses was placed in jeopardy."[62]

of the disclosure referred by OSC. The "substantial likelihood" finding exceeds the "reasonable belief" standard that is generally the threshold to qualify for anti-retaliation protection.[63]

4 **THERE IS A CONFIDENTIALITY OPTION.**

OSC is not allowed to disclose your identity unless you consent or it feels disclosure of identity is necessary due to an imminent danger to the public or an imminent violation of criminal law.[64] If the process protects your identity, it can be a very effective way to shield you from retaliation (but not always).

Limitations:

1 **OSC DOES NOT MEET ITS OWN DEADLINES.**

The small OSC disclosure unit is hopelessly backlogged. That means that scores of agency-employee disclosures languish for months and even years without action.[65] Even when OSC forwards disclosures to the agency, OSC can allow the agency extension after extension so that the 60-day agency response period routinely results in delays of a year or longer. This can make an investigation less likely to succeed: during a delay, agencies can destroy evidence, people's memories can grow fuzzy, and officials responsible for wrongdoing or witnesses to their wrongdoing may leave the government. (OSC and inspectors general cannot compel individuals who are not currently government employees to cooperate.[66])

2 **THE PROCESS HAS NO TEETH.**

While the OSC disclosure process may be an excellent transparency tool to highlight wrongdoing, OSC has no corrective power to force the agency to desist from waste, fraud, or abuse.

3 **CONFIDENTIALITY CAN BE ILLUSORY.**

An agency may figure out your identity even if you requested confidentiality from OSC because the agency will associate you with the issues OSC is requiring that the agency investigate. See Chapter 6 for more information on retaliation protections, how circumstantial evidence

WHO WATCHES THE WATCHERS?

In some cases, federal offices dedicated to upholding government integrity have their own problems, including corrupt or unethical leaders. Whistleblowers are often key to exposing wrongdoing inside these watchdog offices.

Under Scott Bloch's tenure as special counsel from late 2003 through 2008, employees within the Office of Special Counsel (OSC) blew the whistle on his actions, disclosing mass dismissals of whistleblower cases without adequate investigation. Another act that insiders disclosed was that Bloch had created a new field office in Detroit to which he wanted to "ship out" homosexual employees from D.C. Additionally, Bloch "hurriedly" changed the agency's long-standing interpretation of civil service law to exclude protections for LGBT federal employees.[67] In 2005, represented by the law firm Bernabei and Katz, the Project On Government Oversight, Public Employees for Environmental Responsibility, and the Government Accountability Project joined with OSC whistleblowers to file a complaint against Bloch for committing prohibited personnel practices—the very prohibitions Bloch was himself supposed to prevent and investigate.[68] In 2008, the FBI raided the Office of Special Counsel to seize records and find out if Bloch was destroying records relevant to a Congressional investigation.[69] In 2010, Bloch pleaded guilty to withholding information from Congress.[70]

Whistleblowers were also instrumental in putting a spotlight on unethical acts by the top watchdog at the Department of Homeland Security (DHS). They disclosed to the Senate that Charles Edwards, the acting inspector general at DHS from 2011 to 2013, inadequately protected his office's independence, abused his office's resources, sought legal advice from DHS rather than his office's counsel, and altered oversight reports in ways that "did not comport with standard [Office of Inspector General] processes," according to a 2014 Senate investigation.[71] One audit report on acquisition was not published. A "senior official believed it appeared that Mr. Edwards delayed the report out of a concern for his relationship with the Undersecretary for Management, who had recently hired Mr. Edwards' wife," the Senate report stated.[72] A separate government review found that Edwards "failed to disclose his wife's employment…which appeared to impair the independence of a DHS-OIG audit that cost the government $659,943.32 and resulted in the rescission of the audit report." Edwards also had staff work on taxpayer-funded time on his doctoral dissertation.[73] He stepped down from his role at the end of 2013 after his office produced records requested by Senate investigators.[74]

can be used to establish management's awareness that someone is a whistleblower, and how perceived whistleblowers are protected too.

The False Claims Act and Other Bounty Programs

If you have non-public information that a company is defrauding taxpayers in Medicare or a government contract or grant, you may be able to sue under the False Claims Act to recover taxpayer dollars.[75] While the law has been used mostly by insiders working in the private sector whose companies do business with the federal government—such as defense contractors and drug manufacturers—some government employees have also been able to use it after reporting the fraud internally.[76]

If False Claims Act lawsuits are successful, whistleblowers are entitled to a percentage of the funds recovered for the U.S. Treasury, from a ten percent minimum to a 30 percent maximum of the monetary penalties enforced. There are certain requirements that must be met in these lawsuits, also known as *qui tam* actions: the individual filing the suit must be an original source basing the disclosure on non-public information. The lawsuit, the information within it, and the whistleblower's role in filing the suit must also be kept secret until the Justice Department has had a chance to determine if it wants to join the suit.[77] Since that can take years, ironically whistleblowers can be gagging themselves through this option.

There are attorneys who specialize in *qui tam* lawsuits, and due to the technical nature of this area of litigation, we highly recommend that you work with an experienced attorney in this field if you're considering a False Claims Act lawsuit.[78]

The False Claims Act contains anti-retaliation provisions as well, which are discussed briefly in Chapter 6.

There are also bounty programs in some federal agencies. The 2010 Dodd-Frank law, which was modeled partly on the False Claims Act,[79] created bounty programs for those disclosing violations of law that lead to enforcement penalties greater than one million dollars at two agencies responsible for protecting financial markets—the Securities and Exchange Commission (SEC) and the Commodities Future Trading Commission (CFTC).[80]

The main difference from *qui tam* actions is that the former are "private attorney general" actions where the whistleblower, alone or with the

government, must fight and win the battle against fraud. While the Dodd Frank bounty rewards also range from 10 to 30 percent of penalties greater than $1 million, whistleblowers do not have to participate in the trial. They are rewarded merely for giving evidence to the government. Most significant for this guide are the carefully constructed provisions in Dodd-Frank and its implementing regulations for anonymous and confidential disclosures. Whistleblowers can make anonymous disclosures, but they have to do so through counsel if they want to be eligible for an award.[81] If they receive an award, their identity must then be disclosed to the enforcement agency, but the SEC and the CFTC are prohibited by law from publicly revealing the whistleblowers' identities, even at that point.[82]

As with False Claims Act lawsuits, government employees can make disclosures through these bounty programs. Also similar to the False Claims Act, the disclosures must involve company misconduct, not government misconduct.[83]


PRESS RELEASE
For immediate release
"We must not confuse dissent with disloyalty."
EDWARD R. MURROW
BROADCAST JOURNALIST

5
CHAPTER

The Medium is the Message[1]

The media is an effective tool to influence decision-makers. It can bring transparency to government agencies and shape public opinion. Government leaders are both senders and recipients of messages via the media. For these reasons, the media alternately is respected, exploited, and feared by politicians and heads of agencies.

The media can play the role of a leveler. It can bring disputes about misconduct out of the secret world of bureaucrats and into the glare of public attention. Media coverage can show the world that someone the agency is portraying as a workplace "troublemaker" is actually a public hero, or can force the resignation of a corrupt agency head who had previously been untouchable. But media exposure can also cause an agency to change its stance on negotiations with an employee from constructive and open-minded to antagonistic and closed as it finds itself on the defensive in an embarrassing public fight.

While the media can be powerful, the effects of its coverage can be evanescent. The attention span of the public and our leaders can be distressingly short, especially in this era of the 24-hour news cycle where people

consume information immediately through fast-paced social media and online news outlets, but rarely have time to digest everything they consume.

Try not to let the excitement or ego boost from media coverage undercut the point of your publicity—exposing and fixing problems. The news media frequently focuses its stories on individuals, and any stories about you may not stress the issues you are raising. And media attention is often fleeting. The cliché is true: today's headlines are tomorrow's fish wrap. New distractions compete daily for media attention, and the news media is a competitive business, driven by financial as well as informational dynamics, so you want to make the most of its attention while you have it.

If It Bleeds, It Leads

The saying "if it bleeds, it leads" reflects the value that the news industry places on gore. By contrast, stories about government bureaucracies or complex scientific or technical issues rarely elicit the same widespread media interest or keep viewers' attention. And telling those stories in a compelling and succinct way can be challenging, particularly on television. As a consequence, coverage of complex or "wonky" issues is usually confined to less-sensational print or online media. Only occasionally do internal agency stories cross over from specialized publications or websites into mainstream news coverage.

Media attention is often fleeting. The cliché is true: today's headlines are tomorrow's fish wrap.

This means that the interest in any story about an internal agency scandal may be limited to a handful of journalists. In order to identify that limited pool and work with them effectively to educate their readers, consider the following tips:

- **Decide beforehand what your role will be.** Professional journalists need to feel confident that their sources are solid and that the documents they provide are real. Do not contact a reporter until you have made up your mind about whether you want to be quoted in the story or to be an unnamed source. It is vital that you know which ground rules you want to govern the interaction. Be prepared to explain why you want to be anonymous if you do, and consider whether there may

be other people you can recommend the reporter talk to in order to substantiate your concerns, on or off the record.

- **Think about whether to let even the reporter know your identity.** Reporters usually know who their "anonymous" sources are. This information can help them assess a source's credibility—an extremely important consideration if the whistleblower's information could lead to a high-profile, hard-hitting story that an agency may aggressively push back on.

- **Know the outlet.** Try to figure out whether national or local outlets are the best fit for what you are trying to accomplish. The newspaper or other outlet may have business ties (such as substantial advertising buys or sponsored events) to the entity whose misconduct you are trying to expose. Research what kind of coverage, if any, your issue has garnered in the past. Look at the outlet's relevant editorials on the issue. Look at whether that outlet has done investigative work in the past, and whether it carries critical stories that challenge agency statements.

- **Know the reporter.** Read several articles by the reporter written over time about this or a related issue and look at their social media profiles to see what interests or biases they may have. Compare the reporter's work on a story with that of the competition. See whether your concerns are similar to issues that the reporter has highlighted, and whether that reporter does follow-up work. Consider the writer's tone—it can be very telling. While the facts may all appear in the story, the tone can lead the reader toward one side of the story or the other.

- **Get familiar with the reporter's ground rules.** Reporters generally accept information on three levels: off the record, on background, and on the record. Unless you negotiate a different condition in advance, a reporter will assume everything you tell them is on the record and they can use it however they want. It is too late if you wait until after an interview or other interaction with the reporter to set the ground rules. If you try to place restrictions after sharing the information, the reporter may cooperate as a favor but they are not bound to do so.

Make sure you both share an understanding of what each of the levels means and entails before you share sensitive information. Asserting something is on background or off the record in an email, without the journalist agreeing to those terms, may not be sufficient. We provide the general definitions for "off the record" and "background" below. But it's always a good idea to verify those definitions with the specific reporter you might work with before you expose your identity or your evidence, since journalists don't consistently agree on the definitions.[2]

Unless you negotiate a different condition in advance, a reporter will assume everything you tell them is on the record and they can use it however they want.

The definitions below largely reflect how they are interpreted by the Associated Press.[3]

"Off the record" means that your name cannot be used, and you cannot be quoted. It also means that journalists cannot publish the information you provide (unless a different source independently provides the information to them). This information can help a journalist climb the learning curve, but it cannot be exposed or referenced in reporting. You should go off the record if the information you tell the reporter—regardless of whether your name or general information about your position was mentioned—would likely identify you as the source if the information were it to be published or relayed to your agency. You should let the reporter know up front whether and how, if they use the information you give them to ask questions to other sources, they could inadvertently tip off an agency that a whistleblower is talking to the reporter.

"On background" ("not for attribution" is similar) means that your name cannot be used, but that the information you provide can be published under terms that you negotiate with the reporter. This should be for information that is an essential part of the story and could be provided by people other than you (so you won't be identified as the source) but you think should not be attributed to you by name. This is typically seen in news stories attributing information to "senior administration officials." On background can mean many things and it is especially important to have a conversation with the reporter about

what you're comfortable with. Are you okay if the information is sourced vaguely to you but not by name (such as "an employee in the agency who does not want to be named out of fear of retaliation")? Would you rather a reporter simply use the information to get official confirmation or confirmation from other insider sources? Most serious news organizations will not base reporting on a sole anonymous source.

"On the record" means whatever you say can be quoted and attributed to you by name.

Pin down confidentiality before sharing any information. Depending on the nature of the information you provide, the issue in question, and a reporter's ability to get information out of an agency through official channels, you and the reporter may have multiple conversations about how your information can be used.

If you choose to remain anonymous, you may want to start out with an "off the record" interview and later ease into an "on background" interview as you grow more comfortable with a journalist. But wherever you start, you should be cautious when interacting with the media and be clear in each conversation on what basis you're providing information. It can be easy to assume all conversations are covered by a previous agreement, especially if you talk to the reporter repeatedly.

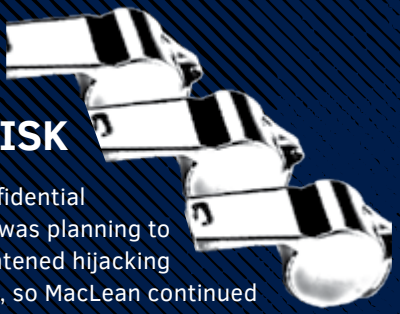
When whistleblowers are casual about the ground rules, too often their identity gets involuntarily "outed." Reporters have quoted whistleblowers who thought they were speaking off the record or on background but who had failed to pin it down. Such mishaps occur, and once that media bell is rung, it cannot be un-rung.

Even if you are clear about the ground rules, you are always taking a risk that your identity will be compromised when you go directly to the press. In rare cases, an overzealous or sloppy journalist mistakenly has named an off-the-record source. More frequently, the identity of the whistleblower becomes known through a revealing description of the unnamed source.

Talking to a reporter about how to protect your confidentiality can also help them avoid inadvertent mistakes when trying to verify documents.

Have the story prepared. Start by visualizing the headline and lead paragraph of the news story you would like the reporter to write,

A REPORTING MISTAKE CAN PUT YOUR CAREER AT RISK



In 2003, federal air marshal Robert MacLean's confidential disclosure to MSNBC showed that the government was planning to reduce security on airlines during a period of heightened hijacking threats.[4] These policies put the flying public at risk, so MacLean continued to make disclosures about those policies. When he went on *NBC Nightly News* in 2004, the television program shielded his face but failed to camouflage his voice. The agency discovered his identity and also asked if he made the 2003 disclosure. He admitted to it and his agency fired him in 2006, charging him with releasing "Sensitive Security Information."[5]

After a years-long legal battle, throughout which he was represented by the Government Accountability Project and supported by the Project On Government Oversight, his case ended up at the Supreme Court, where he prevailed in 2015. The Court ruled that the Whistleblower Protection Act does not exclude disclosures made to the press or public unless the information is classified or otherwise prohibited by statute from public release. The information MacLean disclosed to the press was neither classified nor protected from disclosure by statute.[6] While he was reinstated in his agency, as of this book's publication, his employment struggles with management continue. His agency has ordered him to take psychiatric examinations, delayed processing his security clearance for over a year, placed him under criminal investigations, and proposed to terminate him—which all began because *NBC* concealed his name and his face, but not his voice.[7]

The lesson here is that in order to truly conceal your identity you must think through the myriad ways an agency can figure out who you are and make sure the organization you are working with is as detail-oriented in protecting your identity as they need to be. A simple mistake can lead to huge consequences.

By establishing ground rules with a journalist, you can help reduce the risk of them unintentionally compromising your identity. For example, a court document suggests that a reporter unintentionally blew the cover of National Security Agency whistleblower Reality Winner in 2017, at least in part because the reporter shared a classified original document he received from Winner with the government in an attempt to verify it. Though Winner had anonymously mailed the classified NSA report on Russian attacks to *The Intercept*, an online news outlet, the government was able to identify that she was one of six individuals who had printed the report.[8]

The reporter should have known the risks of sharing the document, but sources are often in the best position to communicate sensitivities the media might miss or overlook. Other government or contractor employees with security clearances who could verify the accuracy of information may feel obligated to report a potential breach of national security. As *The Washington Post's* media critic Erik Wemple wrote, "It's apparent that the document came straight out of the blue, with little or no instructions as to sensitivity and handling."[9] Such instructions, perhaps, could have helped Winner avoid jail time.

including why the information you are providing matters to a broader audience. Start with your bottom line. Write a short, to-the-point summary and back it up with definitive documentation. Respect that the reporter has limited time, so make the research as easy as possible.

The key to publicizing problems within an agency is to make the story interesting and clear, so present reporters with a compelling description of the problems and their ramifications for the media audience. That means emphasizing consequences in language that will create an image for readers. Adjectives like "horrible" and "tragic" are not news. But it is news if a town could become rubble or a crater. Remember to keep the emphasis on the story, not on yourself.

- **Set a deadline.** Try not to leave the timing completely up to the reporter; if you do, you may find yourself frustrated. Some television networks will keep a completed story "in the can" until "sweeps" week, when they can use it to get the best ratings. By then, however, the abuse of power may be a *fait accompli.* If the information is time-sensitive (for instance, you are trying to prevent a likely accident or tragedy, or affect an upcoming agency action or decision), you should make that clear to the reporter in your first interaction. Try to get a commitment, or find someone else whose schedule will make the story relevant as more than a history lesson. If there is a pending action, that usually helps a reporter prioritize your story and make the case to their editor about the news value of your disclosures. Most reporters have no shortage of items competing for their attention.

You may have access to trustworthy journalists and choose to contact them on your own, but it is usually much easier and more effective to partner with an advocate who can make those contacts on your behalf. Advocacy groups have experience working with the press and often keep tabs on journalists who cover specific topics or "beats." These groups can also help package your information and put your story into a larger policy context than you may be able to do on your own.

Not every internal agency dispute or problem will merit media coverage.

Keep in mind that following these steps does not guarantee a news story.

Not every internal agency dispute or problem will merit media coverage. Moreover, even if the issue is covered, you may not like the result.

Reporters Are Not Your Friends

The best reporters add value and context to information that whistleblowers provide to them. They can also bring information to the attention of senior leaders more effectively than more-junior public servants. In some instances, by refusing to take no for an answer (or a non-answer for an answer), a reporter can take a story far deeper and have much greater impact than you ever thought possible. They can also be invaluable resources for sharing or trading evidence, and referring other whistleblowers to you or your advocacy-organization partners.

That said, the reporter is not your friend, advocate, or supporter.[10] It is not the reporter's job to find you a lawyer, to get your job back, or even to right a wrong. The reporter is just supposed to report the news accurately and fairly. Part of that process is likely to include challenging or fact-checking your allegations.

Reporters working for news organizations are not free agents. They work in a business with a chain of command and idiosyncrasies, perhaps just like your agency.

Consequently:

- **An editor may veto or cut a story.** A reporter who tells you they are committed to writing a story cannot actually guarantee when it will be printed, that it will be printed in its entirety, or that it will be printed at all. Often, a reporter's editor will cut parts of a story, even if the reporter thinks it contains key facts or analysis. Further, reporters usually do not write the headlines; a hard-hitting story may be introduced with a painfully boring—or worse, inaccurate—headline.

- **The agency may get equal time.** In almost all cases, reporters and their editor will want to include the agency reaction or explanation as part of any story. The result may come out appearing as a "he said/she said" standoff, leaving it to the reader to guess who is right. (This is where your familiarity with the tone of the outlet is particularly valuable.)

- **The agency may be able to preempt your story.** As the government, the agency has the advantage of being able to, on occasion, make news through an announcement or other action. Astute agencies have been known to release an announcement or other breaking news out the front door of their public affairs office to distract from the bad news coming out the back door from employees.

Yesterday's News

Rarely is media coverage an end unto itself. Rather, it is just one component of a larger effort.

Sometimes the moment of greatest leverage with an agency is just before a news story runs because the agency may be willing to take steps it would otherwise not take in order to avoid or mitigate the media exposure. Conversely, the day after the story runs, the agency may be set in a defensive posture, unwilling to take any steps that imply an admission of guilt.

If your goal is to correct a problem, you should have a strategy for how to accomplish that and precisely what role media coverage will play. In other words, it is important to think of the process in terms of a campaign. This is another reason why it can be to your advantage to partner with advocacy groups that can help ensure your story reaches the audiences necessary to effect change. Very few problems within agencies evaporate simply because they have been the subject of one article in a newspaper. Most agencies can shrug off one story, or even one week's worth of stories. It may take sustained media exposure to effect change.

Very few problems within agencies evaporate simply because they have been the subject of one article in a newspaper.

If sustained coverage is necessary, you must plan for an entire campaign and not just the first step or a single story. It can be very difficult to garner sustained media attention. Reporters may think your concerns merit only one or a handful of stories based on the information you give them. In this scenario, you need a strategy to keep up the pressure. That may include working with advocacy groups or a Member of Congress to spark an official investigation or audit of an agency, or to question the agency during a hearing. These actions may help you make your case that an agency needs to

rectify the issue, especially since agencies can often waive off news reports alone as biased and slanted. But it's harder for an agency to ignore, for instance, an inspector general's report that confirms news reporting.

The key to earning public solidarity is sustained exposure of steadily accumulating evidence. That means pacing your releases of evidence. If you use everything at once, you're likely to get one story that's a blip. Your goal is to expose the story that won't go away, generating progressively less credible denials and cover-ups.

In order to generate a series of stories in any scenario, you must assemble a lot of raw material and then refine it down to individual stories. Once you assemble an arsenal of "ammunition," you should release pieces of it separately so that each salvo reinforces the effects of the one before it. If you can pace the intervals between "hits," you can give the agency ample opportunity to do something counterproductive, such as putting forth a demonstrably untrue fact in its defense, instituting a "gag" order forbidding employee contact with the media, or otherwise overreacting in a way that may be newsworthy as well. Similarly, you can intersperse releases of new evidence with other developments such as letters or expressions of support from political leaders, which can be their own complementary news hooks.

It may be that a single journalist will be interested in every piece of ammunition, but if that single journalist loses steam, approaching other outlets can increase pressure on an agency. That said, recognize that journalism is a very competitive field and a reporter may feel burned if they feel like the source is playing them against their competitors. Some journalists also won't be interested in covering what they view as the "scraps" that their competitors didn't pursue, or will simply feel like the story has already been sufficiently covered and doesn't merit their time.

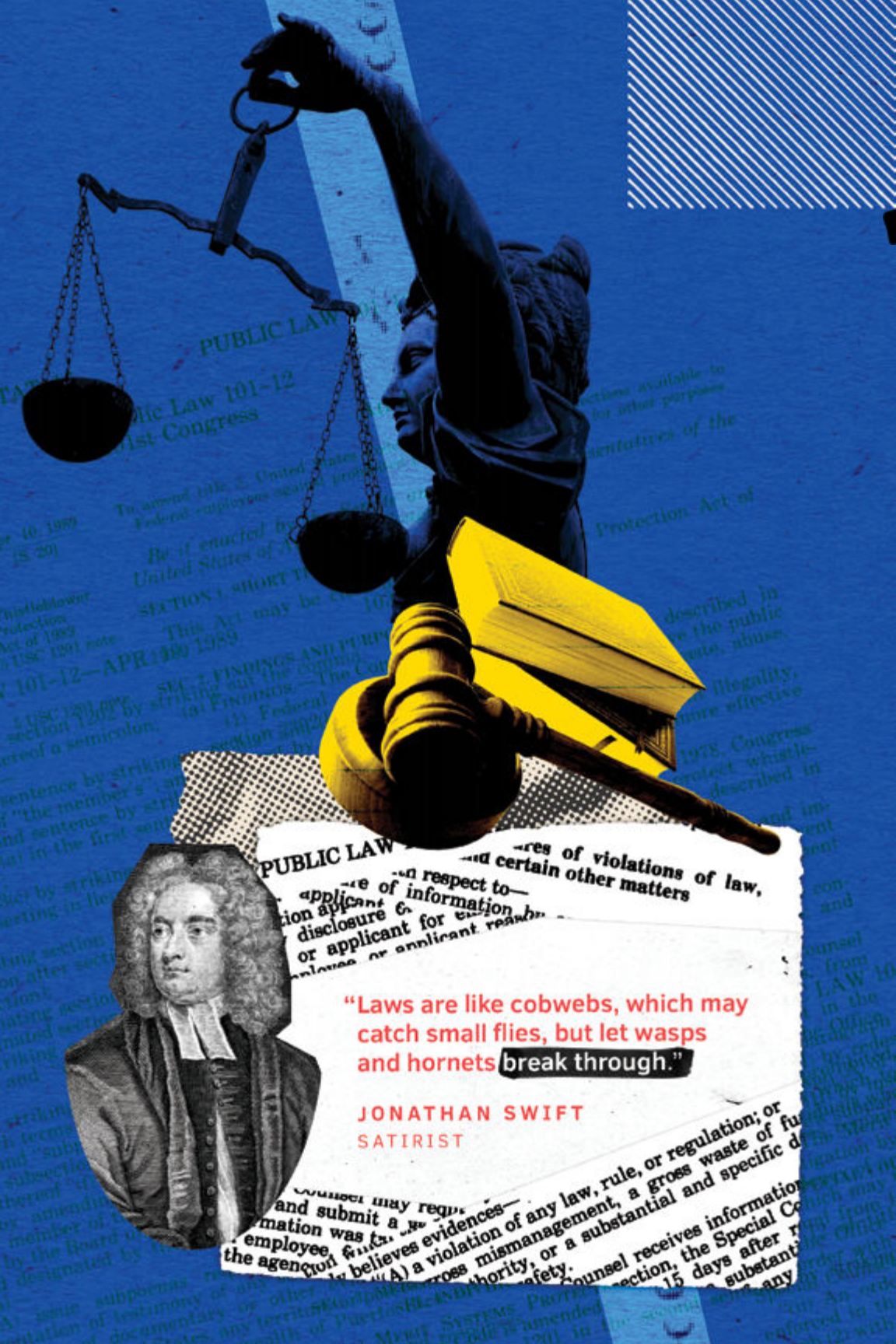
If your goal is to correct a problem, you should have a strategy for how to accomplish that and precisely what role media coverage will play.

If you conduct your campaign successfully, the deepest wounds to the agency will be self-inflicted. If the wrongdoing involves the leadership of an agency, including leadership's failure to meaningfully address problems, after a few weeks or months of unrelenting bad news, media accounts may start to refer to the agency head as "embattled" or "beleaguered." At that point, support for the agency

may erode as political patrons shrink away from the prospect of guilt by association.

Sustained media attention also tends to spawn official investigations (see Chapter 4) that put even more pressure on agency leadership. Each investigation not only becomes a new, separate story, but each may provide a new forum to air allegations and be a magnet for new witnesses who are starting to hope that something can be done. Each new story will recount the previous developments, like an arrest rap sheet, so that the allegations continue to build toward a climax.

Media attention can also backfire. If you are still working inside an agency and are thinking about working with the press, extreme caution is in order. The agency leadership will correctly see its professional survival at stake and critical coverage can get deeply under their skin. Breaking ranks to go public often is viewed as an act of unforgivable betrayal. Even if you were initially able to raise your concerns anonymously, you may eventually be revealed by the new spotlight you've created.


PUBLIC LAW
certain other matters
"Laws are like cobwebs, which may catch small flies, but let wasps and hornets break through."
JONATHAN SWIFT
SATIRIST

CHAPTER 6

Whistleblower Laws

LEGAL DISCLAIMER

The material in this guide is provided for informational purposes only. Nothing in this publication should be construed as legal advice. Nor is this chapter intended as a comprehensive review of your rights. It is an introduction to legal protections that may be relevant for you.

Before acting on any of the material in this guide, the authors STRONGLY urge you to seek legal counsel.

When you experience, witness, or hear about a practice at work that you believe violates the public trust, you may feel a sort of fight or flight response: Do I tell someone with power about this in the hope of changing it, or do I look the other way?

In today's "see something, say something" world, the hope of society is that you speak up—but repeated federal surveys have shown that one of the main reasons federal employees say they might not blow the whistle is fear of retaliation.[1] Up until this point, this guide has laid out options for getting the truth out while keeping your role as a whistleblower secret from your

management in order to avoid the potentially devastating professional consequences you could face. But what if such anonymity is impossible because your disclosures are easily tied to you or your identity is exposed some other way? What kind of protections exist if you face retaliation? And what does a retaliation investigation look for? This chapter is an introductory menu for answers to these questions.

First the good news: In the almost 20 years since the last edition of this book, Congress and the executive branch have strengthened whistleblower rights and protections for federal employees and contractors, as well as for corporate workers. In 2012, Congress closed loopholes in the Whistleblower Protection Act that had left many federal civilian whistleblowers unprotected if they disclosed concerns to supervisors in the course of carrying out their job duties or if they weren't the first person to make the disclosure, among countless other judicially created loopholes. Employees of government contractors, intelligence agencies, and the FBI, and uniformed members of the military have all seen improvements in their legal protections, and there has been a legal revolution in corporate free-speech rights.

But, despite these and other major victories advancing whistleblower protections, there are still critical flaws in existing laws. In addition, barriers like bureaucratic red tape, partisan squabbles in Congress, resource limitations, and timid officials who are unwilling to make waves can and do hold up access to justice, sometimes well within their discretionary authority under the law.

And the sobering truth is that even where the strongest possible protections exist, there will always be people who violate them and get away with it. Whistleblowers themselves regularly become the subject of retaliatory actions or criminal investigations, even though most of them were merely trying to right a wrong.

This chapter focuses mainly on the laws that protect most career federal civil-service employees working in the executive branch. These are employees who are protected under the Whistleblower Protection Act (WPA), as amended.[2]

The chapter will also outline protections for federal contractors, intelligence community employees and contractors, FBI employees, and members of the armed services. All have distinct protections and processes for blowing the whistle separate from the WPA.

Note that some federal employees lack whistleblower protections entirely and so aren't discussed in this chapter. They include political appointees and employees in the legislative and judicial branches of government. They also

include executive branch employees still in their probationary period, who have curtailed employment appeal rights under the WPA.[3]

If you are a covered employee and file a retaliation complaint, an investigation into your complaint will focus on four key questions regardless of whether you are a federal civilian, FBI or intelligence community, or contractor employee, or a uniformed member of the armed services. Those five key questions are:

- Did you make a disclosure protected under any law or regulation?
- Did you face an adverse employment action?
- Did the managers who took the action or played a part in it know about your protected disclosure, and if so, was there a connection between your disclosure and the subsequent personnel action you wish to challenge?
- Did your management have a legitimate, non-whistleblowing reason to take that action?

This chapter will walk you through what the answers to these questions must be in order to win a retaliation claim. It will also discuss how the different laws and regulations covering other types of federal-sector employees affect these questions. For instance, to defend itself against a retaliation claim, the military can produce weaker evidence to show it had a legitimate, non-whistleblowing reason to discipline a uniformed military whistleblower than civilian or intelligence agencies, the FBI, or contractors have to show to defend themselves.

The scope of what qualifies as a protected disclosure varies to some degree, too: for example, unclassified disclosures by most civilian federal employees to the press can receive protection, whereas unclassified disclosures by FBI and intelligence employees or uniformed members of the armed forces to the press do not. Nobody is protected for disclosing classified information to the press or public, period.

When deciding whether to blow the whistle, your best bet is to remain realistic in your expectations, know your rights, and speak with a knowledgeable whistleblower-law attorney before pressing forward. Your situation will likely have many nuances. And the law is not always as straightforward as it sometimes seems. For instance, case law—binding decisions by judges—makes legal analysis even more complex. This guide is just a starting point.

FEDERAL CIVILIANS

What's a Protected Disclosure?

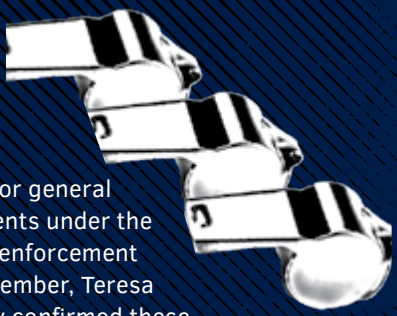
Many employees communicate concerns without thinking of their communications as whistleblowing or of themselves as whistleblowers. So it's important for every employee to understand what types of communications are protected by law.

Under the Whistleblower Protection Act, a protected disclosure is a formal or informal communication or transmission of information that a covered employee, former employee, or applicant reasonably believes evidences:

- A violation of a law, rule, or regulation
- Gross mismanagement
- A gross waste of funds
- Abuse of authority
- A substantial and specific danger to public health or safety[4]

When making a disclosure, you must have a "reasonable belief" that the information is evidence to demonstrate one of these prohibited activities. This means that you must have believed that the information evidenced a prohibited activity, and your belief must be objectively reasonable, meaning it would be reasonable for someone in your position to draw the same conclusion that you did.[5]

There are, however, explicit exceptions. If your disclosure includes classified information, you are protected by the law *only* if you disclose that information to a relevant Office of Inspector General, the Office of Special Counsel (OSC), or other authorized channel that can legally receive classified material (the role of inspectors general and OSC in accepting disclosures is discussed in Chapter 4). There are no protections for disclosing classified information to the press, the public, or to any other parties not listed in the channels for making a protected disclosure. Such disclosures are grounds for discipline up to and including termination, and possibly for criminal prosecution. The same goes for other information that statutory law restricts from public dissemination, such as private medical information and confidential tax and financial records. You will not receive protection if you disclose that information to the public or the press.[6]



THE LONG ROAD TO JUSTICE

In August 2003, the Interior Department's inspector general warned of inadequate security at national monuments under the jurisdiction of the United States Park Police, a law enforcement agency within the National Park Service.[7] That December, Teresa Chambers, then-chief of the Park Police, seemingly confirmed these findings, when she said in an interview published in *The Washington Post* that her agency was stretched thin and underfunded.[8] Within days, the National Park Service made Chambers surrender her badge, forbade her from speaking to the media, and placed her on administrative leave. According to Chambers, her comments to the *Post* upset Interior Department political leaders. Those political leaders threatened her with discipline unless she agreed to speak at a press conference and rescind her statements to the *Post*.[9]

"After reflection, I concluded that these conditions required me to lie and prevented me from doing the job I was hired to do. I refused to agree to what was, essentially, an effort to blackmail me into misleading Congress and the public," she later testified to Congress.[10]

Following her refusal, the Department accused her of giving "law enforcement sensitive information" to the press and of several other trumped-up charges, such as not quickly returning a phone call from a Department attorney.[11]

Chambers appealed the charges by filing a complaint with the Office of Special Counsel (OSC), and ended up taking her case to the Merit Systems Protection Board (MSPB) after the OSC failed to act for five months. During the review of her case, an MSPB administrative judge warned her against pressing for a formal hearing of the case. The administrative judge said Chambers would "embarrass" herself and that she should resign, Chambers recalled in her testimony before Congress. Chambers persisted in seeking the hearing. During the hearing, Chambers said the judge "seemed in a hurry, limiting the number of witnesses who could be questioned and refusing to order the Department of the Interior to produce requested and relevant documents."[12] In an October 2004 decision, the judge upheld four of the Department's charges against Chambers and her termination partly because she "expressed no remorse."[13]

Chambers appealed to the full MSPB, which ruled against her in 2006, finding "this case presents a classic policy disagreement over which reasonable minds might differ, and that as a result, the appellant's interview with the reporter was not protected whistleblowing."[14] Chambers, represented by Public Employees for Environmental Responsibility (PEER), appealed to the Federal Circuit Court of Appeals, which ruled in her favor in 2010 finding that the Board made legal mistakes.[15] Her case went back to the MSPB again. In 2011, with a new set of judges because so much time had passed, MSPB found she was retaliated against, and she was reinstated.[16]

In total, Chambers' fight lasted over seven years.

"Without their help," she said of PEER in an interview with *The Washington Post* in 2013, "I'm sure I would have had to give up the battle long ago."[17]

Likewise, you generally will not receive protections for disclosing your disagreement with an agency policy decision unless you have a reasonable belief that the policy's consequences are among the protected categories of disclosures (such as a violation of law, or a substantial and specific danger to public health or safety).[18]

In addition to the protected disclosures mentioned above, the law also protects employees who take certain actions from employer retaliation.[19] The law makes it unlawful to retaliate against a covered employee for:

- Exercising any appeal, complaint, or grievance right granted by law, rule, or regulation, or testifying on behalf of or helping someone who is exercising one of those rights
- Cooperating with or disclosing information to an Inspector General or the Office of Special Counsel
- Refusing to obey an order that would require the employee to violate a law, rule, or regulation

For example, these rights protect against retaliation resulting from a covered employee filing discrimination complaints with the Equal Employment Opportunity Commission (EEOC). Note that OSC typically refers these retaliation complaints to the EEOC to investigate, but the act of filing a disclosure is protected as a complaint right.[20]

For example, these rights protect against retaliation resulting from a covered employee filing discrimination complaints with the Equal Employment Opportunity Commission (EEOC). Note that OSC typically refers these retaliation complaints to the EEOC to investigate, but the act of filing a disclosure is protected as a complaint right.[21]

Choosing Your Audience

After you and your attorney, if you have one, determine that your disclosure falls into one of the protected categories, your next decision is to choose the recipient of your disclosure. Most federal civilian employees protected under the WPA have a wide array of people and offices they can make protected disclosures to.

For instance, you can choose to make disclosures internally to a supervisor or to someone else in your agency. However, the law does not require

CHANGES MADE BY THE WHISTLEBLOWER PROTECTION ENHANCEMENT ACT

The Whistleblower Protection Enhancement Act of 2012 helped to finally close major loopholes that plagued federal whistleblowers for decades. As a result, the law now protects whistleblowers:

- For disclosures made internally to a supervisor
- For disclosures that were already made by someone else
- For disclosures regardless of the motive of the whistleblower
- For disclosures not made in writing
- For disclosures made off duty
- For disclosures made before the whistleblower applied to their position or was appointed
- Regardless of how much time has passed between the disclosure and the retaliation

that you do this,[22] and internal disclosures are not always safe or effective. After all, your supervisors could very well be the subject of your disclosure or become messengers to warn the wrongdoer.

You can also choose to make your disclosure externally to an Inspector General, the Office of Special Counsel, Congress, advocacy groups, or the press. As noted above, if your disclosure involves classified information or other information prohibited by statute from public dissemination, you are not protected for those disclosures made to the press, the public, or anyone else not legally authorized to receive that material.

Most other types of federal workers who are excluded from the WPA—such as those in the intelligence community, the military, and the FBI—do not have the same array of outlets they can disclose to and still receive protection.[23]

For more on filing an initial disclosure, see Chapter 4, which details the main official oversight bodies you can bring your disclosure to: Offices of Inspectors General, the Office of Special Counsel, and Congress. Chapter 2

discusses non-governmental organizations as potential recipients for disclosures, and Chapter 5 discusses working with the press.

FEDERAL CIVILIANS

What's a Personnel Action?

The Whistleblower Protection Act, as amended, makes it illegal for anyone with authority to take, direct others to take, threaten to take, recommend, or approve any "personnel action" relating to a covered employee in retaliation for blowing the whistle. This doesn't just mean terminations or poor performance evaluations—it also includes actions *not* taken, such as promotions or appointments that weren't granted.

A personnel action means a decision by someone with authority related to:

- An appointment
- A promotion
- Disciplinary or corrective action, also known as adverse action
- A detail, transfer, or reassignment
- A reinstatement
- A restoration
- A reemployment
- A performance evaluation
- A decision concerning pay, benefits, or awards, or concerning education or training if the education or training may reasonably be expected to lead to an appointment, promotion, performance evaluation, or other action
- A decision to order psychiatric testing or examination
- The implementation or enforcement of any nondisclosure policy, form, or agreement
- Any other significant change in duties, responsibilities, or working conditions[24]

While this is a fairly comprehensive list of employment-related actions, it's important to note what the list doesn't include.

An unfortunate reality is that whistleblowers often become subjects of retaliatory civil and criminal investigations.[25] It's an awful tactic that diverts attention away from the whistleblower's disclosure by refocusing attention on the whistleblower. After opening such an investigation, the agency then offers the whistleblower a choice of facing criminal prosecution, or resigning and dropping the retaliation claim. Many agencies are getting away with this, because opening a retaliatory investigation isn't a prohibited personnel practice under the Whistleblower Protection Act. The employee is powerless until the investigation leads to a subsequent personnel action.[26] But criminal referrals for prosecutions are not listed personnel actions, either, so the employee is left defenseless against retaliatory prosecutions.[27] Going to jail is far worse retaliation than getting fired. The Office of Special Counsel can informally ask an agency to cease a retaliatory investigation as a part of OSC's larger investigation into the retaliation but unfortunately has very limited resources and can only investigate a few of these cases at a time.[28]

If you have an attorney, speak with them before blowing the whistle. Be candid—it's important for them to be able to weigh any potential fuel that your employer may try to use against you and for you to understand the kinds of claims agencies make in an attempt to discredit whistleblowers.

FEDERAL CIVILIANS

What's Management Knowledge and How Is It Proven?

After considering whether you made a protected disclosure and faced a retaliatory action under the law, investigators will look at management knowledge of your disclosure. In order for agency officials to have taken retaliatory action against you, they first must have known about your disclosure—otherwise the action wouldn't have been retaliatory. Note that it is not necessary that the proposing or deciding official on the personnel action have knowledge if some management official who influenced the decision had such knowledge.

To determine managers' knowledge of your disclosure, investigators can look at direct and circumstantial evidence. Direct evidence can be things like emails, confessions, testimony or documents that tie the personnel action taken against you to your disclosure. While this evidence is obviously

preferred, it's not always easy to come by unless agency officials are careless.

Circumstantial evidence can also be used either instead of or in addition to direct evidence to prove that management knew about your disclosure and retaliated. Circumstantial evidence looks at the circumstances around your disclosure and the personnel action, such as coincidental timing (you made a disclosure on Friday and were fired on Monday) or disparate treatment where all of your co-workers get some work-related reward except you, to draw logical conclusions connecting the two.

Also note that the adverse personnel action doesn't have to stem from actual knowledge of your disclosure, but can be the result of what management should have known or of "constructive knowledge," where the retaliating manager was influenced by someone else with actual knowledge.[29] This prevents a manager from developing plausible deniability by deliberately avoiding the truth. Further, "mistaken knowledge" triggers your rights. Even if you haven't made a disclosure, if agency officials retaliate against you based on a mere belief that you made or intended to make a protected disclosure, that would be unlawful retaliation under the WPA.[30]

FEDERAL CIVILIANS

When Can an Agency Claim that the Personnel Action was Legitimate?

In retaliation cases, the burden of proof is on you to demonstrate that you made a protected disclosure, faced an adverse employment action, and that there is evidence the action was taken when management knew, should have known, or suspected you blew the whistle. To meet that burden, you must satisfy the "preponderance of the evidence" standard, meaning there is more than a 50 percent likelihood that your claim is true, which is a fairly low bar. If you meet that burden, the agency is then put on the defensive. Did it have a legitimate, non-whistleblowing-related reason to take action against you?

In order to prevail, the agency must demonstrate that they had a legitimate reason to take the action, and must satisfy the "clear and convincing" standard—one of the highest burdens in civil law—to overcome the presumption that it retaliated. Basically, the agency has to show that it would have taken the same personnel action even if there had not been

whistleblowing. Agencies can do this by showing that their treatment of you was the same as that of other employees, that they had no motive to retaliate, that their action was put in motion before the whistleblowing, that your purported poor performance or misconduct was real, or similar valid justifications.

For this reason, you should always remember that you need to be cautious about maintaining quality performance at work. Even if you are being retaliated against, you should always try to perform your job to the best of your ability and with professionalism. Whistleblowers who face retaliation at work and a newly and unreasonably difficult work environment may feel tempted to start using all of their sick leave or otherwise refuse to perform their job function. But underperforming would only provide ammunition to employers who will be looking for anything legitimate to use against you to defend against your claim of retaliation. While it may be frustrating, you should strive to still provide your best work and be as professional as possible.

Don't Misuse Government Resources, Facilities, or Time

Agencies have explicit rules limiting unofficial or personal use of government resources, facilities, and time. So, at all costs, avoid using agency resources including equipment, materials, or facilities for your disclosure, and don't work on your disclosure or gather information while at work or otherwise on the government's time. A whistleblower caught with private correspondence to a civil society group or faxing or emailing documents to a reporter will often be disciplined for misuse of the equipment or misappropriation of government resources.

You should assume that any information on your work computer(s) or devices is open to management review. This includes work and personal email, documents saved, programs accessed or downloaded, and messages sent.

You should also forgo whistleblowing telephone conversations conducted over workplace telephone lines or on government-issued cellphones. That can not only lead to termination, but some agencies (such as certain law enforcement agencies) have regulations that allow them to monitor conversations or record all telephone calls. Furthermore, most government agencies keep a computer log of all incoming and outgoing telephone numbers dialed to or from agency telephones. These logs are frequently reviewed to find out who employees are talking with.

Similarly, agency fax machines, copiers, and scanners keep logs of all sent and received documents and may have the capacity to keep electronic copies of documents. These logs may be used to prove that an employee improperly used government equipment.

Finally, avoid using government facilities for personal purposes. For example, don't mail corroborating documents to the press from your agency's mailroom or fax machine.

FEDERAL CIVILIANS

Where Can You File Whistleblower Retaliation Claims?

Above, we've outlined the legal requirements to win a claim that your whistleblower rights were violated. But who do you file your claim with?

If you are a federal civilian employee seeking relief from the retaliation you've suffered for blowing the whistle, there are three offices you should become familiar with: the Office of Special Counsel (OSC), the Merit Systems Protection Board (MSPB), and your agency's Office of Inspector General (IG). (The roles of IGs and OSC in receiving whistleblower disclosures are discussed at length in Chapter 4. This chapter focuses on their roles in investigating retaliation claims.) Remember that if you are an intelligence community employee, you have unique protections that will be described in detail later in this chapter.

The Office of Special Counsel is specifically authorized by Congress to, among other things, investigate claims of retaliation.[31] All federal civilian employees who have whistleblower protections can file claims of retaliation directly with OSC. If OSC believes there is sufficient evidence showing retaliation, it can negotiate with your agency to make you "whole" or propose other corrective actions. While OSC itself can't compel agencies to take remedial action, it can go to the Merit Systems Protection Board, an administrative court that hears executive-branch employment disputes, to seek enforcement of OSC's corrective action recommendations. MSPB is essentially OSC's court. OSC can also seek to temporarily block an agency's negative action through negotiation or by asking MSPB to order a "stay," blocking the retaliation while the case in pending, if the agency doesn't voluntarily comply with OSC's request. It often obtains "informal" stays from agencies

while investigating the reprisal complaint. If resolution is not possible, OSC either takes the case before the MSPB or dismisses the claim, which then gives the employee the right to file directly with the MSPB on their own.

Federal civilian employees can file whistleblower retaliation claims directly with the MSPB only if they involve unpaid suspensions of more than 14 days, terminations, or other serious employment actions. For other actions, as well as action by probationary employees who cannot otherwise bring a case to MSPB, federal civilian employees must go to OSC first. If OSC closes their case, or 120 days pass after the claim was filed with OSC without hearing about a corrective action, an employee can then proceed to MSPB. Individuals bringing their own case to the MSPB are exercising an "Individual Right of Action" (IRA). Note that employees can only raise issues in their MSPB that they've already raised with OSC.

There are three offices you should become familiar with: the Office of the Special Counsel, the Merit Systems Protection Board, and your agency's Office of Inspector General.

Offices of Inspectors General are internal federal agency watchdogs. Under the WPA, IGs can receive claims of whistleblower retaliation, and the Inspector General Act, as amended, dictates IG staff training and the creation of best practices for whistleblower intake and investigations.[32] Each IG office must have a whistleblower coordinator who makes sure that the office is trained in whistleblower law, and to assist the IG with investigations. [33] IG's also have a general counsel that can, among other things, advise the IG on whistleblower law. IGs are limited to investigating and making recommendations to the agency head on the whistleblower's retaliation claim. They cannot negotiate relief for a whistleblower or pursue enforcement, even if they find retaliation occurred. Always remember, too, that an IG's general counsel and whistleblower coordinator are not your legal representatives. They work for the IG. Further, whistleblower coordinators do not investigate retaliation cases.

Some federal employees can also use a union process to adjudicate their claims of prohibited whistleblower retaliation.

You and your attorney, if you have one, should choose your outlet for relief based on your needs. But be cautious in doing so, as exercising one

right could permanently eliminate the other options. For example, if an employee goes to MSPB first with a claim that they were fired in retaliation and they lose that case, they cannot later go to OSC with that claim. Employees who are a part of a union may have the option of participating in arbitration with the agency. This can be a good option to settle disputes quickly, and with the support and resources of the employee's union. However, it is no longer the whistleblower's case at that point. The union is the party in an arbitration, not the employee. Before arbitration hearings begin, unions can and frequently do drop cases that the whistleblower wants to pursue. Further, someone who elects arbitration can no longer seek relief through the Office of Special Counsel or Merit Systems Protection Board.

For most federal employees, the OSC and MSPB adjudication processes are the only way to seek legal relief when facing retaliation for blowing the whistle without losing control over their rights.[34] These processes are outlined in greater detail below.

The Office of Special Counsel

The first step for most federal employees when they are subjected to whistleblower retaliation will be filing a claim with the OSC.[35] If you go this route, here is what to expect.

After receiving your retaliation claim, OSC must acknowledge receipt and assign the claim to an OSC contact within 15 days.[36] From there, the OSC must decide whether to terminate or pursue an investigation based on the information you provided. OSC may terminate the investigation at the outset if the whistleblower is filing a repeat claim with the same facts—in other words, OSC won't investigate the same claim filed by the same person twice, or if the whistleblower has already filed their claim with the MSPB. OSC may also terminate the investigation if it doesn't have jurisdiction over the claim (for example, if your position isn't covered by whistleblower retaliation protection law), or if the retaliation happened more than three years prior to being filed with OSC.[37]

If OSC decides to terminate the investigation immediately, it must notify you within 30 days of termination.[38] If it doesn't terminate immediately, they will proceed with an investigation.

OSC investigations aim to determine if there are "reasonable grounds to believe that a prohibited personnel practice has occurred, exists, or is to be

taken."[39] Investigators are required to notify you within 90 days of the complaint's filing if OSC is proceeding with the investigation and must update you on the status of the case every 60 days.[40] OSC then has 240 days to conduct its investigation.[41]

If, in the course of the investigation, OSC determines that reasonable grounds of a prohibited personnel practice do not exist, it must notify you 10 days before terminating the case.[42] That window gives you an opportunity to provide more information or comments related to their claim. If OSC still decides to terminate the investigation, you have 65 days to take their case directly to the MSPB to seek relief on their own.[43]

If OSC ultimately finds that retaliation has occurred, it will send notice to the relevant parties, with recommendations to the agency on how to correct the retaliation.[44]

If the OSC and you believe the agency has sufficiently followed the OSC's recommendations, the case can end there and the OSC files a final report. However, if the agency fails to correct the identified problems within "a reasonable period of time," OSC can then petition the MSPB to compel the agency to act. If the petition is not resolved, it triggers a formal hearing process at the MSPB.[45] Because Congress did not empower OSC to force agency action itself, it must rely on MSPB to order the agency to take action to fix the prohibited practices.

Know that the Office of Special Counsel has extremely limited resources compared to the number of claims it receives.

Know that the OSC has extremely limited resources compared to the number of claims it receives, and for that reason is slow to act and is only able to bring a small percentage of cases in front of the MSPB. As a result, the cases it does bring are typically high-stakes or legally significant. If the OSC doesn't tell you whether it will investigate the case within 120 days of filing, you can skip the investigative process and can take the case directly to the MSPB on your own.[46]

It's up to you and your attorney, if you have one, to decide whether to file first with OSC or the MSPB (if you qualify to do so). While filing first with MSPB will cut out a significant portion of time by eliminating an OSC investigation, it also prevents you from seeking OSC relief if things don't work out at MSPB. Filing first with OSC gives you two bites at the apple and also gives you an option

of formal mediation through its alternative dispute resolution program, which has been highly effective (this program is discussed in more detail below).[47]

Merit Systems Protection Board

The Merit Systems Protection Board is a quasi-judicial entity in the executive branch made up of administrative judges (AJs) and a three-member bipartisan Board, whose members are appointed by the president with the advice and consent of the Senate. The AJs make initial decisions in retaliation cases, and the Board can review AJ decisions.[48]

Unlike OSC, MSPB is empowered by Congress to compel agencies to correct illegal behavior. Because of that power, the MSPB can also issue "stays" at the request of the OSC or at the request of an employee in an Individual Right of Action, preventing the agency from taking further action against a whistleblower or forcing them to rescind an action that was already taken, while an OSC investigation or MSPB case is pending.[49]

The MSPB applies basically the same standards in evaluating a whistleblower case that OSC does, described above. In order to get a favorable ruling at the MSPB, you must demonstrate that your whistleblowing was a "contributing factor" in the retaliation you suffered. That is a low bar: it covers any factor which, alone or in combination with other factors, tends to affect the outcome in any way. However, the agency has an ace in the hole: If it can prove by clear and convincing evidence that it would have taken the personnel action regardless of your disclosure, the MSPB cannot order corrective action.

The process of review can be multi-tiered, depending on any appeals filed by you or the agency.

First, usually after an evidentiary hearing, administrative judges make initial decisions on allegations of prohibited personnel practices.

After an AJ's initial decision, agencies have one option for appeal and whistleblowers have two. The losing side can appeal the case to the three-member Board. If neither you nor the agency appeals the AJ's initial decision to the Board within 35 days, the AJ decision becomes a "final decision" of the MSPB.[50]

However, whistleblowers have the additional option of appealing the case to a federal appeals court. This option is available to whistleblowers because they have the right to appeal a "final decision" of the MSPB to federal

court.[51] Agencies do not have this option in the absence of exceptional circumstances.[52]

Choosing to appeal an unfavorable "initial decision" to the three-member Board may be the less-expensive route to take. It also gives you another chance to prevail, in that you can appeal the three-member Board's final decision, if you want, to federal court. But there are downsides to this process. Once you appeal to the three-person board, the case can't proceed to federal court until the Board releases its final decision on the appeal. (This is true, too, if the agency appeals the case to the board. By filing a petition for review, the agency keeps an AJ's decision in favor of a whistleblower from becoming "final." However, the relief ordered by the AJ, including reinstatement but not back pay or attorneys' fees, goes into force while the appeal to the Board is pending.[53])

While AJs have only 120 days to complete their review of a case, the Board can take as long as it wants.[54] Delays of one to two years are not uncommon.[55] Appeals to the Board are particularly a problem at the time this book went to press. In order to make decisions on cases, the Board needs at least two active members, but, as of March 2019, it has lacked the necessary quorum for over two years, largely due to politics, since the president must nominate and the Senate must confirm the members. In fact, at the time of this book's publication there are no Board members. As a result, there are over 2,000 whistleblower cases stuck in limbo, waiting on the Board to make a final decision of whether to uphold the administrative judge's initial decision.

Going straight to federal court is not without its pitfalls.

You can alternatively choose to allow the AJ's initial decision to become final, thereby triggering the right to take their case directly to federal court. Although it is highly unlikely that a whistleblower will win at that level, this bypasses the perhaps years-long wait for a final decision from the Board.[56]

However, going straight to federal court is not without its pitfalls. It will be much more expensive, because you would certainly want to hire an experienced attorney if you hadn't already. Further, attorneys are likely to make whistleblowers pay as they go, because current law does not provide attorney's fees for lawyers' work in appellate courts, even if they win. By cutting out the three-member Board and instead going to federal court, you may save time but will run up your bill and give up an additional bite at the

appeals apple. Further, the appellate court could remand your case back to the MSPB, placing you back where you started.

If you first file a petition for review with the Board but later want to try your case at the federal court instead, you have the option to request a withdrawal of their petition. With no Board, this decision to approve the withdraw request is now made by the clerk of the Board. However, any objection by the agency would kill the request to withdraw because there is no Board to review it.[57]

Note that if an AJ's initial decision is in your favor, the relief is granted immediately, even if the agency appeals.[58] This applies to pay, benefits, and other terms of employment, but does not include back pay or attorney's fees. However, it is up to the agency to decide whether to allow an employee to physically return to work, pending the agency's appeal to the Board.[59]

If an AJ's initial decision is in favor of the agency, on the other hand, the agency's action against the whistleblower remains in place, pending the whistleblower's appeal. So, if the agency fired you, you are still fired while your appeal is heard.

Alternative Dispute Resolution

Another option for employees making claims of retaliation is OSC's alternative dispute resolution program (ADR). This relatively new program sidesteps the investigative and adjudication process, which can be lengthy and expensive, and replaces it with mediation between you and the agency. The ADR unit is largely successful, and obtaining relief through agreement rather than "victory" can lessen the chances for renewed retaliation.

If you and the agency fail to settle, you can then seek relief through the investigative process described above.

Given the large backlog of cases due to OSC's limited resources, mediation can be a good option. As always, however, we strongly advise that you speak with an experienced attorney before moving forward.

The MSPB also has a mediation program, as well as a settlement judge program.

A Note on Relief and the Courts

Federal civil-service-employee whistleblowers are now the only major sector of the workforce who are not able to enforce their legal rights before a jury

WHISTLEBLOWERS SHOULD ALWAYS TELL THE TRUTH

Telling the truth is paramount when it comes to whistleblowing. Lying to any federal official is a felony and can result in criminal liability.[60] But beyond that, telling the truth is important to preserve a whistleblower's credibility and integrity, particularly with congressional offices, members of the press, and advocacy organizations, who are aligning their own name and credibility with a whistleblower by repeating and acting on what that whistleblower told them.

Even a small exaggeration can prevent those who sincerely want to help from feeling like they can trust anything a whistleblower says. If you stretch the truth a little bit, it will give wrongdoers ammunition to discredit your entire claim. Further, it will distract from their underlying wrongdoing.

For that reason, you should always be honest with investigators, law enforcement, your attorneys, and anyone else involved in your disclosure or retaliation claim. While you may be tempted to exaggerate out of a fear that you're not adequately conveying the facts, trained investigators won't need embellishment to understand the implication of the facts of your claim, and will likely have a stronger understanding of the law.

Also consider that once a whistleblower is caught in a lie, no matter how small, the case against their retaliation claim is strengthened. This is doubly true in the intelligence community where clearances can be revoked when clearance holders demonstrate traits that may present national security risks, such as dishonesty. Even if the truth is painful or embarrassing at first, you should always be honest. Once your credibility is lost it will be difficult—if not impossible—to regain.

in federal court. Although whistleblowers can eventually appeal MSPB decisions to a federal appeals court, those appeals are not fact-finding proceedings tried in front of a jury, but arguments about the law's interpretation and the adequacy of MSPB proceedings heard by appellate judges appointed by the president with advice and consent of the Senate. As a result, federal-employee whistleblower-retaliation cases lack the extra layer of insulation from politics that typical jury trials would.

Recent Major Federal Whistleblower Laws

All Circuit Review Act (July 2018): Allowed whistleblowers to appeal Merit Systems Protection Board decisions to a U.S. court of appeals of jurisdiction rather than just to the federal circuit court of appeals in Washington, D.C., which has an abysmal track record for whistleblowers.[61]

Whistleblower Protection Coordination Act (June 2018): Created the position of whistleblower coordinator within each federal inspector general office, and requires the Council of the Inspectors General on Integrity and Efficiency (CIGIE)[62] to issue best practices on how IGs should communicate and work with whistleblowers.[63]

Follow the Rules Act (June 2017): Extended retaliation protections to employees who refuse to comply with an order that would violate a law, rule, or regulation.[64]

Dr. Chris Kirkpatrick Whistleblower Protection Act of 2017 (October 2017): Prohibited employers from accessing an employee's medical records for the purpose of retaliating against the employee; required an agency head to propose disciplinary measures when an agency supervisor is found through an initial OSC or inspector general investigative ruling, or an AJ's initial decision, to have committed a prohibited personnel practice; required the agency head to report whenever an employee dies by suicide after making a disclosure and having a prohibited personnel action taken against them; and required the head of an agency to ensure that new employees are trained on their whistleblower rights, the roles of the Office of Special Counsel and the Merit Systems Protection Board, and the process for making a lawful disclosure.[65]

FBI Whistleblower Protection Enhancement Act of 2016 (December 2016): Expanded the list of officials to whom FBI employees may make a protected disclosure, to include their supervisors or someone within their managerial chain of command.[66]

Act to Enhance Whistleblower Protection for Contractor and Grantee Employees (December 2016): Permanently extended retaliation protections to personal service contractors, grantees, and sub-grantees.[67]

Whistleblower Protection Enhancement Act of 2012 (November 2012): Extended whistleblower protections for non-intelligence community civil-service employees by protecting disclosures made to supervisors regardless of whether the information had been previously disclosed, despite the employee's motives for making the disclosure, whether or not the disclosure was in writing, and regardless of the amount of time that passed between the event and the disclosure. It also included provisions allowing government employees to blow the whistle on censorship or suppression of their peer-reviewed research, codified protections against Nondisclosure Agreements and other gag orders or policies; and began the whistleblower-coordinator and appellate-review pilot programs that were later made permanent in the All Circuits Review Act and Whistleblower Protection Coordination Act.[68]

A NOTE ON FEDERAL INSPECTORS GENERAL

Be cautious if the statute granting you whistleblower protections relies heavily on a federal inspector general to substantiate your claim of retaliation. While that can be immensely helpful in certain cases, you shouldn't blow the whistle with the assumption that the truth will come out just because your case will eventually require investigation by the IG. Even if an IG substantiates your claim, IGs are investigative offices that make recommendations—they don't order agency action.

You should also know that IG investigations can lack transparency and the offices generally aren't as effective at keeping a whistleblower informed about the progress of their case as the Office of Special Counsel. Further, IGs vary in their track record of maintaining a whistleblower's confidentiality.[69]

Further, whistleblower retaliation seldom is a priority for IGs. Their primary mission is investigating fraud, waste, and abuse.

Finally, remember that IGs are a part of the underlying agency. While in an ideal world IGs would be totally independent from the agency, some are more beholden to the agency head than others, or share resources like IT systems with the agency. And, IG investigative reports on whistleblower claims normally are sent to the agency head to make a final determination in the case.

Protections for Contractors and Other Federal Employees

The Whistleblower Protection Act excludes a large cross section of the federal workforce, including employees of private companies that contract with the federal government, employees of intelligence agencies, and members of the military. Even if you are not a "covered" employee under the Whistleblower Protection Act, though, there are unique whistleblower laws for contractors, intelligence community employees and members of the military that could protect you from retaliation. There is a collection of statutory and regulatory rules and protections that dictate the whistleblowing options for those sectors.

Federal Contractors and Grantees

Many federal agencies utilize contract workers—individuals who are employed by companies that contract with the federal government to perform certain jobs. Contractors and recipients of federal grants are covered under a separate law that aims to encourage employees who work for contractors or grantees that are defrauding the federal government to blow the whistle.

If you are an employee of a government contractor, subcontractor, grantee, or subgrantee, the laws protecting you from retaliation dictate that your employer can't retaliate against you if you blow the whistle on:

- Gross mismanagement of a federal grant or contract
- Gross waste of federal funds
- An abuse of authority relating to a general contract or grant
- A substantial and specific danger to public health or safety
- A violation of law, rule, or regulation related to a federal contract or grant[70]

If you make a protected disclosure under these laws and experience retaliation, you can file a claim with the inspector general overseeing the agency administering your organization's grant or contract. You must file that claim within three years of the date of the retaliation. After filing, the inspector general must investigate and submit a report of the findings to you, your

employer, and the head of the agency. The head of the agency must then decide if there is sufficient basis to find retaliation.

After reviewing the IG's report, if the agency head finds that your employer retaliated against you, the agency head must then order your employer to take specific corrective action. If the agency head finds that retaliation didn't occur, or if they fail make a finding one way or the other within 210 days, you can take your case to federal court with the option of a jury trial, and can use the IG's investigative findings as evidence. Interestingly, this law gives contractor and grantee employees stronger protections than federal civil service employees, who don't have the option of requesting a jury trial.

Note that this law does not protect federal contractors working in the intelligence community. Their protections are discussed on the following page.

THE FALSE CLAIMS ACT

The False Claims Act aims to curb fraud against the government by allowing individuals to sue on behalf of the federal government in what are known as *qui tam* lawsuits and to keep a portion of the recovery (see Chapter 4 for more information on the False Claims Act). In recent years, this has resulted in massive settlements that have recovered billions of dollars from entities that were found to have defrauded the government.

The law has strong whistleblower protection provisions but imposes a statute of limitations of three years on retaliation claims.[71] It prohibits retaliation against whistleblowers filing suit under the Act, and allows whistleblowers to challenge retaliation in federal court with the possibility of recovering double back-pay.[72]

The courts have ruled that if they have raised the issue with your supervisors and agency and they have failed to act, federal employees can bring suits challenging fraud under the Act. However, the Act's retaliation provisions don't apply to federal employees because Congress did not waive its sovereign immunity in the statutory language.

Intelligence Community

If you are a federal or contractor employee working in one of the 17 "elements" of the Intelligence Community (IC), you are excluded from protection under the Whistleblower Protection Act. However, depending on your position within the IC and what, exactly, you're disclosing, you can claim protection from retaliation under a patchwork of laws and directives.[73]

Importantly, IC whistleblower protections under this patchwork only apply to disclosures made to very specific audiences. So, unlike non-IC federal whistleblowers, IC whistleblowers can't make disclosures to the press or advocacy groups and claim retaliation protection under the law.[74]

Moreover, while many of the laws covering the IC create rights against retaliation, enforcement of those rights is usually left to the IC's opaque internal review processes rather than to an independent adjudicator like the MSPB. As a result, while you might have rights on paper that protect you from retaliation, those rights are only enforced sporadically in practice—and implementation of the enforcement mechanisms vary widely across the IC.

Congress has passed several laws over the years making it illegal to retaliate against IC whistleblowers. Specifically, the Intelligence Authorization Acts of Fiscal Year 2010 and 2014 were significant leaps forward, creating an inspector general for the intelligence community and making it unlawful to retaliate against IC employees for making protected whistleblowing disclosures, respectively.[75] Under the overarching law prohibiting whistleblower retaliation, it is illegal to retaliate against a covered IC employee by taking or failing to take certain personnel actions against the employee as reprisal for their lawful whistleblowing disclosures. [76]

Covered disclosures under law are those made to:

- The Director of National Intelligence
- The Inspector General of the Intelligence Community
- The head of the employing agency
- The inspector general of the employing agency
- A Congressional intelligence committee, or a Member of a Congressional intelligence committee

The employee must make their disclosure with a reasonable belief that the information they're providing evidences a violation of any federal law, rule, or regulation; mismanagement;[77] a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety.[78]

Unfortunately, the law doesn't provide actual mechanisms to enforce these rights. This means that until Congress modifies that law to provide for enforcement within the statute, IC whistleblowers must rely on agency policies and presidential directives for enforcement of their rights.

The main mechanism for enforcing your rights as an IC whistleblower is Presidential Policy Directive-19 (PPD-19). Created by President Obama in 2012, PPD-19 lays out general enforcement mechanisms protecting IC employees from retaliation for making protected disclosures and requires each IC element to create a more specific process within their own agency.[79]

PPD-19 is broken into several sections. Section A prohibits retaliation against covered employees for making protected disclosures and provides a method of enforcement through review by an inspector General. Section B outlines protections for retaliatory clearance revocation, and Section C creates a three-inspector-general panel to hear appeals from those covered under Sections A and B.

Section A of PPD-19 prohibits retaliation against whistleblowing disclosures and establishes a review process but excludes certain IC employees. It won't protect you if you are an FBI employee, and it does not mention protections for you if you are a contractor employee or a member of the armed services working for an IC element.[80]

The review process created in Section A requires your corresponding agency inspector general to investigate and to make a recommendation of corrective action to your agency head, who can choose whether or not to follow the inspector general's recommendation. The Intelligence Community Inspector General can also conduct the initial investigation, but typically delegates that authority to the corresponding agency's IG.

If you don't agree with the decision reached by the inspector general's initial review, PPD-19 Section C allows you to file a request for review with the Intelligence Community Inspector General. The Intelligence Community Inspector General can choose to set up an external review panel made up of the Intelligence Community Inspector General and two other federal inspectors general to review the agency head's decision. The review panel must complete their review within 180 days. Once the review panel reaches

WHEN THE LEGAL PROCESS LACKS TEETH

In 2016, George Ellard, the inspector general for the National Security Agency (NSA), was found to have retaliated against one of his own employees for blowing the whistle, according to a decision by a group of other inspectors general called the External Review Panel. The Panel was created by Presidential Policy Directive 19 (PPD-19), a set of whistleblower protections for Intelligence Community employees. Following the Panel's finding, the NSA's director proposed Ellard's termination.[81]

But decisions by the External Review Panel in Intelligence Community retaliation cases are not binding on agencies, unlike decisions by the Merit Systems Protection Board or by courts. Ellard appealed to a higher authority: the NSA's parent agency, the Department of Defense. On appeal, the Office of the Assistant Secretary of Defense overruled the External Review Panel and the director of the NSA, and Ellard was allowed to stay employed with the federal government.[82] No details have been reported on what happened to the whistleblower or what they blew the whistle on.

a decision and recommends corrective action, it sends its recommendation back to the agency head. Implementation of the panel's recommendation is never guaranteed, however, and is left to the agency head's discretion.

It isn't clear how well the PPD-19 program is working for IC whistleblowers. It's possible that Section C's secondary review by the panel of three federal IGs could effectively put more pressure on an agency head to take the retaliation claim seriously. Nevertheless, the absence of a more independent review process renders it deficient.

Importantly, because PPD-19 and the agency policies created under its mandate are not laws passed by Congress, they could be revoked by any sitting president at any time without approval by Congress.

Also, Section A of PPD-19 does not expressly protect IC contractor, subcontractor, grantee, subgrantee, or personal services contractor employees, although the Obama Administration interpreted Section B to cover retaliatory security clearance actions against them (security clearance protections will be discussed later in the chapter). This means that if you are a covered IC contractor employee who blows the whistle, while you are technically

protected from retaliation under the law, you are not explicitly entitled to enforcement under PPD-19 as of this writing. The effect of this, we fear, is that IC contractor whistleblowers may feel empowered to come forward but won't get a fair review of their claim if they are retaliated against. Be wary of this and other "Trojan horse" whistleblower protection laws that outlaw retaliation but offer no process for recourse.

Of course, it's possible that individual agencies could choose to extend IC whistleblower protections to contractors under their own policies. But unless PPD-19 is amended to explicitly include contractors, there is no IC-wide mechanism to enforce your statutory protection against retaliation.

The takeaway as an intelligence community whistleblower should be that while there are protections you can point to in law, the main enforcement mechanism, PPD-19 Section A, only covers certain employees and isn't a law created by Congress. Proceed with great caution, and consult with your attorney, if you have one, at every step.[83]

For further reading, the Intelligence Community Inspector General maintains a helpful guide on IC whistleblowing on its website.[84]

FBI Employees

FBI whistleblowers have protections, but despite recent improvements, they are still much weaker than the protections for most of the rest of the federal civilian workforce. When Congress passed the Civil Service Reform Act of 1978, the FBI convinced Members to omit statutory rights in favor of requiring the Bureau to issue regulations creating equivalent protections for its employees.[85] But the FBI failed to issue any until 1998.[86]

In December 2016, Congress passed into law improvements to FBI whistleblower protections.[87] The law expanded the number of protected channels FBI employees can make their disclosures to after the Government Accountability Office found that nearly a third of retaliation complaints it examined were dismissed because FBI employees made disclosures to someone in their chain of command not designated to receive the disclosure.[88]

The protected audiences now include supervisors in an employee's "direct chain of command" up to the FBI director and the attorney general, Congress, the Justice Department's Office Inspector General and Office of Professional Responsibility, the FBI's Office of Professional Responsibility, the FBI Inspection Division, the Office of Special Counsel, and anyone

designated by the above offices and persons to receive disclosures.[89]

If you face retaliation, the first step in the FBI process is to file a claim in writing to either the Justice Department's Office of Inspector General or the Department's Office of Professional Responsibility.[90]

The burdens of proof considered in an FBI whistleblower retaliation case are similar to those in federal civilian cases. If, by a preponderance of evidence standard, you prove that your disclosure "was a contributing factor in the FBI's decision to take or fail to take, or threaten to take or fail to take, a personnel action" against you, then the FBI must show—under the higher clear and convincing standard—that it would have taken that action absent your disclosure.[91]

If the Justice Department's Inspector General or Office of Professional Responsibility closes your case or 120 days have passed since you filed a claim with those offices, you can file a request for correction action with the Department's Office of Attorney Recruitment and Management.[92] You can request a stay—or temporary block—of a pending adverse personnel action, and the director of the Office must rule on that request within 10 business days. The Office can also hold a hearing on the evidence in your case.

However, this process is not as independent for the one for most other federal civilians. It is presided over by an office within the department, ruling on that department's actions. This is in contrast to Merit Systems Protection Board, where most federal civilians can have their retaliation claims heard. The MSPB is independent of the agencies whose actions it is reviewing.

Furthermore, Office of Attorney Recruitment and Management does not publish its decisions, unlike the MSPB.[93] This means you cannot review how other cases, possibly with similar facts as yours, fared before Office.[94]

In order for your agency to find a violation, there must be a finding that your whistleblowing disclosure was a "contributing factor" in the decision to threaten, suspend, or revoke your clearance or access to classified information. However, those who threatened, suspended, or revoked the clearance can get around this by demonstrating by a "preponderance of the evidence" that they would have taken the same action, regardless of the whistleblowing. Congress makes a point to state in the law that the agency should give "utmost deference" to its own assessment of national security interests.

You have the option to appeal an adverse decision but the final choice of whether to restore your clearance or access is left to the agency head rather than an independent body.

EXTRA RISKS FOR GOVERNMENT-ATTORNEY WHISTLEBLOWERS

In 2004, Thomas Tamm was a Justice Department attorney serving in its Office of Intelligence Policy and Review. Tamm was concerned about the George W. Bush Administration's warrantless wiretapping program, so he brought it to the attention of a Senate staffer, who, according to *Newsweek*, was "wary of discussing what sounded like government secrets [and] shut down their conversation." Weeks later, Tamm went to a pay phone and called the *The New York Times*.[95] After the *Times* published a story based on his disclosures and corroborating accounts,[96] Tamm faced an FBI investigation for leaking classified information—during which his house was raided by federal agents seeking evidence—and the threat of an Espionage Act prosecution.[97] The Justice Department ultimately declined to pursue that prosecution.[98]

Even as the threat of criminal prosecutions for revealing secrets receded, however, Tamm still faced discipline as an attorney for revealing information shared with him by his client, the Justice Department. The Office of Disciplinary Counsel for the D.C. Bar, of which he was then a member, pursued a case against him that dragged on for years. In order to settle the charges against him, more than a decade after his disclosure, he accepted censure by the D.C. Bar in 2016, but was allowed to keep his law license.[99] The D.C. Bar's Office of Disciplinary Counsel agreed that Tamm was "motivated solely by his grave concern that the program was unlawful," that "he was careful not to disclose any methods, sources, or specific intercepts about 'the program' to the reporter," and that he believed going to the attorney general with his concerns would have been "futile."[100]

Tamm's case illustrates the professional conflict presented when a government attorney feels a moral obligation to expose wrongdoing but in doing so would reveal information disclosed to them in confidence by their government-agency client. It also raises a profound question: for a government attorney, who is the client? The government agency they work for, the executive branch, the government as a whole, or the public? The answer is not straightforward. Landing on the wrong side of this thorny issue can lead to professional repercussions.

Military Whistleblower Protections

The Military Whistleblower Protection Act makes it illegal to restrict a service member from making lawful communications to Congress or an inspector general.[101] More specifically, it protects you, as a service member, when you make or prepare to make whistleblowing disclosures to a Member of Congress; an Inspector General; a member of a Defense Department audit, nvestigation, or law enforcement organization; or a person in your chain of command.[102]

Protected disclosures communicate information concerning:

- A violation of law or regulation, including a law or regulation prohibiting rape, sexual assault, or other sexual misconduct in violation of the Uniform Code of Military Justice, sexual harassment or unlawful discrimination[103]
- Gross mismanagement
- A gross waste of funds
- Abuse of authority
- A substantial and specific danger to public health or safety
- Certain threats by another member of the armed forces or employee of the federal government[104]

Once you've made a protected disclosure, it's unlawful for anyone with authority to:

- Threaten to take any unfavorable action
- Withhold or threaten to withhold any favorable action
- Make or threaten to make a significant change to your duties or responsibilities that would not be commensurate with your rank
- Fail to respond, as a superior, to any claim of retaliatory action or harassment (where the superior had knowledge of the claim)
- Conduct a retaliatory investigation against a service member[105]

The burden of proof is placed differently in military whistleblower retaliation cases than it is in civilian cases. Military whistleblowers must prove

A NOTE ON SECURITY CLEARANCES

As far as the government is concerned, security clearances are a privilege, not a right. Taken at face value, this is reasonable—we want intelligence agencies to be able to quickly revoke someone's access to classified or sensitive information if they present a genuine threat to our national security. However, limiting your access to classified materials can also be threatened or used in retaliation for your whistleblowing as a clearance holder.

This kind of retaliation against federal employees and contractors is prohibited by law.[106] Your security clearance cannot be threatened or revoked in retaliation for your lawful whistleblower disclosures to the Director of National Intelligence, the head of your agency, the agency IG, or Congress. Lawful disclosures in connection with an appeal, complaint, or other grievance right are also protected.

Unfortunately, the MSPB and the OSC cannot investigate or act against a retaliatory clearance revocation.[107] Instead, there is an administrative process to appeal wrongful revocation through your agency. If you believe your security clearance is being unlawfully threatened, suspended for more than a year, or revoked, you can file a claim with your agency within 90 days. If your agency determines that you were wrongfully retaliated against, it must take corrective action to make you whole. In addition to clearance restoration, you may recover back pay and benefits, expenses, and damages up to $300,000. As with claims of retaliation under PPD-19 Section A, employees who are dissatisfied with the outcome of their security clearance retaliation claim can ask the Intelligence Community Inspector General to establish a three-inspector-general panel to review it. Again, the Intelligence Community Inspector General only has authority to recommend remedies, not enforce your rights.

that they were illegally retaliated against, whereas in civilian cases the agency must prove that they did not retaliate.[108]

Retaliation claims under this law must be filed with the Defense Department Inspector General (or, for the Coast Guard, the Inspector General for the Department of Homeland Security), or the inspector general for the relevant branch of the military. Once the claim is received, the IG must investigate it "expeditiously" under law.[109] Importantly, there is a statute of limitations for retaliation claims: the IG is only required to investigate a claim

of retaliation if you file that claim within one year of when you first learned about the prohibited retaliation.

In the course of investigating the retaliation claim, the IG must also investigate your underlying disclosure of misconduct if an investigation isn't already taking place, or if the investigation is inadequate.[110]

Within 180 days, the IG must report the status of your retaliation claim to you, to the secretary of defense, and the secretary of the relevant military branch. The IG must continue to send updates every 180 days until the investigation is complete.[111]

As the IG begins to investigate your retaliation claim, it can choose to make a "preliminary finding" in order to stall an adverse action against you pending the full investigation. If the IG makes a preliminary finding that it is more likely than not that prohibited retaliation occurred and will result in an immediate hardship to you, the IG must immediately notify the head of the military branch concerned. At that time, the secretary of that branch can choose to "stay"—temporarily suspend—the personnel action, pending the final results of the IG investigation.[112]

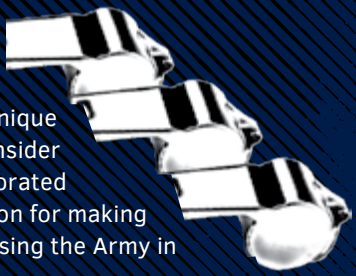
After investigating your retaliation claim and, where applicable, your underlying disclosure, the inspector general must send a detailed report outlining its findings to the secretary of defense, the secretary of the relevant branch of the military, and to you.[113]

Within 30 days of receiving the IG's report, the secretary of the relevant military branch must determine whether or not to take corrective or disciplinary action. If the secretary decides to move forward with corrective or disciplinary action, it's up to the individual secretary to carry that out and to work with the board that corrects military records to ensure that your service record reflects the secretary's decision. If the IG's report concluded that you were retaliated against, the deciding secretary must report back to the IG on whether they will take disciplinary or corrective action.[114]

If the secretary decides that your claim doesn't warrant corrective or disciplinary action, they must report that decision to the secretary of defense.[115]

In addition to this review process on retaliation, there may be a secondary investigation by a statutory board that corrects military records through which a service member can request a formal correction to their record. That board reviews the IG's report, can ask for further evidence, and can hold a full evidentiary hearing on the matter. Unfortunately, this due process

LT. COL. JASON AMERINE



To better understand the overlap of protections and unique fact patterns in an individual whistleblower's case, consider the experience of Lt. Col. Jason Amerine, a highly-decorated war hero who had his clearance suspended in retaliation for making disclosures to Congress and, in our opinion, embarrassing the Army in the process.

Amerine, a Green Beret officer, earned a Bronze Star with a "V" device and a Purple Heart for his service fighting the Taliban in Afghanistan shortly after the September 11 attacks.[116] Amerine observed fatal flaws in the Army's hostage-recovery system after witnessing several avoidable deaths of Americans held hostage overseas and unnecessary interagency fighting over the hostage-recovery process.

Amerine began working with Congress to improve hostage recovery as a result of his experiences. Although the law explicitly prohibits anyone from restricting service members from speaking with Congress or an inspector general, the Army opened a retaliatory criminal investigation against Amerine for his whistleblowing, claiming that he improperly disclosed classified information.[117]

As a result of the retaliatory investigation, Amerine lost his security clearance, was stripped of his duties, temporarily had his pay suspended, and was treated as a criminal by the Army.

To make matters worse, the Defense Department Inspector General did not substantiate Amerine's retaliation claim, allegedly to avoid political controversy.[118]

Fortunately, the Army eventually dropped the investigation, likely due to the high-profile nature of Amerine's career and significant intervention by Congress and civil society groups like the Project On Government Oversight.

Amerine's experiences show the lengths to which those in power will go in their attempts to silence and shame whistleblowers into submission. In the end, Amerine was awarded the Legion of Merit for his service in a private ceremony. Had he not been such a high-profile whistleblower, it is likely that the Army would have succeeded in silencing him.[119]

is discretionary, and in practice has been dormant.

If you are unsatisfied with the final decision of the branch secretary, you can take your case to the secretary of defense, who must decide whether to overturn or uphold the military branch secretary's decision within 90 days of receiving the whistleblower's case.[120]

Note that substantiation rates for military whistleblowers are abysmally low, approximately three percent in any given year,[121] and the DoD IG has yet to exercise its stay authority, according to a spokesperson for that office.[122]

What About the First Amendment?

In an ideal world, whistleblowers would never need to make use of the laws protecting them from retaliation. But it's better to be prepared when going up against agency cultural norms of covering up wrongdoing and punishing anyone who pushes back.

The constitutional freedom of speech is often considered the bedrock of our democracy, protecting diverse ideas and ideologies. For that reason, the First Amendment may be the first protection many whistleblowers want to rely on when facing undue retaliation. But it's more complicated than that.

What we think of as freedom of speech comes from a clause in the First Amendment: "Congress shall make no law…abridging freedom of speech." The Supreme Court has considered whistleblower rights in the context of the First Amendment a handful of times.

In the 1968 landmark case of *Pickering v. Board of Education*,[123] Marvin Pickering, a teacher, had written a letter to a local newspaper criticizing the Township Board of Education in Will County, Illinois, for what he felt was an improper use of funds. The board fired Pickering in response, claiming that the letter was detrimental to their ability to efficiently operate the school system. Pickering appealed, claiming that the board violated his First Amendment rights. The Court ruled in favor of Pickering and established a legal precedent that public employees are protected from retaliatory termination when exposing matters of public concern. Those rights are highly difficult to enforce. The public employee first must demonstrate that the speech was on a matter of public concern, and if so that the public benefits outweigh the disruption to agency operations. Then, the employee must prove that retaliation was a "predominant motivating factor" in the action, after which the employer still can win by proving only through a

OTHER WHISTLEBLOWER LAWS

There are many other federal whistleblower protection laws and regulations that are not covered in detail in this guide but are relevant to federal employees or federal contractor employees. For state employees, note that all states have unique whistleblower laws offering varied coverage. Public Employees for Environmental Responsibility (PEER) tracks and analyzes these laws on their website.[124]

While we can't include all of these laws here, some of the major federal laws not covered in detail in this chapter include:

- The Occupational Safety and Health Act protects certain whistleblowers in the federal government and private sector when they make disclosures about health and safety concerns in their workplace.[125]
- The seven major federal environmental laws—the Clean Water Act, Clean Air Act, Safe Drinking Water Act, Toxic Substances Control Act, Solid Waste Disposal Act, Energy Reorganization Act, and Comprehensive Environmental Response, Compensation and Liability Act (also known as Superfund)—protect disclosures made by public and private employees, and are all enforced by the Department of Labor.[126] The coverage is in some ways broader than under the WPA, as an activity in furtherance of the environmental law in question is protected. Also, the process involves a hearing before an Administrative Law Judge, not just an Administrative Judge like at the MSPB. These judges have more independence and are generally of higher quality than MSPB AJs. For environmental whistleblowers, this can be a preferable route. There is also nothing preventing taking both routes.
- Sarbanes Oxley Act of 2002 protects whistleblowers who report securities fraud to the federal government.[127]
- The FDA Food Safety Modernization Act protects employees in the food industry from retaliation when they make covered disclosures on food safety violations of their employer.[128]
- The Consumer Product Safety Improvement Act protects employees in the manufacturing and distribution industries from retaliation when they make disclosures on consumer safety concerns.[129]

preponderance of the evidence that it would have taken the same action for independent reasons.[130]

Following the Supreme Court's decision in *Bivens v. Six Unknown Agents*,[131] whistleblowers could sue for damages in federal court, and request a jury trial. In *Bush v. Lucas*,[132] however, the Court removed that option for federal employees. It held that since the Civil Service Reform Act established a comprehensive system for remedying retaliation, federal employees must use that system instead of making a constitutional claim. Federal employees now can only challenge constitutional violations through that law's administrative remedies as a prohibited personnel practice.[133]

Finally, in the 2006 case *Garcetti v. Ceballos*,[134] the Court ruled that for a government employee's speech to be protected by the First Amendment, the employee must be speaking as a private citizen, and not as a part of the employee's official duties.

None of these court decisions are provided here to say that it's impossible to get judicial relief as a whistleblower experiencing retaliation, just that it's more difficult than most might think to make a First Amendment free-speech claim as a whistleblower facing retaliation.

Because of the precedent that the Supreme Court established through these cases, rather than seeking relief through the First Amendment, attorneys representing federal employee whistleblowers typically must look first to statutory whistleblower protections when they are fighting agency retaliation. State and local employees still can seek jury trials and compensatory damages through the Civil Rights Act of 1871.[135]

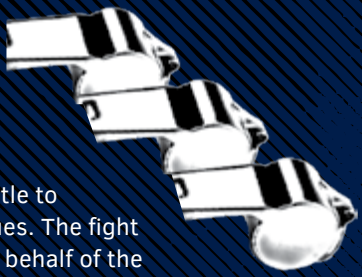
COURTROOM DRAMA

Lawsuits Filed Against Agencies

It is not uncommon for citizen groups to sue an agency on the very issue over which some of the agency's own internal specialists are blowing the whistle. These situations can be extremely delicate for the internal specialists at the agency, particularly if the citizen group suing the agency is doing so largely based upon a specialist's internal dissent.

If you are called as an agency employee witness in litigation to testify about your area of expertise, work product, or knowledge of agency-related matters, you must either be subpoenaed or given permission to testify by agency supervisors. Unless disclosing information protected by whistleblower

THE SAGA OF JEFFREY VAN EE



Jeffrey van Ee, an Environmental Protection Agency employee based in Nevada, waged a ten-year legal battle to guarantee his right to speak out on environmental issues. The fight began in 1990 when van Ee, on his own time, spoke on behalf of the Sierra Club at a Bureau of Land Management (BLM) forum concerning the treatment of endangered desert tortoises.[136]

In an attempt to silence van Ee, the EPA reprimanded van Ee for his participation and ginned up grounds for criminal charges under a part of the criminal code that forbids federal employees from serving as "an agent or attorney" in any case or claim against the United States. After a U.S. attorney declined to prosecute van Ee, the EPA threatened van Ee with disciplinary action or termination if he continued to act as an "agent" of the Sierra Club.[137]

The underlying issue concerning his freedom of speech remained unaddressed until the U.S. Court of Appeals in Washington, DC, ruled in 2000 that federal employees are free to speak on behalf of nonprofit citizen groups when addressing federal agencies. The Court said the law van Ee was charged with violating, 18 U.S.C. Section 205, is not intended to "act as a general gag order on federal employees."

The decision reversed previous rulings by both a lower court and the federal Office of Government Ethics that this type of speech by federal workers was a crime.[138]

"I never believed it would be considered a crime to try to make a difference in my community," van Ee, who was legally represented by the Government Accountability Project and later Public Employees for Environmental Responsibility, reflected after the ruling. "I hope no other federal employee has go to through what I've been through in the past ten years."[139]

statutes, you can be fired for testifying about internal matters unless you have the agency's permission or are acting pursuant to a subpoena.

Lawyers employed within an agency are among the first to be involved in a disputed matter. They enter the scene while the issue is still at the agency level and has not yet gone into litigation. Usually, they also know the agency's weak points and internal analysis of the problem. They have immediate

access to most types of agency information. The agency lawyer does not represent agency whistleblowers and anything told to them can be relayed up the chain of command. The agency's managers closely direct the lawyers' work and greatly influence how agency lawyers handle matters. Ultimately, agency management has control over a government lawyer's continued employment. This can be a difficult situation for an agency lawyer who favors a whistleblower's position.

Once a lawsuit reaches federal court through an appeal, however, the agency is usually compelled to turn the matter over to lawyers in the Department of Justice (DOJ). The DOJ lawyers do not report to the agency management, but handle the case on the agency's behalf generally with assistance from agency counsel. They have their own separate chain of command and handle many separate agency matters. Their client is the United States government, and they do not have loyalty to a particular agency's political agendas, governing regulations, financial concerns, or mission. Their continued employment with the government usually is not dependent on pleasing a specific agency's managers.

These DOJ lawyers usually want to win the litigation or settle it quietly. Further, they want to conduct the process in such a fashion that they do not embarrass themselves in court or anger the judge. This is especially true in a court where the lawyer appears often. They do not want their names associated with scandal, big losses, or publicly disclosed government misconduct.

Even if the DOJ lawyer is friendly to your cause, there are ethical rules that control any interaction between you and a government lawyer. If the lawyer has been directly involved in representing the agency on the matter, the whistleblower should not expect the lawyer to meet with them privately, give them confidential agency documents, breach attorney-client privilege, or sabotage the agency's defense in any overt fashion. Their ethical duty requires them to vigorously represent their client's position and place it above their personal feelings.

Any government lawyer who violates the ethics rules governing their representation of the agency is subject to being fired and disbarred from the practice of law. If you find a friendly government lawyer, you must be especially careful not to put them into a conflicted position or take advantage of their private position on a case.

Not every government lawyer involved in the litigation process is equal, but all are working to represent the agency. Likewise, attorneys representing

the citizen group suing the agency also have a unique agenda and are representing their clients, not the whistleblower whose disclosures their case is based on.

For this reason (among many others) you should always work with your own attorney whose only agenda is protecting and upholding your rights as a whistleblower.


"I didn't like whistleblowing, because I was simply doing my job."
BUNNATINE H. GREENHOUSE
PENTAGON WHISTLEBLOWER

Conclusion

While this guide issues many dire warnings about the dangers of blowing the whistle, it should in no way dissuade you from following your conscience and your desire to make the world a better place.

Frank Serpico, who revealed rampant corruption inside the New York Police Department in the 1970s, prefers the term "lamp lighters" to "whistleblowers." "It's the lamplight that shines on corruption, injustice, ineptitude and abuse of power," as he wrote in the foreword to the first edition of this book. "I shudder at the thought of living in a country without lamp lighters to ignite the torch of liberty as a beacon, welcoming the assembly of freedom-loving people."

This guide is meant to help you shine a light on problems adversely affecting the public and minimize potential harm to your career and life.

Sometimes blowing the whistle is how public servants can best serve the public.

If you decide to become a whistleblower, you will be joining an elite group of people distinguished by their exceptional moral character and their commitment to public justice. The viability of our democracy depends in large part upon this small group of people who are willing to challenge corruption by speaking out about government deception.

Sometimes blowing the whistle is how public servants can best serve the public, despite the negative connotation the word "whistleblower" has in the minds of many.[1] Indeed, most whistleblowing information comers from those are just trying to serve the public by doing their jobs without sacrificing their professional integrity. As Bunnatine Greenhouse, a former senior Pentagon acquisition official who blew the whistle on no-bid military contracts awarded to Halliburton, said during a television interview, "We can't let a term like whistleblower override the fact that when we take oath for office, when we become public servants, that we have responsibility and accountability for the jobs that we are supposed to do."[2]

Knowing the risks involved in whistleblowing and managing those risks effectively can be a challenge. The Project On Government Oversight, Government Accountability Project, and Public Employees for Environmental Responsibility are available to help you manage that process.

Over the years, working with public employees who "commit truth" has been a great honor for the three organizations authoring this guide. We dedicate this guide to the whistleblowers we have known throughout the years—to their sacrifice, their incredible accomplishments, and their legacy of ethical government stewardship.

Endnotes

INTRODUCTION

1 David W. Ewing, "Protecting Whistle-Blowers," *The New York Times*, September 1, 1977. https://www.nytimes.com/1977/09/01/archives/protecting-whistleblowers.html (Downloaded February 21, 2019)

2 Hearing before the House Committee on Oversight and Government Reform Subcommittee on Government Operations, "Five Years Later: A Review of the Whistleblower Protection Enhancement Act" (115-10), February 1, 2017. https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg26314/pdf/CHRG-115hhrg26314.pdf (Downloaded January 15, 2019)

3 For example, Department of Defense Inspector General, *Assessment Report: Review of Office of Deputy Inspector General for Administrative Investigations, Directorate for Military Reprisal Investigations*, May 16, 2011. https://www.documentcloud.org/documents/5750722-Dod-Ig-Internal-Review-of-Whistleblowing.html#document/p5/a484197 (Downloaded January 15, 2019); Government Accountability Office, *Actions Needed to Improve Processing of Prohibited Personnel Practice and Whistleblower Disclosure Cases* (GAO-18-400), June 2018, p. 16. https://www.gao.gov/assets/700/692545.pdf; Robert Barnes, "Supreme Court says former air marshal did not violate law in whistleblower case," *The Boston Globe,* January 22, 2015. https://www.bostonglobe.com/news/nation/2015/01/22/supreme-court-says-former-air-marshal-did-not-violate-law-whistleblower-case/JrpBlphsMVlnj9cKpyZ2IJ/story.html; Adam Zagorin, "CIA Inspector General Nominee Has Three Open Whistleblower Retaliation Cases Implicating Him," Project On Government Oversight, October 16, 2017. https://www.pogo.org/investigation/2017/10/cia-inspector-general-nominee-has-three-open-whistleblower-retaliation-cases-implicating-him/ (All downloaded February 27, 2019)

4 For some examples of whistleblowers seen through a partisan lens, see Nick Schwellenbach, "The Modern Politics of American Whistleblowing: Insiders Valued More Highly in U.S. Society, But Still Face Perils," The Society of Professional Journalists, March 12, 2018. https://www.spj.org/whistleblower/the-modern-politics-of-american-whistleblowing.asp (Downloaded February 21, 2019)

5 Some do not see every insider who exposes government secrets as a hero. For example, see Steven Nelson, "Edward Snowden Unpopular at Home, A Hero Abroad, Poll Finds," *US News,* April 21, 2015. https://www.usnews.com/news/articles/2015/04/21/edward-snowden-unpopular-at-home-a-hero-abroad-poll-finds (Downloaded January 15, 2019)

6 Merit Systems Protection Board, *Blowing the Whistle: Barriers to Federal Employees Making Disclosures,* November 2011, p. i. https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=662503&version=664475 (Downloaded January 15, 2019)

7 Merit Systems Protection Board, "U.S. Merit Systems Protection Board 2017 Annual Employee Survey Results." https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=1455015&version=1460526 (Downloaded January 15, 2019)

8 Global Business Ethics Survey, *The State of Ethics & Compliance in the Workplace,* Ethics & Compliance Initiative, March 2018, p. 9. https://higherlogicdownload.s3.amazonaws.com/THEECOA/11f760b1-56e0-43c6-85da-03df2ce2b5ac/UploadedImages/research/GBES2018-Final.pdf (Downloaded January 15, 2019); for an in-depth description of the challenges faced by corporate whistleblowers, see Tom Devine and Tarek Maassarani, *The Corporate Whistleblower's Survival Guide: A Handbook for Committing the Truth,* San Francisco: Berrett-Koehler Publishers, 2011.

9 Elizabeth W. Morrison, "Employee Voice and Silence," *Annual Review of Organizational Psychology and Organizational Behavior,* Vol. 1, January 2014, pp. 173-197. https://www.researchgate.net/publication/275508087_Employee_Voice_and_Silence; David M. Mayer et al., "Encouraging employees to report unethical conduct internally: It takes a village," *Organizational Behavior and Human Decision Processes,* Vol. 121, February 2013,

pp. 89-103. http://webuser.bus.umich.edu/dmmayer/Published%20Articles/Mayer,%20Nurmohamed,%20Trevino,%20Shapiro,%20%26%20Schminke,%202013.pdf (All downloaded January 15, 2019)

10 5 U.S.C. § 2302(b)(8)

11 At the Office of Special Counsel, in fiscal year 2008, only 1.6 percent of prohibited personnel practice complaints led to favorable outcomes. That rate climbed steadily annually to 5.2 percent in fiscal year 2015. Office of Special Counsel, Communication with Congress 2015-2017. [Disclosure: POGO staffer Nick Schwellenbach, who worked on this book, formerly worked at the Office.] Response of Carolyn Lerner, Office of Special Counsel, to Questions from Chairman Mark Meadows, following the House Committee on Oversight and Government Reform Subcommittee on Government Operations hearing on "Merit Systems Protection Board, Office of Government Ethics, and Office of Special Counsel Reauthorization," December 16, 2015, pp. 4-5 [PDF pp. 298-299]. https://www.governmentattic.org/26docs/OSCcommWcongress_2015-2017.pdf (Downloaded March 5, 2019)

12 "The Make It Safe Coalition is a nonpartisan, trans-partisan network of 75 good government, taxpayer, scientific, labor, civil liberties, and law enforcement organizations dedicated to strengthening protections for whistleblowers in private and public sector who protect the public by exposing waste, fraud and abuse in government." Government Accountability Project, "Make It Safe Coalition Praises Congressional Approval of the Whistleblower Coordination Act," June 19, 2018. https://www.whistleblower.org/press/make-it-safe-coalition-praises-congressional-approval-whistleblower-coordination-act/ (Downloaded February 27, 2019)

13 Hearing before the House Committee on Oversight and Government Reform Subcommittee on Government Operations, "Five Years Later: A Review of the Whistleblower Protection Enhancement Act" (115-10), February 1, 2017. https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg26314/pdf/CHRG-115hhrg26314.pdf (Downloaded January 15, 2019); Jason Zuckerman, "Congress Strengthens Whistleblower Protections for Federal Employees," November-December 2012. https://www.zuckermanlaw.com/wp-content/uploads/2019/01/Whistleblower-Protection-Enhancement-Act.pdf (Downloaded February 22, 2019)

14 Jon O. Shimabukuro, L. Paige Whitaker, and Emily E. Roberts, *Survey of Federal Whistleblower and Anti-Retaliation Laws* (R43045), Congressional Research Service, April 22, 2013. https://fas.org/sgp/crs/misc/R43045.pdf (Downloaded February 22, 2019)

15 The need to better educate employees on their rights and protections has been acknowledged in the law (5 U.S.C. § 2302(c)) and in recent years by the White House. *Second Open Government National Action Plan for the United States of America*, December 5, 2013, p. 6. https://obamawhitehouse.archives.gov/sites/default/files/docs/us_national_action_plan_6p.pdf (Downloaded February 27, 2019)

16 "Testimony of Carolyn Lerner, Special Counsel, U.S. Office of Special Counsel," before the Senate Committee on Appropriations, Subcommittee on Military Construction, Veterans Affairs, and Related Agencies, on "Review of Whistleblower Claims at the Department of Veterans Affairs," July 30, 2015. https://osc.gov/Resources/OSC_Lerner_Testimony_VA_Whistleblowers_7.30.2015.pdf (Downloaded January 15, 2019)

17 Department of Justice Office of Inspector General, *A Review of ATF's Operation Fast and Furious and Related Matters*, November 2012. https://oig.justice.gov/reports/2012/s1209.pdf (Downloaded February 27, 2019)

18 Office of Special Counsel, "Two ATF 'Fast and Furious' Whistleblowers Settle Cases," September 11, 2012. https://osc.gov/News/pr12_17.pdf (Downloaded February 27, 2019)

19 Hearing before the Senate Committee on Homeland Security and Governmental Affairs, "Blowing the Whistle on Retaliation: Accounts of Current and Former Federal Agency Whistleblowers" (114-447), June 11, 2015. https://www.govinfo.gov/content/pkg/CHRG-

114shrg97355/pdf/CHRG-114shrg97355.pdf; Marlow Stern, "The Purple Heart Recipient Hunted by the FBI," *The Daily Beast,* May 29, 2017. https://www.thedailybeast.com/the-purple-heart-recipient-hunted-by-the-fbi downloaded February 27, 2019)

20 Gretchen Gavett, "Why Was President Obama Called As a Witness for WikiLeaks Suspect?," *Frontline*, December 16, 2011. https://www.pbs.org/wgbh/frontline/article/why-was-president-obama-called-as-a-witness-for-wikileaks-suspect/ (Downloaded February 27, 2019)

21 Sean Spicer, "White House Daily Briefing," January 30, 2017, *C-SPAN* video 40:53. https://www.c-span.org/video/?423194-1/sean-spicer-briefs-reporters-white-house&start=2430 (Downloaded March 1, 2019)

22 Bryan Logan, "Trump suggests bombshell New York Times op-ed criticizing his presidency amounts to 'treason,'" *Business Insider,* September 5, 2018. https://www.businessinsider.com/trump-treason-anonymous-new-york-times-op-ed-2018-9 (Downloaded January 15, 2019); Anonymous, "I Am Part of the Resistance Inside the Trump Administration," *The New York Times,* September 5, 2019. https://www.nytimes.com/2018/09/05/opinion/trump-white-house-anonymous-resistance.html (Downloaded February 27, 2019)

23 Rebecca Jones, "Revoking Clearances on a Whim Hurts Whistleblowers—and the Rest of Us," Project On Government Oversight, September 14, 2018. https://www.pogo.org/analysis/2018/09/revoking-clearances-on-a-whim-hurts-whistleblowers-and-the-rest-of-us/; Steve Holland and Jonathan Landay, "Targeting critics, Trump threatens ex-officials' security clearances," *Reuters,* July 23, 2018. https://www.reuters.com/article/us-usa-trump-russia-clearances-idUSKBN1KD2BU (All downloaded February 27, 2019)

24 Office of Special Counsel, "OSC Obtains Stay for VA Doctor Fired after Disclosing Mistakes Made by Inexperienced Anesthesiologists at LA Medical Center," December 4, 2018. https://osc.gov/News/pr-19-2.pdf (Downloaded February 27, 2019)

25 "For the fourth year in a row, OSC received around 6,000 new matters in FY 2018." Office of Special Counsel, "OSC Looks to Build on Notable 2018 Accomplishments," December 20, 2018. https://osc.gov/News/pr-19-4.pdf; In any given year, roughly 40 to50 percent of prohibited-personnel-practice claims are for whistleblower retaliation. Letter from Special Counsel Carolyn Lerner, Office of Special Counsel, to James Read, Merit Systems Protection Board, regarding "Solicitation of Public Comments on MSPB's Proposed Research Agenda," October 16, 2014. https://osc.gov/Resources/10%2016%2014%20James%20Read%20MSPB.pdf; There are different interpretations of what the number of complaints filed with OSC means: it could mean greater awareness and/or confidence in OSC as a venue to file complaints and does not necessarily mean there is more or less retaliation. Federal Drive with Tom Temin, "Tristan Leavitt: What it's like to work at the Office of Special Counsel," *Federal News Network,* July 10, 2018. https://federalnewsnetwork.com/federal-drive/2018/07/tristan-leavitt-what-its-like-to-work-at-the-office-of-special-counsel/ (Downloaded February 27, 2019)

26 Phil Mattingly and Hans Nichols, "Obama Pursuing Leakers Sends Warning to Whistle-Blowers," *Bloomberg Business,* October 17, 2012. https://www.bloomberg.com/news/articles/2012-10-18/obama-pursuing-leakers-sends-warning-to-whistle-blowers (Downloaded January 15, 2019); Jon Greenberg, "CNN's Tapper: Obama has used Espionage Act more than all previous administrations," *Politifact,* January 10, 2014. https://www.politifact.com/punditfact/statements/2014/jan/10/jake-tapper/cnns-tapper-obama-has-used-espionage-act-more-all-/ (Downloaded February 27, 2019)

27 "Since January, the Department has more than tripled the number of active leak investigations compared to the number pending at the end of the last Administration." Department of Justice, "Attorney General Jeff Sessions Delivers Remarks at Briefing on Leaks of Classified Materials Threatening National Security," August 4, 2017. https://www.justice.gov/opa/pr/attorney-general-jeff-sessions-delivers-remarks-briefing-leaks-classified-materials (Downloaded February 27, 2019)

28 Department of Justice, "Former U.S. Senate Employee Indicted on False Statements

Charges," June 7, 2018. https://www.justice.gov/usao-dc/pr/former-us-senate-employee-indicted-false-statements-charges (Downloaded January 15, 2019)

29 James Risen, "The Leaks That Trump's Justice Department Prosecutes Are Mostly About Trump, His Cronies, and Russia," *The Intercept*, February 27, 2019. https://theintercept.com/2019/02/27/trump-russia-leaks-mueller-investigation/ (Downloaded March 2, 2019); In addition, the FBI has formed a new media leaks unit. Ken Klippenstein, "FBI Formed New Media-Leaks Unit, Internal Documents Show," The Young Turks, January 2, 2019. https://tyt.com/stories/4vZLCHuQrYE4uKagy0oyMA/6fo5Taxd1mSGcIQmgoAkOG (Downloaded March 2, 2019)

30 While executive branch employees' whistleblower protections do not include the right to a jury trial, staff in the legislative and judicial branches do not have meaningful whistleblower protections.

31 5 U.S.C. § 2302(b)(9)(D)

32 David Ewing, "Protecting 'Whistle-Blowers,'" *The New York Times*, September 1, 1977. https://www.nytimes.com/1977/09/01/archives/protecting-whistleblowers.html (Downloaded February 27, 2019)

CHAPTER 1

1 Greg Jaffe and Ed O'Keefe, "Obama accepts resignation of VA Secretary Shinseki," *The Washington Post*, May 30, 2014. https://www.washingtonpost.com/politics/shinseki-apologizes-for-va-health-care-scandal/2014/05/30/e605885a-e7f0-11e3-8f90-73e071f3d637_story.html; Richard A. Oppel, Jr., "After Criticism, Investigator Steps Down From the V.A.," *The New York Times,* July 2, 2014. https://www.nytimes.com/2014/07/03/us/after-criticism-investigator-steps-down-from-the-va.html; Donovan Slack, "Embattled VA watchdog stepping down," *USA Today*, June 30, 2015. https://www.usatoday.com/story/news/politics/2015/06/30/va-inspector-general-to-resign-this-week-in-face-of-criticism/29525497/ (All downloaded March 3, 2019)

2 Government Accountability Office, *Department of Veterans Affairs: Actions Needed to Address Employee Misconduct Process and Ensure Accountability* (GAO-18-137), July 2018. https://www.gao.gov/products/GAO-18-137 (Downloaded January 15, 2019)

3 Eric Katz, "The 'Chilling Effect' of Forced Reassignments at Trump's Interior Dept.," *Government Executive,* July 20, 2017. https://www.govexec.com/management/2017/07/its-walking-morgue-whistleblower-explains-decision-speak-out/139612/ (Downloaded March 4, 2019)

David A. Farhenthold, "For whistleblowers, a bold move can be followed by one to department basement," *The Washington Post*, August 3, 2014. https://www.washingtonpost.com/politics/for-whistleblowers-bold-move-can-be-followed-by-one-to-department-basement/2014/08/03/39d12656-182f-11e4-9e3b-7f2f110c6265_story.html (Downloaded March 5, 2019)

4 One manager said of a whistleblower, "I don't like her, so I don't want you to like her either. I don't talk to her, so I don't want you to talk to her either." Office of Special Counsel, *Report of Prohibited Personnel Practice: OSC File No. MA-14-3308 (Teresa Gilbert),* June 8, 2017, p. 11. https://www.documentcloud.org/documents/5756985-Redacted-PPP-Report-Teresa-Gilbert-2-5-18.html#document/p11/a485064 (Downloaded March 4, 2019)

5 For example, Office of Special Counsel, *Report of Prohibited Personnel Practices: Complaint Number MA-07-0385 (Diem-Thi Le),* April 16, 2010, p. 11. https://www.documentcloud.org/documents/263272-osc-redacted-report-on-dcaa-whistleblower-diem.html#document/p11/a484971 (Downloaded March 4, 2019)

6 "Another prominent whistleblower agreed to accept a reassignment after being advised that his career at the Bighorn [National Forest] was in jeopardy. He was later passed over

for promotion to a leadership position in the regional office." Office of Special Counsel, "U.S. Office of Special Counsel Announces Group Settlement of Whistleblower Retaliation Complaints Filed by Former and Current Employees of the Bighorn National Forest," April 22, 2003. https://osc.gov/News/pr03_10.htm (Downloaded March 4, 2019)

7 The Department of Veterans Affairs' Katherine Mitchell is an example. "I worked 2 years of unlimited scheduled shifts without compensation in order to keep my position as medical co-director and provide even bare bones physician staffing…. Staffing was increased after I was removed from the ER. Additional resources were provided including additional patient rooms." Testimony of Dr. Katherine L. Mitchell before the House Committee on Veterans' Affairs hearing on "VA Whistleblowers: Exposing Inadequate Service Provided to Veterans and Ensuring Appropriate Accountability," July 8, 2014, pp. 6-7. https://docs.house.gov/meetings/VR/VR00/20140708/102441/HHRG-113-VR00-Wstate-MitchellMDK-20140708.pdf (Downloaded March 4, 2019)

8 Julie Miller, "Paying The Price For Blowing The Whistle," *The New York Times,* February 12, 1995. https://www.nytimes.com/1995/02/12/nyregion/paying-the-price-for-blowing-the-whistle.html (Downloaded March 4, 2019)

9 For example, in the case of Air Force whistleblower William Zwicharowski, "When Colonel Edmondson [a senior manager] learned that a Privacy Act complaint was filed… he immediately initiated an investigation focused almost exclusively on Mr. Zwicharowski. The investigation included the unusual seizure of Mr. Zwicharowski's computer and needless comprehensive forensic analysis of the computer….The transparent purpose of this thorough forensic analysis was for Colonel Edmondson to attempt to gather evidence of unrelated misconduct." Office of Special Counsel, *Report of Prohibited Personnel Practices: OSC File Nos. MA-10-0764 (William Zwicharowski), MA-10-1699 (Mary Ellen Spera), MA-10-3819 (James Parsons), and MA-10-3820 (David Vance),* January 30, 2012, updated March 14, 2012, p. 34. https://osc.gov/Resources/Amended%20Port%20Mortuary%20Report%20(redacted).pdf (Downloaded March 4, 2019)

10 "The Defense Intelligence Agency is on a witch-hunt. They accused him of stealing pens." Representative Curt Weldon (R-PA), speaking on "Lou Dobbs Tonight," *CNN,* October 20, 2005. http://transcripts.cnn.com/TRANSCRIPTS/0510/20/ldt.01.html (Downloaded March 4, 2019)

11 "The Board will consider evidence regarding the conduct of an agency investigation when the investigation was so closely related to the personnel action that it could have been a pretext for gathering evidence to retaliate against an employee for whistleblowing activity." *Russell v. Department of Justice*, 76 M.S.P.R. 317 (1997), p. 4. https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=247617&version=247889; "And the [Whistleblower Protection Enhancement Act] provides certain forms of relief to employees who are subjected to a retaliatory investigation, which culminate in a personnel action. 5 U.S.C. § 1214(h). An enforcement gap remains, however, for employees who are subjected to a retaliatory investigation—but suffer no discipline as a result." Testimony of Deputy Special Counsel Eric Bachman, Office of Special Counsel, before the House Committee on Oversight and Government Reform Subcommittee on Government Operations Hearing regarding "Five Years Later: A Review of the Whistleblower Protection Enhancement Act," February 1, 2017, p. 7. https://osc.gov/Resources/Bachman-WPEA-testimony.pdf (All downloaded March 4, 2019)

12 Shanna Devine and Tom Devine, *Whistleblower Witch Hunts: The Smokescreen Syndrome,* Government Accountability Project, November 2010. https://www.whistleblower.org/wp-content/uploads/2018/05/WWHfinal.pdf (Downloaded March 4, 2019)

13 Ron Nixon, "Scandals and Investigations, but Few Arrests, for Air Marshals Program," *The New York Times,* April 25, 2018. https://www.nytimes.com/2018/04/25/us/politics/air-marshals-scandals-investigations.html; "Her troubles worsened after she reported the attack: Men continued to harass and intimidate her, she said, and they accused her of informing on them. She was reprimanded for calling out sick, which she said she did to

avoid her attackers, and was ordered to undergo psychiatric evaluations." Katie Benner, "A Nuclear Site Guard Accused Colleagues of Sexual Assault. Then She Was Fired.," *The New York Times,* January 25, 2019. https://www.nytimes.com/2019/01/25/us/politics/department-of-energy-sexual-assault.html (All downloaded March 4, 2019)

14 Statement of Kimberly Hughes to the House Committee on Veterans' Affairs Subcommittee on Oversight and Investigation hearing on "Addressing Continued Whistleblower Retaliation Within VA" (114-13), April 13, 2015, p. 59. https://www.govinfo.gov/content/pkg/CHRG-114hhrg98630/pdf/CHRG-114hhrg98630.pdf; Kate Kenny, "Mental Health as a Weapon: Whistleblower Retaliation and Normative Violence," *Journal of Business Ethics,* April 17, 2018. https://link.springer.com/article/10.1007/s10551-018-3868-4 (All downloaded March 4, 2019)

15 For example, see Associated Press, "Supervisor: Halliburton whistleblower harassed," *NBC News,* November 1, 2004. http://www.nbcnews.com/id/6379190/ns/business-corporate_scandals/t/supervisor-halliburton-whistleblower-harassed/; Neely Tucker, "A Web of Truth," *The Washington Post,* October 19, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801796_pf.html; Tom Fox, "Corporate culture around whistleblowers," *Compliance Week,* October 3, 2017. https://www.complianceweek.com/blogs/the-man-from-fcpa/corporate-culture-around-whistleblowers; One empirical study of whistleblowing at an Air Force based published in 2008 found that women were "more likely to suffer retaliation than men when they are whistleblowers." Frederick D. Lipman, "Women as Whistleblowers: Does Gender Affect Retaliation?," *The Legal Intelligencer,* June 30, 2015. https://www.blankrome.com/publications/women-whistleblowers-does-gender-affect-retaliation; (All downloaded March 4, 2019)

16 "CBS News interview with ICE whistleblower interrupted by surprise visit from government agents," *CBS This Morning*, June 28, 2018. https://www.cbsnews.com/news/former-ice-spokesman-james-schwab-opens-up-about-resignation-trump-administration/ (Downloaded March 4, 2019)

17 Office of Special Counsel, *Report of Prohibited Personnel Practices: Complaint Number MA-07-0385 (Diem-Thi Le),* April 16, 2010, p.14. https://www.documentcloud.org/documents/263272-osc-redacted-report-on-dcaa-whistleblower-diem.html#document/p16/a484991 (Downloaded March 4, 2019)

18 Peter van der Velden et al., "Mental Health Problems Among Whistleblowers: A Comparative Study," *Pyschological Reports,* February 16, 2018. https://doi.org/10.1177%2F0033294118757681; Sally McDonald and Kathy Ahern, "Physical and emotional effects of whistleblowing," *Journal of Psychosocial Nursing and Mental Health Services,* Vol. 40, No. 1, February 2002, pp. 14-27. https://www.ncbi.nlm.nih.gov/pubmed/11813350; Eric Westervelt, "For VA Whistleblowers, A Culture Of Fear And Retaliation," *NPR,* June 21, 2018. https://www.npr.org/2018/06/21/601127245/for-va-whistleblowers-a-culture-of-fear-and-retaliation (All downloaded March 4, 2019)

19 "I'd like to thank my wife for her loyalty during a seven-year nightmare from which we never knew if we would wake up. Without her, I could not have made it." Government Accountability Project, "GAP Praises Settlement of Marine Corps Whistleblower Case," September 25, 2014. https://www.whistleblower.org/press/gap-praises-settlement-marine-corps-whistleblower-case/ (Downloaded March 4, 2019)

20 Nuclear Regulatory Commission analyst Larry Criscione was illegally referred for prosecution because he disclosed to Congress "For Official Use Only" information about nuclear power plants' inability to withstand upstream dam breaks that would cause a meltdown worse than the Fukushima accident, forcing multi-state evacuations. Dave Lochbaum, "Nuclear Regulatory Crusader," *Union of Concerned Scientists*, January 23, 2017. https://allthingsnuclear.org/dlochbaum/nuclear-regulatory-crusader; Department of Justice Office of Legal Counsel, "Applicability of Criminal Statutes and 'Whistleblower' Legislation to Unauthorized Employee Disclosures," February 7, 1980. https://www.justice.gov/file/22466/download (All downloaded March 4, 2019)

21 SLAPP (Strategic Lawsuit Against Public Participation) suits are used to intimidate critics through a lawsuit that is expensive and time-consuming to defend. See Kristen Rasmussen, *SLAPP Stick: Fighting frivolous lawsuits against journalists,* The Reporters Committee for Freedom of the Press, Summer 2011, p. 2. https://www.rcfp.org/wp-content/uploads/imported/ANTISLAPP.pdf; Lori Potter, "SLAPP Lawsuits: Measuring the Threat Against a Right to Petition," Freedom Forum Institute, February 2015. https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-petition/slapp-lawsuits-measuring-the-threat-against-a-right-to-petition/; Nicola Morrow, "The Dakota Access Pipeline Company Is Abusing the Judicial System to Silence Dissent," American Civil Liberties Union, March 1, 2019. https://www.aclu.org/blog/free-speech/rights-protesters/dakota-access-pipeline-company-abusing-judicial-system-silence; Seventeen states do not have laws curbing use of these lawsuits. Public Participation Project, "State Anti-SLAPP Laws." https://anti-slapp.org/your-states-free-speech-protection/ (All downloaded March 4, 2019)

22 For a more complete description of corporate efforts to criminalize whistleblowers for disclosing internal documents, see Tom Devine and Tarek Maassarani, *The Corporate Whistleblower's Survival Guide: A Handbook for Committing the Truth*, San Francisco: Berrett-Koehler Publishers, April 4, 2011, pp. 55-63; Nick Schwellenbach, "Case implicates free speech," *Seattle Post-Intelligencer*, May 7, 2008. https://www.seattlepi.com/local/opinion/article/Case-implicates-free-speech-1272709.php (Downloaded March 4, 2019)

23 Ellen Nakashima and Lisa Rein, "FDA staffers sue agency over surveillance of personal e-mail," *The Washington Post*, January 29, 2012. https://www.washingtonpost.com/world/national-security/fda-staffers-sue-agency-over-surveillance-of-personal-e-mail/2012/01/23/gIQAj34DbQ_story.html (Downloaded March 4, 2019)

24 In one example of an agency appearing to have used a charge of misappropriating government resources against a whistleblower, after Department of Veterans Affairs whistleblower Troy Thompson exposed sanitation and safety issues in his facility, he was charged with stealing government property—expired sandwiches that were going to be thrown away. Office of Special Counsel, "OSC Secures Relief for Additional VA Whistleblowers," July 22, 2015. https://osc.gov/News/pr15-15.pdf (Downloaded March 4, 2019)

25 The Securities and Exchange Commission's Office of the Whistleblower only accepts anonymous disclosures submitted by counsel (this channel is only available for certain types of claims involving companies). Securities and Exchange Commission, "Submit a Tip." https://www.sec.gov/whistleblower/submit-a-tip (Downloaded January 15, 2019)

CHAPTER 2

1 One example of whistleblowers working with advocacy partners to effectively address problems is when federal air marshals worked through the Federal Law Enforcement Officers Association to criticize decisions by their agency's leadership, such as dress-code and early-boarding policies that made it easy for the public—and therefore terrorists—to identify air marshals, who are supposed to be undercover. Those widely reported criticisms led the then-head of the Federal Air Marshal Service to call members of the Association "disgruntled amateurs," among other names. The policies were eventually changed. "Brief of Robert MacLean in Support of Petition for Review," *MacLean v. Department of Homeland Security*, no. 2011-3231, (U.S. Fed. Cir.), p. 13. http://pogoarchives.org/m/wi/maclean/maclean-v-dva-at-brief-20120309.pdf; Government Accountability Office, *Aviation Security: Federal Air Marshal Service Has Taken Actions to Fulfill Its Core Mission and Address Workforce Issues, but Additional Actions Are Needed to Improve Workforce Survey* (GAO-09-273), January 2009, pp. 2, 22. https://www.gao.gov/assets/290/284904.pdf (Downloaded March 5, 2019)

2 In the 1980s, Colonel James Burton, the tester of the Bradley Fighting Vehicle, and his

allies would broadly circulate Burton's memos detailing shortcomings in the vehicle and how the Army rigged tests to make the vehicle appear less vulnerable than it was. Burton's memos would end up being covered by *The Washington Post*. James G. Burton, *Pentagon Wars*, Annapolis, Maryland: Naval Institute Press (1993), pp. 199-201.

3 Lacy MacAuley, "How the Institute for Policy Studies Helped Release the Pentagon Papers: IPS co-founder Marcus Raskin and others provided crucial aid to whistleblower Daniel Ellsberg," Institute for Policy Studies, June 13, 2011. https://ips-dc.org/how_the_institute_for_policy_studies_helped_release_the_pentagon_papers/ (Downloaded March 5, 2019)

4 The Project On Government Oversight successfully worked with anonymous sources to release internal Pentagon documents detailing how the Air Force spent counterterrorism funds on luxury accommodations being built for generals. POGO's sources were never identified. R. Jeffrey Smith, "Terrorism Funds May Let Brass Fly in Style," *The Washington Post,* July 18, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/17/AR2008071703161.html; After POGO worked with Senator John McCain to oppose the Air Force's spending, the Air Force scaled back its plan to build more of these accommodations. Editorial, "I'm Comfortable. How About You?," *The New York Times,* July 24, 2008. https://www.nytimes.com/2008/07/24/opinion/24thu2.html; Danielle Brian, "Remembering John McCain," *Project On Government Oversight,* August 29, 2018. https://www.pogo.org/analysis/2018/08/remembering-john-mccain/ (All downloaded March 5, 2019)

5 Douglas Jehl, "The 43rd President; Interior Choice Sends a Signal On Land Policy," *The New York Times,* December 30, 2000. https://www.nytimes.com/2000/12/30/us/the-43rd-president-interior-choice-sends-a-signal-on-land-policy.html (Downloaded March 14, 2019)

6 "Transition In Washington; Excerpts From Senate Hearing on Norton's Selection as Interior Secretary," *The New York Times,* January 19, 2001. https://www.nytimes.com/2001/01/19/us/transition-washington-excerpts-senate-hearing-norton-s-selection-interior.html (Downloaded March 14, 2019)

7 Michael Grunwald, "Departmental Differences Show Over ANWR Drilling," *The Washington Post,* October 19, 2001. https://www.washingtonpost.com/archive/politics/2001/10/19/departmental-differences-show-over-anwr-drilling/cf80543c-3ad9-4a5d-99b8-bab2afc9c468/ (Downloaded March 14, 2019)

8 Public Employees for Environmental Responsibility, "Secretary Norton Falsified Arctic Refuge Data," October 19, 2001. https://www.peer.org/news/press-releases/secretary-norton-falsified-arctic-refuge-data.html (Downloaded March 14, 2019)Michael Grunwald, "Departmental Differences Show Over ANWR Drilling," *The Washington Post,* October 19, 2001. https://www.washingtonpost.com/archive/politics/2001/10/19/departmental-differences-show-over-anwr-drilling/cf80543c-3ad9-4a5d-99b8-bab2afc9c468/; Society of Environmental Journalists, "Agenda summary: SEJ Eleventh Annual Conference." http://www.sejarchive.org/confer/port/agenda.htm (Downloaded March 14, 2019)

9 Michael Grunwald, "Departmental Differences Show Over ANWR Drilling," *The Washington Post,* October 19, 2001. https://www.washingtonpost.com/archive/politics/2001/10/19/departmental-differences-show-over-anwr-drilling/cf80543c-3ad9-4a5d-99b8-bab2afc9c468/ (Downloaded March 14, 2019)

10 Deborah Schoch and Kenneth Weiss, "Norton Admits 'Mistake,'" *Los Angeles Times,* October 20, 2001. https://articles.latimes.com/2001/oct/20/news/mn-59484 (Downloaded March 14, 2019)

11 Michael Grunwald, "Departmental Differences Show Over ANWR Drilling," *The Washington Post,* October 19, 2001. https://www.washingtonpost.com/archive/politics/2001/10/19/departmental-differences-show-over-anwr-drilling/cf80543c-3ad9-4a5d-99b8-bab2afc9c468/ (Downloaded March 14, 2019)

12 Jon Margolis, "The Arctic: A slave to luck," *High Country News,* November 5, 2001. https://www.hcn.org/issues/214/10848 (Downloaded March 14, 2019); Deborah Schoch and Kenneth Weiss, "Norton Admits 'Mistake,'" *Los Angeles Times,* October 20, 2001. https://articles.latimes.com/2001/oct/20/news/mn-59484 (Downloaded March 14, 2019)

13 Mike Soraghan, "Norton resigns from Interior," *The Denver Post,* March 10, 2006. https://www.denverpost.com/2006/03/10/norton-resigns-from-interior/ (Downloaded March 14, 2019)

14 Jimmy Tobias, "Did a Top-Level Department of the Interior Nominee Commit Scientific Fraud?," Pacific Standard, May 17, 2017. https://psmag.com/environment/did-a-top-level-department-of-the-interior-nominee-commit-scientific-fraud (Downloaded March 14, 2019)

15 Response of David Bernhardt to Senator Mazie Hirono following the Senate Committee on Energy and Natural Resources Hearing on Bernhardt's Nomination to be Deputy Secretary of the Interior, May 18, 2017, p. 217. https://www.govinfo.gov/content/pkg/CHRG-115shrg26073/pdf/CHRG-115shrg26073.pdf (Downloaded March 15, 2019)

16 Note that just because you are speaking to or working with an attorney at an organization does not mean you have an attorney-client relationship with them: you must formally establish the relationship. If the advocacy organization is eligible to represent clients, you can establish an attorney-client relationship with the organization itself. Otherwise, you would establish an attorney-client relationship with an individual attorney at the organization.

17 Note that just because you are working with an attorney does not mean you have a formal attorney-client relationship with them. Information that you share during a consultation to set up an attorney-client relationship is also usually covered by the attorney-client privilege, even if you do not ultimately establish an attorney-client relationship. American Bar Association, "Rule 1.8: Duties to Prospective Client," August 16, 2018. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_18_duties_of_prospective_client/; In certain situations, non-attorneys working at an organization can also be covered by the attorney-client privilege if they are "acting as the agent of a duly qualified attorney under circumstances that would otherwise be sufficient to invoke the privilege." However, a non-attorney cannot, on their own, establish an attorney-client relationship. "Memorandum Re: Privilege Logs," *Sodexomagic, LLC v. Drexel University,* no. 16-5144 (E.D. Pa. Feburary 23, 2018) , pp. 2-3. http://www.paed.uscourts.gov/documents/opinions/18d0129p.pdf (All downloaded March 5, 2019)

18 Not all communications you have with your attorney may be privileged. Congress has, at times, ignored attorney-client privilege. "In the end, it is the congressional committee alone that determines whether to accept a claim of attorney-client privilege." Alissa Dolan, et al., *Congressional Oversight Manual* (RL30240), Congressional Research Service, December 19, 2014, p. 48. https://fas.org/sgp/crs/misc/RL30240.pdf

19 *U.S. v. Zolin*, 491 U.S. 554, 562-63 (U.S. Supreme Court 1989); Fritz Riesmeyer and Emily Crane, "Tips for Addressing Crime-Fraud Exception to the Attorney-Client Privilege in Civil Cases," American Bar Association, June 24, 2018. https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/practice/2018/tips-for-addressing-crime-fraud-exception-to-attorney-client-privilege-in-civil-cases/

20 Julia Donheiser, "The United States has Spent at Least $2.8 Trillion on Counterterrorism Since 9/11," The Center for Public Integrity, May 18, 2018. https://publicintegrity.org/national-security/the-united-states-has-spent-at-least-2-8-trillion-on-counterterrorism-since-9-11/ (Downloaded March 15, 2019)

21 R. Jeffrey Smith, "Terrorism Funds May Let Brass Fly in Style," *The Washington Post,* July 18, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/17/AR2008071703161.html (Downloaded March 15, 2019)

22 Danielle Brian, "POGO Letter to DoD Secretary Robert Gates Regarding extravagant 'Senior Leaer In-Transit Comfort Capsules,'" Project On Government Oversight, July 17, 2008. https://www.pogo.org/letter/2008/07/pogo-letter-to-dod-secretary-robert-gates-regarding-extravagant-senior-leader-in-transit-comfort-capsules/

23 R. Jeffrey Smith, "Terrorism Funds May Let Brass Fly in Style," *The Washington Post,* July 18, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/17/AR2008071703161.html (Downloaded March 15, 2019)

24 Editorial, "I'm Comfortable. How About You?," *The New York Times,* July 24, 2008. https://www.nytimes.com/2008/07/24/opinion/24thu2.html (Downloaded March 15, 2019); The Colbert Report, "The Word – Fight to the Furnish," *Comedy Central*, July 22, 2008. http://www.cc.com/video-clips/twxrmk/the-colbert-report-the-word---fight-to-the-furnish

25 Questions from Senators John McCain and John Warner to Air Force General Duncan McNabb, following the Senate Committee on Armed Services Hearing on "Nominations of Michael B. Donley to be Secretary of the Air Force; Gen. Norton A. Schwartz, USAF, for Reappointment to the Grade of General and to be Chief of Staff, United States Air Force; and Gen. Duncan J. McNabb, USAF, for Reappointment to the Grade of General and to be Commander, United States Transportation Command" (110-666), July 22, 2008, p. 462. https://www.govinfo.gov/content/pkg/CHRG-110shrg46092/pdf/CHRG-110shrg46092.pdf; Senator Clair McCaskill (D-MO), "McCaskill Presses for Better Accountability from Air Force Leadership," July 23, 2008. https://web.archive.org/web/20140912065134/https://www.mccaskill.senate.gov/media-center/news-releases/mccaskill-presses-for-better-accountability-from-air-force-leadership (All downloaded March 15, 2019)

26 Editorial, "I'm Comfortable. How About You?," *The New York Times,* July 24, 2008. https://www.nytimes.com/2008/07/24/opinion/24thu2.html (Downloaded March 15, 2019)

27 The Navy, for example, puts restrictions on the use of personal email accounts for government business under threat of "administrative or punitive action." Memorandum from Robert Foster, Chief Information Officer, Department of the Navy, regarding "Acceptable Use of Department of the Navy (DON) Information Technology (IT)," February 12, 2016, pp. 3-4 https://www.doncio.navy.mil/FileHandler.ashx?id=8019 (Downloaded March 5, 2019)

28 *Department of Homeland Security v. Robert MacLean,* 135 S. Ct. 913 (U.S. Sup. Ct. 2015). https://caselaw.findlaw.com/us-supreme-court/13-894.html (Downloaded January 16, 2019)

29 Joe Davidson, "VA uses patient privacy to go after whistleblowers, critics say," *The Washington Post*, July 17, 2014. https://www.washingtonpost.com/politics/federal_government/va-uses-patient-privacy-to-go-after-whistleblowers-critics-say/2014/07/17/bafa7a02-0dcb-11e4-b8e5-d0de80767fc2_story.html (Downloaded March 5, 2019)

30 "18 U.S.C. § 641 prohibits the theft or misuse of federal government 'things of value.' The federal government has used this statute to prosecute leakers of information: The government considers disclosure to be a type of theft or conversion, and government-produced or government-held information to be government property." Jessica Lutkenhaus, "Prosecuting Leakers the Easy Way: 18 U.S.C. § 641," *Columbia Law Review*, Vol. 114, No. 5, June 2014, pp. 1167. https://columbialawreview.org/wp-content/uploads/2016/04/Lutkenhaus-J..pdf (Downloaded March 5, 2019)

31 Cynthia Crossen, "A Medical Researcher Pays For Doubting Industry Claim," *The Wall Street Journal*, January 3, 2001. https://www.wsj.com/articles/SB978479119332376537 (Downloaded March 14, 2019)

32 Cynthia Crossen, "A Medical Researcher Pays For Doubting Industry Claim," *The Wall Street Journal*, January 3, 2001. https://www.wsj.com/articles/SB978479119332376537 (Downloaded March 14, 2019)

33 Cynthia Crossen, "A Medical Researcher Pays For Doubting Industry Claim," *The Wall*

Street Journal, January 3, 2001. https://www.wsj.com/articles/SB978479119332376537 (Downloaded March 14, 2019)

34 Project On Government Oversight, *Children's Ears & Antibiotics: Gold Mine for Pharmaceutical Companies, Land Mine for Children,* August 1, 1994. https://www.pogo.org/report/1994/08/childrens-ears-antibiotics-gold-mine-for-pharmaceutical-companies-land-mine-for-children/

35 A private attorney, even in the rare case that they have a security clearance, is unlikely to be able to legally access classified material unless an agency consents, and may in fact be required to report the disclosure to the agency. Private attorneys can be authorized to receive and review classified information if they have a need to know and pass government background checks. Justin Elliott and Jesse Eisinger, "Trump's Russia lawyer isn't seeking security clearance, and may have trouble getting one," *ProPublica,* July 12, 2017. https://www.cnbc.com/2017/07/12/trumps-russia-lawyer-isnt-seeking-security-clearance-and-may-have-trouble-getting-one.html; But it is legal for an attorney to be provided patient health information under certain conditions. Littler Mendelson, P.C., "What Three Pending Issues Could Blow Open the Doors of the Whistleblower Provisions of Sarbanes-Oxley/Dodd-Frank," Presented by Harry Wellford, Jr. and Jacqueline Prats, February 24, 2018, slide 13. https://www.americanbar.org/content/dam/aba/events/labor_law/2018/papers/Hot%20Topics%20in%20Whistleblower%20Law.pdf (All downloaded March 5, 2019)

36 "So long as employees are speaking as citizens about matters of public concern, they must face only those speech restrictions that are necessary for their employers to operate efficiently and effectively." *Garcetti v. Ceballos*, 547 U.S. 410 (U.S. Sup. Ct. 2006). https://www.supremecourt.gov/opinions/05pdf/04-473.pdf (Downloaded March 5, 2019)

37 Trevor Timm, "The Trump administration's new method for cracking down on leakers," Columbia Journalism Review*,* October 18, 2018. https://www.cjr.org/covering_trump/trump-leaker-arrest-natalie-mayflower-sours-edwards.php (Downloaded March 5, 2019)

38 Peter Sterne, "America's 'Official Secrets Act' — the long, sad history of the 100 year-old Espionage Act," Freedom of the Press Foundation*,* June 15, 2017. https://freedom.press/news/americas-official-secrets-act-long-sad-history-100-year-old-espionage-act/ (Downloaded March 5, 2019)

39 John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *The Washington Post,* July 18, 2014. https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html (Downloaded January 16, 2019)

40 Jason Leopold, "Meet John Napier Tye, the US Government's Ideal New Whistleblower," *VICE News,* July 30, 2014. https://news.vice.com/en_us/article/mbw4xx/meet-john-napier-tye-the-us-governments-ideal-new-whistleblower (Downloaded January 16, 2019)

41 Ellen Nakashima and Ashkan Soltani, "Privacy watchdog's next target: the least-known but biggest aspect of NSA surveillance," *The Washington Post,* July 23, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/ (Downloaded January 16, 2019)

42 Marisa Taylor, "Pentagon, CIA instructed to re-investigate whistleblower cases," *McClatchy,* July 23, 2015. https://www.mcclatchydc.com/news/nation-world/national/article28348576.html (Downloaded March 14, 2019)

43 Kel McClanahan, email message to Nick Schwellenbach, regarding John Reidy, March 14, 2019.

44 Zach Dorfman and Jenna McLaughlin, "The CIA's communications suffered a catastrophic compromise. It started in Iran," *Yahoo News,* November 2, 2018. https://www.yahoo.com/news/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html (Downloaded March 14, 2019)

45 According to McClanahan, the CIA considers 5 U.S.C. § 555(b), which states that "[a] person compelled to appear in person before an agency or representative thereof is entitled to be accompanied, represented, and advised by counsel," to be inapplicable to complainants or witnesses in Inspector General investigations, since, according to the Agency's logic, they are not "compelled" to appear.

46 David Wise, "Leaks and the Law: The Story of Thomas Drake," *Smithsonian Magazine,* August 2011. https://www.smithsonianmag.com/history/leaks-and-the-law-the-story-of-thomas-drake-14796786/ (Downloaded January 16, 2019);

47 Jane Meyer, "The Secret Sharer," *The New Yorker,* May 23, 2011. https://www.newyorker.com/magazine/2011/05/23/the-secret-sharer; "Indictment," *United States v. Drake,* no. RDB-10-CR-0181 (D. Md. April 14, 2010), pp. 5-7. https://fas.org/sgp/news/2010/04/drake-indict.pdf (All downloaded March 5, 2019)

48 Department of Justice, "Former NSA Senior Executive Pleads Guilty to Unauthorized Access of Government Computer," June 10, 2011. https://www.justice.gov/opa/pr/former-nsa-senior-executive-pleads-guilty-unauthorized-access-government-computer (Downloaded March 5, 2019)

49 Anne Kornblut, "Translator in eye of storm on retroactive classification," *Boston Globe*, July 5, 2004. http://archive.boston.com/news/nation/articles/2004/07/05/translator_in_eye_of_storm_on_retroactive_classification/; Jonathan Abel, "Do you have to keep the government's secrets? Retroactively classified documents, the First Amendment, and the power to make secrets out of the public record," *University of Pennsylvania Law Review,* Vol. 163, March 2015, pp. 1043-1047 https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9475&context=penn_law_review (All downloaded March 5, 2019)

50 There is a procedure laid out in the Intelligence Community Whistleblower Protection Act of 1998 for lawfully communicating classified disclosures to Congress. "Although the ICWPA provides a process for IC whistleblowers—employees and contractors—to securely report complaints to Congress via the relevant IC agency IG, it offers no specific provisions for protecting whistleblowers from reprisal or punishment." Michael E. DeVine, *Intelligence Community Whistleblower Protections: In Brief* (R45345), Congressional Research Service, January 18, 2019, p. 2. https://fas.org/sgp/crs/intel/R45345.pdf (Downloaded March 5, 2019)

51 Department of Justice, "Freedom of Information Act Exemptions." https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-exemptions.pdf (Downloaded March 5, 2019)

52 Nate Jones, "The Next FOIA Fight: The B(5) 'Withhold It Because You Want To' Exemption," *Unredacted*, March 27, 2014. https://unredacted.com/2014/03/27/the-next-foia-fight-the-b5-withold-it-because-you-want-to-exemption/ (Downloaded March 5, 2019)

53 James G. Burton, *Pentagon Wars*, Annapolis, Maryland: Naval Institute Press (1993), pp. 199-201.

54 Through FOIA, the Project On Government Oversight and Open The Government obtained the policy memo directing the separation of immigrant families at the southern U.S. border signed by Department of Homeland Security Secretary Kirstjen Nielsen, a policy that she denied existed, from Customs and Border Protection, not from the Office of the Secretary. Project On Government Oversight, "New Document Shows Nielsen Signed Off on Family Separation Policy," September 25, 2018. https://www.pogo.org/press/release/2018/new-documents-show-nielsen-signed-off-on-family-separation-policy/

55 American Oversight, "HUD Senior Official Lynne Patton Thinks American Oversight Needs To Get A Life," February 12, 2019. https://www.americanoversight.org/hud-senior-official-lynne-patton-thinks-american-oversight-needs-to-get-a-life (Downloaded March 5, 2019)

56 *Applegate v. NRC*, No. 82-1829 (D. D.C. 1983).

57 Letter from Representative Elijah Cummings (D-MD), to Scott Pruitt, Administrator of the Environmental Protection Agency, about delaying production of Freedom of Information Act records, June 11, 2018. https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2018-06-11.EEC%20to%20Pruitt%20re.%20FOIA%20requests.pdf; "If not for a whistleblower, the truth of the matter may never have come to light." Remarks of Chairman Darrell Issa during the House Committee on Oversight and Government Reform hearing, "Why isn't the Department of Homeland Security Meeting the President's Standard on FOIA?" (112-22), March 31, 2011, p. 2. https://www.govinfo.gov/content/pkg/CHRG-112hhrg67719/pdf/CHRG-112hhrg67719.pdf (All downloaded March 5, 2019)

58 Project On Government Oversight, *An Open Letter To The President: The Superconducting Super Collider's Super Excesses,* June 7, 1993. http://www.pogoarchives.org/m/co/super-collider-1993.pdf; Sharon LaFraniere, "House Votes To Kill SSC," *The Washington Post,* June 25, 1993. https://www.washingtonpost.com/archive/politics/1993/06/25/house-votes-to-kill-ssc/f2f91cc3-176b-4366-81e4-38fc743c822e/ (Downloaded March 14, 2019)

59 Sharon LaFraniere, "House Votes To Kill SSC," *The Washington Post,* June 25, 1993. https://www.washingtonpost.com/archive/politics/1993/06/25/house-votes-to-kill-ssc/f2f91cc3-176b-4366-81e4-38fc743c822e/ (Downloaded March 14, 2019); Project On Government Oversight, *An Open Letter To The President: The Superconducting Super Collider's Super Excesses,* June 7, 1993. http://www.pogoarchives.org/m/co/super-collider-1993.pdf

60 Letter from Danielle Brian, Executive Director of POGO, to Hazel O'Leary, Secretary of Energy, about DOE IG's leak investigation, June 29, 1993. https://www.pogo.org/letter/1993/06/pogo-letter-to-doe-secretary-hazel-oleary-concerning-recent-visit-by-doe-ig/

61 Zack Kopplin, "How the FBI uses the Freedom of Information Act to track down whistleblowers," *The Washington Post,* April 9, 2018. https://www.washingtonpost.com/news/posteverything/wp/2018/04/09/how-the-fbi-uses-the-freedom-of-information-act-to-track-down-whistleblowers/ (Downloaded January 16, 2019)

62 "Affidavit of Matthew Pietropola in Support of an Application for a Search Warrant, *In the matter of the search involving Terry [James] Albury*, no. 0:17-MJ-00670-DTS (D. Mn. 2017), pp. 9-10. https://www.documentcloud.org/documents/4426181-Minneapolis-FBI-Agent-Search-Warrant-Application.html#document/p15/a414403 (Downloaded March 5, 2019)

63 "Statement of Delmer Jones, President, National Joint Council of Food Inspection Locals, American Federation of Government Employees," before the House Committee on Government Operations Subcommittee on Human Resources and Intergovernmental Relations, April 11, 1989. https://babel.hathitrust.org/cgi/pt?id=pst.000015447746;view=1up;seq=1 (Downloaded March 13, 2019)

64 Public Employees for Environments Responsibility has an online archive of past surveys it has administered. Public Employees for Environmental Responsibility, "Surveys: Collective Disclosure." https://www.peer.org/publications/surveys-collective-disclosure.html (Downloaded March 5, 2019)

65 The government's official Federal Employee Viewpoint Survey can also be used this way. Nicole Ogrysko, "Lessons from 2 agencies rising the ranks in the Federal Employee Viewpoint Survey," *Federal News Network,* September 26, 2016. https://federalnewsnetwork.com/workforce/2016/09/lessons-2-agencies-rising-ranks-federal-employee-viewpoint-survey/; However, the survey may be being changed in a way that it makes it less useful for evaluating an agency's top leaders than in the past. The definition of "senior leaders" in the Survey changed in 2018 from clearly including the "heads of departments/agencies and their immediate leadership team" to "your nearest senior executive (SES, director or higher-level GS) in your organizational

structure who is responsible for directing policies and priorities within the organization." Erich Wagner, "Advocacy Group Sues for Documents on Federal Employee Viewpoint Survey Tweak," *Government Executive*, November 30, 2018. https://www.govexec.com/oversight/2018/11/advocacy-group-sues-documents-federal-employee-viewpoint-survey-tweak/153188/ (All downloaded March 5, 2019)

66 Dana Wilkie, "Employee Engagement Surveys: Why Do Workers Distrust Them?" Society for Human Resource Management, January 5, 2018. https://www.shrm.org/resourcesandtools/hr-topics/employee-relations/pages/employee-engagement-surveys.aspx (Downloaded March 5, 2019)

CHAPTER 3

1 Citizen Lab, "Security Planner." https://securityplanner.org/#/ (Downloaded January 15, 2019)

2 Electronic Frontier Foundation, "Surveillance Self-Defense." https://ssd.eff.org/en (Downloaded January 15, 2019)

3 Lisa Rein, "Stepped-up computer monitoring of federal workers worries privacy advocates," *The Washington Post*, August 16, 2012. https://www.washingtonpost.com/politics/stepped-up-computer-monitoring-of-federal-workers-worries-privacy-advocates/2012/08/16/94392356-d816-11e1-91e1-eed6436f6d13_story.html (Downloaded January 18, 2019); Ellen Ruppel Shell, "The Employer-Surveillance State," *The Atlantic*, October 15, 2018. https://www.theatlantic.com/business/archive/2018/10/employee-surveillance/568159/ (Downloaded February 19, 2019)

4 Ewen Macaskill and Gabriel Dance, "The NSA Files: Decoded," *The Guardian*, November 1, 2013. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded (Downloaded March 4, 2019)

5 Sean Gallagher, "The Snowden Legacy, part one: What's changed, really?," *Ars Technica*, November 21, 2018. https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/ (Downloaded March 4, 2019)

6 Tim Golden, "Naming Names at Gitmo," *The New York Times Magazine,* October 21, 2007. https://www.nytimes.com/2007/10/21/magazine/21Diaz-t.html (Downloaded March 15, 2019)

7 Carol Rosenberg, "Navy officer sentenced for leak of captives' names," *Miami Herald,* May 19, 2007, updated July 17, 2010. https://www.miamiherald.com/news/nation-world/world/americas/guantanamo/article1928452.html (Downloaded March 15, 2019)

8 Tim Golden, "Naming Names at Gitmo," *The New York Times Magazine,* October 21, 2007. https://www.nytimes.com/2007/10/21/magazine/21Diaz-t.html (Downloaded March 15, 2019)

9 Tim Golden, "Naming Names at Gitmo," *The New York Times Magazine,* October 21, 2007. https://www.nytimes.com/2007/10/21/magazine/21Diaz-t.html (Downloaded March 15, 2019)

10 Scott Horton, "A Tale of Two Lawyers," *Harper's Magazine,* May 20, 2007. https://harpers.org/blog/2007/05/a-tale-of-two-lawyers/ (Downloaded March 15, 2019)

11 Debra Cassens Weiss, "Ex-Navy Lawyer Is Disbarred for Sending Secret Names of Gitmo Detainees to Legal Group," *American Bar Association Journal,* November 26, 2012. http://www.abajournal.com/news/article/ex-navy_lawyer_is_disbarred_for_sending_secret_names_of_gitmo_detainees_to_ (Downloaded March 15, 2019)

12 Associated Press, "U.S. Reveals Identities of Detainees," *The New York Times,* March 4, 2006. https://www.nytimes.com/2006/03/04/politics/us-reveals-identities-of-detainees.html (Downloaded March 15, 2019)

13 Electronic Frontier Foundation. "Printer Dots." https://www.eff.org/cases/foia-printer-dots (Downloaded January 15, 2019)

14 Identity Theft Resource Center, "Photocopying Sensitive Documents? You might want to think again." https://www.idtheftcenter.org/photocopying-sensitive-documents-you-might-want-to-think-again/ (Downloaded March 5, 2019)

15 After *The Intercept* reported a story based on documents leaked by Winner that included apparent scans of the files, security researchers noted potentially identifiable printer dots. The indictment connected to Winner also revealed that a journalist shared the document with a source prior to publication in an attempt to verify the document. Alexis Madrigal, "The Mysterious Printer Code that Could Have Led the FBI to Reality Winner," *The Atlantic*, June 5, 2017. https://www.theatlantic.com/technology/archive/2017/06/the-mysterious-printer-code-that-could-have-led-the-fbi-to-reality-winner/529350/ (Downloaded February 25, 2019)

16 Electronic Frontier Foundation, "HTTPS Everywhere." https://www.eff.org/https-everywhere (Downloaded January 15, 2019)

17 Electronic Frontier Foundation, "Privacy Badger." https://www.eff.org/privacybadger (Downloaded March 13, 2019); NoScript, https://noscript.net/ (Downloaded March 13, 2019)

18 American College of Trial Lawyers, *The Attorney-Client Privilege in Congressional Investigations*, 2010. https://www.actl.com/docs/default-source/default-document-library/newsroom/attorney-client_relationships_2010_final-web.pdf?sfvrsn=4 (Downloaded February 19, 2019)

19 Jennifer Schleshinger and Andrea Day, "How GPS can track you, even if you turn it off," *CNBC*, July 14, 2018. https://www.cnbc.com/2018/07/13/gps-can-spy-on-you-even-when-you-turn-it-off.html (Downloaded March 3, 2019)

20 Dylan Curran, "Are your phone camera and microphone spying on you?," *The Guardian*, April 6, 2018. https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying (Downloaded March 5, 2019.)

21 Electronic Frontier Foundation, "Surveillance Self-Defense." https://ssd.eff.org/en (Downloaded January 15, 2019)

22 Freedom of the Press Foundation, "Guide & Trainings." https://freedom.press/training/ (Downloaded January 15, 2019)

23 Electronic Frontier Foundation, "How to: Use PGP for Windows." https://ssd.eff.org/en/module/how-use-pgp-windows (Downloaded March 6, 2019)

24 Signal, "What is a safety number and why do I see that it changed?" https://support.signal.org/hc/en-us/articles/360007060632-What-is-a-safety-number-and-why-do-I-see-that-it-changed- (Downloaded January 15, 2019)

25 K. Cohn-Gordon et al., "A formal security analysis of the signal messaging protocol," IEEE European Symposium on Security and Privacy (Euro S&P), 2017. https://ieeexplore.ieee.org/abstract/document/7961996 (Downloaded March 4, 2019)

26 Lorenzo Franceschi-Bicchierai, "'Disappearing' Signal Messages Are Store Indefinitely on Mac Hard Drives," Motherboard, May 9, 2018. https://motherboard.vice.com/en_us/article/kzke7z/signal-disappearing-messages-are-stored-indefinitely-on-mac-hard-drives (Downloaded January 15, 2019)

27 A "burner" refers to an inexpensive cell phone typically disposed of soon after using to reduce the likelihood of it being connected to its user.

28 Brett Max Kaufman, "New Documents Reveal Government Effort to Impose Secrecy on Encryption Company," American Civil Liberties Union, October 4, 2016. https://www.aclu.org/blog/national-security/secrecy/new-documents-reveal-government-effort-impose-secrecy-encryption (Downloaded January 15, 2019)

29 Tor Project, "What is Tor Browser." https://www.torproject.org/projects/torbrowser.html.en (Downloaded January 15, 2019)

30 Jason Koebler, "How the NSA (Or Anyone Else) Can Crack Tor's Anonymity," *Motherboard*, November 19, 2014. https://motherboard.vice.com/en_us/article/4x3qnj/how-the-nsa-or-anyone-else-can-crack-tors-anonymity (Downloaded January 15, 2019)

31 Marcy Wheeler, "The Senate Intelligence Committee 702 bill is a domestic spying bill," Emptywheel. https://www.emptywheel.net/2017/10/23/the-senate-intelligence-committee-702-bill-is-a-domestic-spying-bill/ (Downloaded January 15, 2019)

32 Tails, "Privacy for Anyone Anywhere." https://tails.boum.org/index.en.html (Downloaded January 15, 2019)

33 Tails, "Warning." https://tails.boum.org/doc/about/warning/index.en.html (Downloaded January 15, 2019)

34 SecureDrop, "SecureDrop." https://securedrop.org/ (Downloaded January 2015, 2019)

35 SecureDrop, "Source Guide." https://docs.securedrop.org/en/stable/source.html (Downloaded January 15, 2019)

CHAPTER 4

1 "I never wanted to be a whistleblower....I wanted to be an FBI agent, and I wanted to do my job. The only reason I am here is because they prevented me from doing my job." —Michael German, Remarks during the House Committee on Government Reform Subcommittee on National Security, Emerging Threats, and International Relations Hearing on "National Security Whistleblowers in the Post-September 11th Era: Lost in a Labyrinth and Facing Subtle Retaliation" (109-150), February 14, 2006. https://www.govinfo.gov/content/pkg/CHRG-109hhrg28171/html/CHRG-109hhrg28171.htm (Downloaded March 8, 2019)

2 5 U.S.C. § 2302(f)(1)(A)

3 As taped conversations showed, President Nixon ordered the firing of Pentagon whistleblower Ernie Fitzgerald not because he made disclosures, but because he made disclosures publicly to Congress. Nixon told one aide in 1973 that he wanted to "get rid of that son of a bitch." Later that day, he told another aide, "the point was not that he was complaining about the overruns, but that he was doing it in public." Kenneth Bredemier, "Tapes Show Nixon Role in Firing of Ernest Fitzgerald," *The Washington Post,* March 7, 1979. https://www.washingtonpost.com/archive/politics/1979/03/07/tapes-show-nixon-role-in-firing-of-ernest-fitzgerald/048cd88e-60e5-498d-a8e2-e3b39461356b/ (Downloaded March 8, 2019)

4 Council of the Inspectors General on Integrity and Efficiency, "Inspectors General Directory." https://ignet.gov/content/inspectors-general-directory (Downloaded March 8, 2019)

5 5 U.S.C. App. § 5(a)(17)

6 Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Investigations,* November 15, 2011, pp. 2, 8. https://ignet.gov/sites/default/files/files/invprg1211appi.pdf (Downloaded March 8, 2019)

7 Government Accountability Office, *Government Auditing Standards 2018 Revision* (GAO-18-568G), July 2018, pp. 7-14. https://www.gao.gov/assets/700/693136.pdf (Downloaded March 8, 2019)

8 Project On Government Oversight, *Inspectors General: Many Lack Essential Tools for Independence,* February 26, 2008, p. 14. http://pogoarchives.org/m/go/ig/report-20080226.pdf. For a list of agency- and presidentially appointed IGs, see Government Accountability Office, *Inspectors General: Information on Vacancies and IG Community Views on Their Impact* (18-270), March 2018, p. 6. https://www.gao.gov/assets/700/690561.pdf (Accessed March 14, 2019)

9 In testimony, GAO general counsel Gary Kepplinger suggested as much: "the further removed from the appointment source is from the entity to be audited, the greater the level of independence." Testimony of Gary Kepplinger, Government Accountability Office, before the House Committee on Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement, on "Inspectors General: Independent Oversight of Financial Regulatory Agencies," March 25, 2009, p. 3. https://www.gao.gov/new.items/d09524t.pdf (Downloaded March 8, 2019)

10 POGO has recommended improving independence and protections for IGs. Peter Tyler and Rebecca Jones, *The Watchdogs After Forty Years: Recommendations for Our Nation's Federal Inspectors General,* Project On Government Oversight, July 9, 2018. https://docs.pogo.org/report/2018/2018-07-09_POGO_The_Watchdogs_After_40_Years_IG_Report.pdf

11 Seventy-nine percent of federal employees surveyed believed IGs would take their allegations seriously, according to a federal survey administered in 2010. Merit Systems Protection Board, *Blowing the Whistle: Barriers to Federal Employees Making Disclosures,* November 2011, p. 22. https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=662503&version=664475 (Downloaded March 8, 2019)

12 For example, one Office of Inspector General that had its own dysfunctions was the Defense Department IG: It had years of employee satisfaction below the government average; that office recently has turned its employee satisfaction rankings around. Scott Maucione, "DoD IG continues to climb in employee satisfaction ratings," *Federal News Network,* January 3, 2019. https://federalnewsnetwork.com/defense-main/2019/01/dod-ig-continues-to-climb-in-employee-satisfaction-ratings/ (Downloaded March 8, 2019)

13 House Science, Space, and Technology Committee, "Bipartisan Investigation of Commerce IG Raises Troubling Questions About His Current and Past Actions Against Whistleblowers," July 17, 2014. https://science.house.gov/news/press-releases/bipartisan-investigation-commerce-ig-raises-troubling-questions-about-his; Letter from Senators Clair McCaskill (D-MO) and Ron Johnson (R-WI) to the Honorable Phyllis Fong, Chair of the Council of the Inspector General on Integrity and Efficiency, about misconduct committed by the former Acting Inspector General of the Department of Homeland Security, April 23, 2014. https://www.hsgac.senate.gov/imo/media/doc/2014-04-24%20FCO%20Letter%20and%20Investigation%20Report%20into%20Allegations%20of%20Misconduct%20by%20the%20Former%20Acting%20and%20Deputy%20Inspector%20General%20of%20the%20Department%20of%20Homeland.pdf (All downloaded March 8, 2019)

14 The Pentagon IG backed up Government Accountability Project client Franz Gayl's disclosures that U.S. troops were unnecessarily put at risk in vehicles particularly vulnerable to improvised explosive devices and other bombs—a risk known for more than a decade prior to his disclosure. Tom Vanden Brook, "'94 military report panned Humvee as 'deathtrap,'" *USA Today*, February 4, 2009. http://usatoday30.usatoday.com/news/military/2009-02-03-humvee_N.htm; Jeff Schogol, "Marines ask DOD's Inspector General to review MRAP allegations," *Stars and Stripes*, February 27, 2008. https://www.stripes.com/news/marines-ask-dod-s-inspector-general-to-review-mrap-allegations-1.75562 (All downloaded March 8, 2019)

15 Marisa Taylor, "Government ignores audit findings that could save billions, senators conclude," *McClatchy*, October 17, 2016. https://www.mcclatchydc.com/news/nation-world/world/article108692542.html (Downloaded March 8, 2019)

16 5 U.S.C. App § 7(b)

17 Department of Defense Inspector General, *Whistleblower Reprisal Investigation: Mr. Robert Conley* (CRI-HL 112054), April 18, 2011, pp. 10, 14. https://www.documentcloud.org/documents/205667-dod-oig-civilian-reprisal-investigations-report.html (Downloaded March 8, 2019)

18 Office of Special Counsel, *Report of Prohibited Personnel Practices: Complaint Number MA-07-0385 (Diem-Thi Le),* April 16, 2010, p. 11. https://www.documentcloud.org/documents/263272-osc-redacted-report-on-dcaa-whistleblower-diem.html#document/

p4/a37139; Dave Levinthal, "FEC Inspector General Says Top Agency Official Duped Her into Releasing Confidential Criticism," Center for Public Integrity, November 8, 2016. https://publicintegrity.org/federal-politics/fec-inspector-general-says-top-agency-official-duped-her-into-releasing-confidential-criticisms/ (All downloaded March 8, 2019)

19 According to Government Accountability Project Legal Director Tom Devine, such an agreement cannot necessarily be enforced as a contract, but he has never encountered an instance of an IG violating an agreement.

20 The Pentagon IG's report on allegations that then-CIA Director Leon Panetta disclosed classified material to the filmmakers who made the movie *Zero Dark Thirty* was released "six months after it was finished" and IG whistleblowers raised concerns that it was "deliberately suppressed." *Zero Dark Thirty* is a film about the hunt for Osama bin Laden and the operation that led to his death. Letter from Senator Charles Grassley, to John T. Rymer, Inspector General for the Department of Defense, about his investigation of the *Zero Dark Thirty* report, November 17, 2014, pp. 1, 6. https://www.grassley.senate.gov/sites/default/files/judiciary/upload/Zero%20Dark%20Thirty,%2012-02-14,%20final%20report,%20Redacted.pdf (Downloaded March 8, 2019)

21 For example: Editorial, "Unmuzzling the Federal Watchdogs," *The New York Times,* October 10, 2007. https://www.nytimes.com/2007/10/10/opinion/10wed3.html; Jack Anderson and Michael Binstein, "Inspecting the Inspector General," *The Washington Post,* March 21, 1994. https://www.washingtonpost.com/archive/local/1994/03/21/inspecting-the-inspector-general/09287cc5-9ea3-4954-a841-1d56400e43c2/ (All downloaded March 8, 2019)

22 "…what happened to me was that it immediately became—all the questions were what are his motivations for reporting this. And they never would tell me what they thought my motivation was, but the focus became on me as opposed to what the material I reported was." — Michael German, Remarks before the House Committee on Government Reform Subcommittee on National Security, Emerging Threats, and International Relations Hearing on "National Security Whistleblowers in the Post-September 11th Era: Lost in a Labyrinth and Facing Subtle Retaliation" (109-150), February 14, 2006. https://www.govinfo.gov/content/pkg/CHRG-109hhrg28171/html/CHRG-109hhrg28171.htm (Downloaded March 8, 2019)

23 "[T]he focus and tone of the OIG investigations appear to be intended to discredit the whistleblowers by focusing on the word 'secret,' rather than reviewing the access to care issues identified by the whistleblowers and in the OSC referrals." Memorandum from Special Counsel Carolyn Lerner, Office of Special Counsel, to the President, regarding "OSC File Nos. DI-14-2762 and DI-14-3657," February 25, 2016, p. 2. https://osc.gov/PublicFiles/FY2016/16-28%20DI-14-2762%20and%20DI-14-3657/16-28-DI-14-2762-DI-14-3657%20Letter%20to%20the%20President.pdf (Downloaded March 8, 2019)

24 5 U.S.C. App § 7(b)

25 Office of Special Counsel, *Report of Prohibited Personnel Practices: Complaint Number MA-07-0385 (Diem-Thi Le)*, April 16, 2010, p. 4. https://www.documentcloud.org/documents/263272-osc-redacted-report-on-dcaa-whistleblower-diem.html#document/p4/a37139 (Downloaded March 4, 2019)

26 Office of Special Counsel, *Report of Prohibited Personnel Practices: Complaint Number MA-07-0385 (Diem-Thi Le)*, April 16, 2010, p. 29. https://www.documentcloud.org/documents/263272-osc-redacted-report-on-dcaa-whistleblower-diem.html#document/p29/a486327 (Downloaded March 4, 2019)

27 Lydia Dennett, "Fear and Retaliation at the VA," Project On Government Oversight, July 21, 2014. https://www.pogo.org/investigation/2014/07/fear-and-retaliation-at-va/

28 Letter from Richard Griffin, Acting Inspector General for the Department of Veterans Affairs, to the Project On Government Oversight, regarding a subpoena for records, May 30, 2014. https://www.documentcloud.org/documents/1184210-2014-05-30-ig-subpoena

29 Letter from Danielle Brian, Executive Director of POGO, and Scott Amey, POGO General Counsel, to Richard Griffin, Acting Veterans Affairs Inspector General, responding to the VA Inspector General's subpoena, June 9, 2014. https://www.pogo.org/letter/2014/06/pogos-response-to-va-inspector-generals-subpoena-for-whistleblower-records/

30 Letter from Senator Ron Johnson (R-WI) to the Honorable Michael Horowitz, Chair, and Joseph Campbell, Chair of the Integrity Committee, of the Council of the Inspectors General on Integrity and Efficiency, June 11, 2015, p. 1. https://www.hsgac.senate.gov/imo/media/doc/2015-06-11%20RHJ%20to%20CIGIE%20re%20VA%20OIG%20Pogo%20Subpoena.pdf (Downloaded March 15, 2019)

31 Project On Government Oversight, "VA Inspector General Drops Subpoena for POGO's Whistleblower Records," August 12, 2015. https://www.pogo.org/press/release/2015/va-inspector-general-drops-subpoena-for-pogos-whistleblower-records/

32 Project On Government Oversight, *The Art of Congressional Oversight: A User's Guide to Doing it Right* (2nd ed.), 2015, p. 31. http://www.pogoarchives.org/m/coi/pogo-the-art-of-congressional-oversight-handbook.pdf; Senate Homeland Security and Governmental Affairs, "Defense Whistleblowers Tell of Manipulation of Audits," September 10, 2008. https://www.hsgac.senate.gov/media/majority-media/defense-whistleblowers-tell-of-manipulation-of-audits; Statement of the Honorable Calvin L. Scovel III, Inspector General for the Department of Transportation, before the House Committee on Transportation and Infrastructure, on "Actions Needed to Strengthen FAA's Safety Oversight and Use of Partnership Programs," April 3, 2008. https://www.oig.dot.gov/sites/default/files/OIG_STATEMENT_ON_SWA.pdf (All downloaded March 8, 2019)

33 Valerie Heitshusen, *Types of Committee Hearings,* Congressional Research Service, November 15, 2018, p. 1. https://www.senate.gov/CRSpubs/cb39da50-6535-4824-9d2f-e5f1fcf0a3e4.pdf (Downloaded March 8, 2019)

34 "We don't watch these events for new information; rather, they're a form of political theater. Congressional hearings—or at least, those that get media attention or make an appearance in our Facebook feeds—are no longer seen as tools to develop legislation. They are political tools to influence public opinion." Robert Gebelhoff, "Why congressional hearings still matter," *The Washington Post,* September 30, 2016. https://www.washingtonpost.com/news/in-theory/wp/2016/09/30/why-congressional-hearings-still-matter/ (Downloaded March 8, 2019)

35 Michael Stern, "Henry Waxman and the Tobacco Industry: A Case Study in Congressional Oversight," In *When Congress Comes Calling,* Washington: The Constitution Project, 2017. https://constitutionproject.org/wp-content/uploads/2017/05/Waxman.pdf

36 Only 11 percent of Congressional staff are very satisfied that Congress has the "adequate capacity and support (staff, research capability, infrastructure, etc.) to perform its role in democracy." Kathy Goldschmidt, *State of the Congress: Staff Perspectives on Institutional Capacity in the House and Senate,* Congressional Management Foundation, 2017, p. 9. http://www.congressfoundation.org/storage/documents/CMF_Pubs/cmf-state-of-the-congress.pdf (Downloaded March 8, 2019)

37 Seventy and 71 percent of employees said they believed they could trust IGs and OSC, respectively, with protecting their confidentiality. Only 44 percent said the same of Congress. The media fared the worst at 23 percent. Merit Systems Protection Board, *Blowing the Whistle: Barriers to Federal Employees Making Disclosures,* November 2011, p. 22. https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=662503&version=664475 (Downloaded March 8, 2019)

38 Project On Government Oversight, "Green Beret Who Spoke Out Against FBI's Hostage Recovery Efforts is Cleared of Wrongdoing," November 2, 2015. https://www.pogo.org/press/release/2015/green-beret-who-spoke-out-against-fbis-hostage-recovery-efforts-is-cleared-of-wrongdoing/

39 Office of Special Counsel, "Report of Prohibited Personnel Practice: OSC Case No. MA-13-4085," p. 3. https://osc.gov/Resources/PPP%20Report%20FINAL%20Frink_

Redacted-complete.pdf; Emily Wax-Thibodeaux, "Justice for one fired VA whistleblower. But exposing problems is still treacherous," *The Washington Post*, September 9, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/09/09/justice-for-one-fired-va-whistleblower-but-exposing-problems-is-still-treacherous/ (All downloaded March 8, 2019)

40 5 U.S.C. App § 7

41 Department of Justice Inspector General, "Whistleblower Rights and Protections." https://oig.justice.gov/hotline/whistleblower-protection.htm (Downloaded March 8, 2019)

42 For a full discussion of OSC's role regarding federal whistleblowers, see Carolyn Lerner and Jason Zuckerman, *The U.S. Office of Special Counsel's Role in Protecting Whistleblowers and Serving as a Safe Channel for Government Employees to Disclose Wrongdoing,* Office of Special Counsel, May 19, 2014. https://osc.gov/Resources/OSC's%20Role%20in%20Protecting%20Whistleblowers%20(5-19-14).pdf (Downloaded March 8, 2019)

43 Chapter 6 discusses options that different kinds of federal sector employees have for addressing retaliation claims as well as their legal protections. Contractor, FBI, intelligence, and military whistleblowers can file both retaliation complaints and whistleblower disclosures with IGs.

44 5 U.S.C. § 1213(b)

45 5 U.S.C. § 1213(c)(1)(B); Office of Special Counsel, "The OSC Process: What Happens Once An Employee Discloses." https://osc.gov/Pages/DOW-OurProcess.aspx (Downloaded March 8, 2019)

46 5 U.S.C. § 1213(d)

47 5 U.S.C. § 1213(e)

48 5 U.S.C. § 1213(e)(3); Carolyn Lerner and Jason Zuckerman, *The U.S. Office of Special Counsel's Role in Protecting Whistleblowers and Serving as a Safe Channel for Government Employees to Disclose Wrongdoing,* Office of Special Counsel, May 19, 2014, p. 10. https://osc.gov/Resources/OSC's%20Role%20in%20Protecting%20Whistleblowers%20(5-19-14).pdf (Downloaded March 8, 2019)

49 5 U.S.C. § 1213(e)(4)

50 5 U.S.C. § 1213(d)

51 Office of Special Counsel, "Disclosures of Wrongdoing." https://osc.gov/Pages/DOW.aspx (Downloaded March 8, 2019)

52 5 U.S.C. § 1213

53 Julie Gozan and Holley Knaus, "Gagging on Beef," *Multinational Monitor,* Vol. 14, No. 11, November 1992. https://www.multinationalmonitor.org/hyper/issues/1992/11/mm1192_05.html; Associated Press, "Feds: Katrina pump contract mishandled," *East Bay Times,* October 9, 2007. https://www.eastbaytimes.com/2007/10/09/feds-katrina-pump-contract-mishandled/; Mark Hertsgaard, "Nuclear Insecurity," *Vanity Fair,* March 19, 2014. https://www.vanityfair.com/news/2003/11/whistle-blowers-on-vulnerable-us-nuclear-facilities (All downloaded March 8, 2019)

54 Partnership for Public Service, "Donald Sweeney: 2002 Winner, Science and Environment." https://servicetoamericamedals.org/honorees/donald-sweeney/ (Downloaded March 14, 2019)

55 Steven Lee Myers, "Army Corps Falsified Data For a Project, Study Says," *The New York Times,* December 7, 2000. https://www.nytimes.com/2000/12/07/us/army-corps-falsified-data-for-a-project-study-says.html (Downloaded March 14, 2019)

56 Kevin Lavery, "Changing Course: The Whistleblower," *Minnesota Public Radio,* 2000. http://news.minnesota.publicradio.org/features/200009/29_newsroom_mississippi-m/

whistleblower.shtml; Michael Grunwald, "How Corps Turned Doubt Into a Lock," *The Washington Post,* February 13, 2000. http://www.washingtonpost.com/wp-srv/WPcap/2000-02/13/091r-021300-idx.html (All downloaded March 14, 2019)

57 Kevin Lavery, "Changing Course: The Whistleblower," *Minnesota Public Radio,* 2000. http://news.minnesota.publicradio.org/features/200009/29_newsroom_mississippi-m/whistleblower.shtml; Michael Grunwald, "An Agency of Unchecked Clout," *The Washington Post,* September 10, 2000. https://www.washingtonpost.com/archive/politics/2000/09/10/an-agency-of-unchecked-clout/e8e5507f-0fa4-40d7-af98-ed4ac20c23a3/ (All downloaded March 14, 2019)

58 Michael Grunwald, "How Corps Turned Doubt Into a Lock," *The Washington Post,* February 13, 2000. http://www.washingtonpost.com/wp-srv/WPcap/2000-02/13/091r-021300-idx.html (Downloaded March 14, 2019)

59 Michael Grunwald, "Army Corps Delays Study Over Flawed Forecasts," *The Washington Post,* October 5, 2000. https://www.washingtonpost.com/archive/politics/2000/10/05/army-corps-delays-study-over-flawed-forecasts/68275302-15b6-476f-8984-264a01a4d6f8/ (Downloaded March 14, 2019)

60 Michael Grunwald, "Army Corps Rebuked for River Study / Pentagon finds bias, doctored analysis," *The Washington Post,* December 7, 2000. https://www.sfgate.com/news/article/Army-Corps-Rebuked-for-River-Study-Pentagon-2692431.php (Downloaded March 14, 2019)

61 Office of Special Counsel, "Special Counsel Finds That Whistleblower Allegations Demonstrate Substantial Likelihood That Army Corps Of Engineers Engaged In Violations Of Law, Rule Or Regulation, And/Or Gross Waste Of Funds; Requests Investigation By Secretary Of Defense," February 28, 2000. https://osc.gov/News/pr00_07.htm (Downloaded March 14, 2019)

62 Michael Grunwald, "Army Corps Rebuked for River Study / Pentagon finds bias, doctored analysis," *The Washington Post,* December 7, 2000. https://www.sfgate.com/news/article/Army-Corps-Rebuked-for-River-Study-Pentagon-2692431.php (Downloaded March 14, 2019)

63 The Civil Service Reform Act of 1978 does not define what the "substantial likelihood" standard is, but OSC views it as higher than a "reasonable belief" standard. OSC has described the standard as the "high 'substantial likelihood' standard." Office of Special Counsel, "Special Counsel Reports Concerns about Mississippi Veterans Hospital to the White House and Congress," March 18, 2013. https://osc.gov/News/pr13_03.pdf; "In assessing the reasonableness of the discloser's belief, the following objective test is used: whether, given the information available to the whistleblower, a person standing in his shoes could reasonably believe that the disclosed information evidences one of the identified conditions in the statute." The information does not have to ultimately be true to meet the reasonable belief standard. Carolyn Lerner and Jason Zuckerman, *The U.S. Office of Special Counsel's Role in Protecting Whistleblowers and Serving as a Safe Channel for Government Employees to Disclose Wrongdoing,* Office of Special Counsel, May 19, 2014, p. 16. https://osc.gov/Resources/OSC's%20Role%20in%20Protecting%20Whistleblowers%20(5-19-14).pdf (Downloaded March 8, 2019)

64 Office of Special Counsel, "Confidentiality and Anonymity." https://osc.gov/Pages/DOW-Confidentiality.aspx (Downloaded March 8, 2019)

65 "The median lifespan of whistleblower disclosure cases that OSC referred to agencies for investigation increased from 450 days to 668 days from fiscal years 2011 to 2016, a 48 percent increase, with some cases taking as long as 1,523 days (or almost 4.2 years) to close." Government Accountability Office, *Office of Special Counsel: Actions Needed to Improve Processing of Prohibited Personnel Practice and Whistleblower Disclosure Cases* (GAO-18-400), June 2018, p. 18. https://www.gao.gov/assets/700/692545.pdf (Downloaded March 8, 2019)

66 "Too often we lose crucial information or have to end an investigation because the bad

actor either leaves Federal employment or is a contractor or grantee and under current law cannot be subpoenaed. For example, the State Department inspector general oversees the $10.5 billion the agency obligates in grants every year yet cannot compel testimony of the grant recipients even in the event of suspected fraud or misconduct. He can only require current agency employees to speak to his team, which can result in an incomplete or one-sided investigation." Senator Ron Johnson (R-WI). U.S. Congress, Unanimous Consent Request for the "Inspector General Empowerment Act of 2015" (S. 579), Introduced February 26, 2015, by Senator Charles Grassley (R-IA), December 15, 2015. https://www.congress.gov/congressional-record/2015/12/15/senate-section/article/S8665-2 (Downloaded March 11, 2019)

67 Letter from Patrick McFarland, Inspector General for the Office of Personnel Management, to Carolyn Lerner, Special Counsel for the Office of Special Counsel, December 5, 2013, p. 3. https://web.archive.org/web/20131220011531/http://www.osc.gov/documents/Prohibited%20Personnel%20Practices/OPM%20IG_OSC%20Report%20Transmittal%20Letter%20to%20SC.pdf (Downloaded March 15, 2019)

68 "Office of Special Counsel Releases Report Confirming Misconduct by Then-Agency Head Scott Bloch," Project On Government Oversight, December 13, 2013. https://www.pogo.org/analysis/2013/12/office-of-special-counsel-releases-report-confirming-misconduct-by-then-agency-head-scott-bloch/; Debra Katz and Rashida Adams, "Complaint of Prohibited Personnel Practices Against Special Counsel Scott Bloch," Bernabei and Katz, PLLC, March 3, 2005. https://www.kmblegal.com/wp-content/uploads/OSC-Complaint-3-3-05.pdf (Downloaded March 15, 2019); Bernabei and Katz, PLLC no longer exists; the attorneys who worked on the case are now at Katz, Marshall, & Banks, LLP, and Bernabei & Kabat, PLLC. Attorney Deborah Katz serves on POGO's board.

69 Ari Shapiro, "FBI Raids Special Counsel Office, Seizes Records," *National Public Radio,* May 6, 2008. https://www.npr.org/templates/story/story.php?storyId=90223448 (Downloaded March 15, 2019)

70 Federal Bureau of Investigation, "Former Head of the U.S. Office of Special Counsel Pleads Guilty to Criminal Contempt of Congress," April 27, 2010. https://archives.fbi.gov/archives/washingtondc/press-releases/2010/wfo042710.htm (Downloaded March 15, 2019)

71 Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Financial and Contracting Oversight, *Investigation into Allegations of Misconduct by the Former Acting and Deputy Inspector General of the Department of Homeland Security,* April 24, 2014, pp. 2, 6. https://www.hsgac.senate.gov/imo/media/doc/2014-04-24%20FCO%20Letter%20and%20Investigation%20Report%20into%20Allegations%20of%20Misconduct%20by%20the%20Former%20Acting%20and%20Deputy%20Inspector%20General%20of%20the%20Department%20of%20Homeland.pdf (Downloaded March 15, 2019)

72 Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Financial and Contracting Oversight, *Investigation into Allegations of Misconduct by the Former Acting and Deputy Inspector General of the Department of Homeland Security,* April 24, 2014, p. 8. https://www.hsgac.senate.gov/imo/media/doc/2014-04-24%20FCO%20Letter%20and%20Investigation%20Report%20into%20Allegations%20of%20Misconduct%20by%20the%20Former%20Acting%20and%20Deputy%2-0Inspector%20General%20of%20the%20Department%20of%20Homeland.pdf (Downloaded March 15, 2019)

73 Letter from Timothy Delaney, Integrity Committee Chair of the Council of the Inspectors General on Integrity and Efficiency, to Carolyn Lerner, Special Counsel of the Office of Special Counsel, regarding the Integrity Committee Investigation of Charles Edwards, November 19, 2014, p. 2. https://osc.gov/PublicFiles/FY2016/16-38-DI-13-1410-DI-13-1472/16-38-DI-13-1410%20and%20DI-13-1472%20Agency%20Report.pdf

74 Carol Leonnig, "Homeland Security inspector general who was under probe steps

down," *The Washington Post*, December 16, 2013. https://www.washingtonpost.com/politics/homeland-security-inspector-general-who-was-under-probe-stepsdown/2013/12/16/0aeac5ae-66c8-11e3-8b5b-a77187b716a3_story.html (Downloaded March 15, 2019)

75 31 U.S.C. §§3729-3730

76 Department of Justice, "Four Student Aid Lenders Settle False Claims Act Suit for Total of $57.75 Million," November 17, 2010. https://www.justice.gov/opa/pr/four-student-aid-lenders-settle-false-claims-act-suit-total-5775-million; Wiley Rein LLP, "The Fifth Circuit Rules that Government Employees Can Blow the Whistle on Alleged False Claims Act Violations," August 3, 2012. https://www.wileyrein.com/newsroom-articles-2426.html (All downloaded March 8, 2019)

77 Zuckerman Law, "Top-Rated False Claims Act Qui Tam Attorneys." https://www.zuckermanlaw.com/false-claims-act-resources-corporate-whistleblowers/ (Downloaded March 8, 2019)

78 The hub of legal expertise is the nonprofit organization Taxpayers Against Fraud. TAF has an extensive attorney referral list of seasoned False Claims Act specialists (available at https://taf.org/tafef-membership-directory/). It can be particularly tricky for federal employees to succeed in a False Claims Act lawsuit successfully as courts have imposed some additional barriers on them. Wiley Rein LLP, "The Fifth Circuit Rules that Government Employees Can Blow the Whistle on Alleged False Claims Act Violations," August 3, 2012. https://www.wileyrein.com/newsroom-articles-2426.html (Downloaded March 8, 2019)

79 Securities and Exchange Commission, Proposed Rule, "Whistleblower Program Rules," 83 Fed. Reg. 140, July 20, 2018, pp. 34702-34752. https://www.federalregister.gov/documents/2018/07/20/2018-14411/whistleblower-program-rules (Downloaded March 11, 2019)

80 Public Law 111-203, § 922, 124 Stat. 1841; § 748, 124 Stat. 1739 (2010)

81 Securities and Exchange Commission, "Office of the Whistleblower: Submit a Tip." https://www.sec.gov/whistleblower/submit-a-tip (Downloaded March 8, 2019)

82 15 U.S.C. § 78u–6(d)(2)(B); 7 U.S.C. § 26(d)(2)(B)

83 Securities and Exchange Commission, "SEC Announces $2.5 Million Whistleblower Award," July 25, 2017. https://www.sec.gov/news/press-release/2017-130 (Downloaded March 8, 2019)

CHAPTER 5

1 This chapter's title is a phrase coined by media theorist Marshall McLuhan. He wrote in 1964 that, "the medium is the message," meaning how information is transmitted determines what is communicated. Marshall McLuhan, *Understanding Media: The Extensions of Man*, New York, New York: McGraw-Hill, 1964.

2 Rethink Media, "On the Record, Off the Record, On Background, and Not for Attribution – Explained,", September 1, 2016. https://rethinkmedia.org/blog/on-record-off-record-on-background-and-not-attribution-explained (Downloaded January 8, 2019)

3 Associated Press, "Anonymous Sources." https://www.ap.org/about/news-values-and-principles/telling-the-story/anonymous-sources (Downloaded February 5, 2019)

4 Brock Meeks, "Air Marshals pulled from key flights," *MSNBC,* July 29, 2003. https://www.scribd.com/document/221902991/MSNBC-Air-Marshals-Pulled-From-Key-Flights-July-29-2003; *Department of Homeland Security v. MacLean,* U.S. 135 S. Ct. 913 (2015), Opinion p. 3 [PDF p. 6]. https://www.supremecourt.gov/opinions/14pdf/13-894_e2qg.pdf (All downloaded March 15, 2019)

5 *Department of Homeland Security v. MacLean,* U.S. 135 S. Ct. 913 (2015), Opinion p. 4 [PDF p. 5], Opinion p. 7 [PDF p. 10]. https://www.supremecourt.gov/opinions/14pdf/13-894_e2qg.pdf (Downloaded March 15, 2019)

6 *Department of Homeland Security v. MacLean,* U.S. 135 S. Ct. 913 (2015), Opinion p. 2 [PDF p. 7]. https://www.supremecourt.gov/opinions/14pdf/13-894_e2qg.pdf (Downloaded March 15, 2019)

7 POGO interview with Robert MacLean, Federal Air Marshal, on March 11, 2019; Email from Tom Devine, attorney for Robert MacLean, to POGO, March 15, 2019; Alan Maimon, "What happens when a whistleblower returns to work after a decade's fight," *The Washington Post,* March 3, 2016. https://www.washingtonpost.com/lifestyle/magazine/what-happens-when-a-whistleblower-returns-to-work-after-a-decades-fight/2016/03/02/cf3f5062-a41c-11e5-ad3f-991ce3374e23_story.html; Ron Nixon, "Scandals and Investigations, but Few Arrests, for Air Marshals Program," *The New York Times,* April 25, 2018. https://www.nytimes.com/2018/04/25/us/politics/air-marshals-scandals-investigations.html (All downloaded March 15, 2019)

8 Justin Garrick, Affidavit in Support of Arrest of Reality Leigh Winner, June 5, 2017, pp. 4-5. https://www.justice.gov/opa/press-release/file/971331/download (Downloaded February 5, 2019)

9 Erik Wemple, "Did the Intercept bungle the NSA Leak?" *The Washington Post*, June 6, 2017. https://www.washingtonpost.com/blogs/erik-wemple/wp/2017/06/06/did-the-intercept-bungle-nsa-leak/ (Downloaded February 5, 2019)

10 In a 2010 survey, federal employees told the Merit Systems Protection Board that they trust the media less than Congress and inspectors general to keep their identities secret. Merit Systems Protection Board, *Blowing the Whistle: Barriers to Federal Employees Making Disclosures*, November 2011, p. 22. https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=662503&version=664475 (Downloaded February 27, 2019)

CHAPTER 6

1 Ethics Resource Center, *Inside the Mind of a Whistleblower*, May 2012, p. 5. https://www.corporatecomplianceinsights.com/wp-content/uploads/2012/05/inside-the-mind-of-a-whistleblower-NBES.pdf (Downloaded March 19, 2019)

2 To avoid confusion, we refer to the law as the Whistleblower Protection Act of 1989, or WPA. However, the WPA significantly amended the Civil Service Reform Act of 1978, which was the first attempt by Congress to encourage federal whistleblowers to disclose abuses of public trust. These statutory whistleblower protections—found in Title 5 of the U.S. Code—have been amended since 1989.

3 For most federal executive branch employees, the probationary period is one year. At the Department of Defense, it is two years. Merit Systems Protection Board, "Identifying Probationers and Their Rights," in *Adverse Actions: A Compilation of Articles*, December 2016, p. 45. https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=1350368&version=1355695 (Downloaded March 7, 2019); Probationary employees cannot challenge whistleblower retaliation directly to the Merit Systems Protection Board, unless they are dismissed for partisan political reasons (5 C.F.R. 315.806(b)). But they can challenge whistleblower retaliation through the Office of Special Counsel and have the claim graduate into an Individual Right of Action. For a full discussion of probationary employee appeal rights, see Peter Broida, *A Guide to Merit Systems Protection Board Law and Practice*, Arlington: Dewey Publications, 2018, pp. 123-163.

4 5 U.S.C. §1213(a)

5 *Jessica Shannon v. Department of Veterans Affairs,* 2014 M.S.P.B. 41, 10.

6 *Dep't of Homeland Sec. v. MacLean*, 135 S. Ct. 913 (U.S. Sup. Ct. 2015). https://www.supremecourt.gov/opinions/14pdf/13-894_e2qg.pdf (Downloaded March 18, 2019)

7 Department of the Interior Office of Inspector General, *Review of National Icon Park Security* (2003-I-0063), August 2003. https://www.doioig.gov/sites/doioig.gov/files/2003-I-0063.pdf (Downloaded March 15, 2019)

8 David Fahrenthold, "Park Police Duties Exceed Staffing," *The Washington Post,* December 2, 2003. https://www.washingtonpost.com/archive/local/2003/12/02/park-police-duties-exceed-staffing/63830a19-c20e-41ed-9ca7-3832413f6a58/ (Downloaded March 15, 2019)

9 "Testimony of Teresa Chambers before the House Committee on Oversight and Government Reform, on 'Protecting the Public from Waste, Fraud, and Abuse: H.R. 1507, the Whistleblower Protection Enhancement Act of 2009,'" May 14, 2009. https://web.archive.org/web/20170107224308/https://oversight.house.gov/wp-content/uploads/2012/02/20090514Chambers.pdf (Downloaded March 15, 2019)

10 "Testimony of Teresa Chambers before the House Committee on Oversight and Government Reform, on 'Protecting the Public from Waste, Fraud, and Abuse: H.R. 1507, the Whistleblower Protection Enhancement Act of 2009,'" May 14, 2009, pp. 2. https://web.archive.org/web/20170107224308/https://oversight.house.gov/wp-content/uploads/2012/02/20090514Chambers.pdf (Downloaded March 15, 2019)

11 "Testimony of Teresa Chambers before the House Committee on Oversight and Government Reform, on "Protecting the Public from Waste, Fraud, and Abuse: H.R. 1507, the Whistleblower Protection Enhancement Act of 2009,'" May 14, 2009, pp. 2-3. https://web.archive.org/web/20170107224308/https://oversight.house.gov/wp-content/uploads/2012/02/20090514Chambers.pdf (Downloaded March 15, 2019)

12 "Testimony of Teresa Chambers before the House Committee on Oversight and Government Reform, on 'Protecting the Public from Waste, Fraud, and Abuse: H.R. 1507, the Whistleblower Protection Enhancement Act of 2009,'" May 14, 2009, p. 4. https://web.archive.org/web/20170107224308/https://oversight.house.gov/wp-content/uploads/2012/02/20090514Chambers.pdf (Downloaded March 15, 2019)

13 "Brief of Teresa Chambers in Support of Petition for Review," *Chambers v. Interior,* No. 2007-3050, (U.S. Fed. Cir.) March 7, 2007, p. A22. https://www.peer.org/assets/docs/nps/07_5_4_chambers_brief_.pdf (Downloaded March 15, 2019)

14 *Chambers v. Interior,* 2006 M.S.P.B. 279, p. 13. https://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=247802&version=248074 (Downloaded March 15, 2019)

15 *Chambers v. Interior,* No. 2009-3120 (U.S. Fed Cir. 2010). https://caselaw.findlaw.com/us-federal-circuit/1519388.html (Downloaded March 15, 2019)

16 *Chambers v. Interior,* 2011 M.S.P.B. 7. https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=566514&version=568178 (Downloaded March 15, 2019)

17 Joe Davidson, "Unpleasant lessons from case of former Park Police chief," *The Washington Post,* December 10, 2013. https://www.washingtonpost.com/politics/federal_government/unpleasant-lessons-from-case-of-former-park-police-chief/2013/12/10/f3922730-61db-11e3-8beb-3f9a9942850f_story.html (Downloaded March 15, 2019)

18 5 U.S.C. § 2302(a)(2)(D). Some agencies like the State Department, the U.S. Agency for International Development, and the Nuclear Regulatory Commission have separate "dissent channels" where employees can voice policy concerns. Note that these channels are created and controlled by internal agency rules or regulations and not statutory federal law. That means that the channels are created and administered by the agencies themselves, and not Congress, and so could be changed or closed as the agency sees fit without Congressional action.

19 5 U.S.C. § 2302(b)(9)

20 Office of Special Counsel, "Prohibited Personnel Practices (PPPs): Discrimination." https://osc.gov/Pages/PPP.aspx (Downloaded March 19, 2019)

21 Office of Special Counsel, "Prohibited Personnel Practices (PPPs): Discrimination." https://osc.gov/Pages/PPP.aspx (Downloaded March 19, 2019)

22 According to the Government Accountability Project, about 95 percent of whistleblower disclosures are first made internally. Government Accountability Project, *Speaking Up For Science: A Guide to Whistleblowing for Federal Employees*, November 2018, p. 8. https://www.whistleblower.org/wp-content/uploads/2018/11/GAP_Federal-Employees-Whistleblower-Guide.pdf (Downloaded January 26, 2019)

23 There are separate protections that apply to employees of the Intelligence Community, the FBI, and uniformed members of the armed forces that are even more restrictive. While there are substantial similarities in the kinds of disclosures that are protected (e.g. violations of law, gross mismanagement, etc.), those protections are only granted by law if the disclosures are made within the government to certain offices and people. Employees of the intelligence community, the FBI, and uniformed members of the armed forces receive no protections for disclosures to the press or the public even if their disclosures are completely unclassified.

24 5 U.S.C. § 2302(a)(2)(A)

25 See Government Accountability Project, *Whistleblower Witch Hunts*, November 2010. https://www.whistleblower.org/wp-content/uploads/2018/05/WWHfinal.pdf (Downloaded March 19, 2019)

26 *Russell v. Department of Justice*, 76 M.S.P.R. 317 (1997), 324-25 (Merit Systems Protection Board 1997)

27 5 U.S.C. § 1221(g)(4) allows a whistleblower to be compensated for damages resulting from a retaliatory investigation.

28 For example, see "Alleged Intimidation and Potential VA HIPPA Violations Investigated," *HIPPA Journal*, October 11, 2015. https://www.hipaajournal.com/potential-va-hipaa-violations-investigated-8142/ (Downloaded March 19, 2019)

29 *McClellan v. Dep't of Defense*, 53 M.S.P.R. 139 (Merit Systems Protection Board 1994); Jason Zuckerman, "How does a whistleblower prove knowledge of protected whistleblowing?," Zuckerman Law, February 19, 2019. https://www.zuckermanlaw.com/sp_faq/whistleblower-prove-knowledge-protected-whistleblowing/ (Downloaded March 19, 2019)

30 *King v. Dep't of the Army*, 116 M.S.P.R. 689 (Merit Systems Protection Board 2011)

31 The process for making a disclosure to OSC is fully laid out in federal statute at 5 U.S.C. § 1214.

32 5 U.S.C. § 2302(b)(8)(B); Inspector General Act, as amended. 5 U.S.C. App. §§ 3(d)(C) and 11(c)(5)

33 The Inspector General Act of 1978, 5 U.S.C. App. § 3(d)(C)

34 If the whistleblowing involves certain environmental laws, cases can be brought to the Department of Labor. This will be discussed later in the chapter.

35 Whistleblowers who want to have their cases heard before the MSPB must first file with the OSC unless they are facing demotion, suspension of more than two weeks, or termination.

36 5 U.S.C. § 1214(a)(1)(B)

37 5 U.S.C. § 1214(a)(6)(A)

38 5 U.S.C. § 1214(a)(6)(B)

39 5 U.S.C. § 1214(b)(2)(B)

40 5 U.S.C. § 1214(a)(1)(C)(iii)

41 5 U.S.C. § 1214(b)(2)(A)(i)

42 5 U.S.C. § 1214(a)(1)(D)

43 5 U.S.C. § 1214(a)(3)(A)(ii)

44 5 U.S.C. § 1214(b)(2)(B)

45 5 U.S.C. § 1214(b)(2)(C)

46 5 U.S.C. § 1214(a)(3)(B)

47 The resolution rate is 70 percent. Office of Special Counsel, "Alternative Dispute Resolution: FAQs." https://osc.gov/Pages/ADR-FAQs.aspx (Downloaded March 19, 2019)

48 Note that administrative judges are distinct from administrative law judges (ALJ). There are significantly more AJs than ALJs. In practice, while officially following the same procedures, AJs apply them in a more informal, truncated fashion and AJs often lack the independence and impartiality of ALJs. Kent Barnett, "Against Administrative Judges," *UC Davis Law Review*, Vol. 49, No. 5, June 2016. https://lawreview.law.ucdavis.edu/issues/49/5/Articles/49-5_Barnett.pdf (Downloaded March 19, 2019)

49 5 U.S.C. § 1214(b)(1)(A)(i)

50 5 C.F.R. § 1201.113

51 5 U.S.C. § 7703(a)(1)

52 The Office of Personnel Management can seek review of a final MSPB decision that an agency loses, but only if the "Board's decision will have a substantial impact on a civil service law, rule, regulation, or policy directive." 5 U.S.C. § 7703(d)(1)

53 5 U.S.C. § 7701(b)(2)

54 While 5 U.S.C. § 1221 dictates who can go before the board and the standards it uses for review, there is no time limit for how quickly the board must resolve a case.

55 Nicole Ogrysko, "Senate forces 'first' for MSPB as the agency loses all members," *Federal News Network*, March 1, 2019. https://federalnewsnetwork.com/workforce-rightsgovernance/2019/03/senate-forces-first-for-mspb-as-the-agency-loses-all-members/ (Downloaded March 19, 2019)

56 Merit Systems Protection Board, *APR-APP for FY 2018-2020*, March 18, 2019, p. 14. https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=1598039&version=1603838 (Downloaded March 19, 2019)

57 Merit Systems Protection Board, *Policy Regarding Clerk's Authority to Grant Requests to Withdraw Petitions for Review,* May 11, 2018. https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=1515773&version=1521400 (Downloaded March 12, 2019)

58 5 U.S.C. § 7703(d)(1)

59 Under limited circumstances, the employee does not have to be returned to their place of work but must get full pay and benefits. 5 U.S.C. § 7701(b)(2)

60 18 U.S.C. § 1001

61 All Circuit Review Act (Public Law No. 115-195), July 7, 2018. https://www.congress.gov/115/plaws/publ195/PLAW-115publ195.pdf (Downloaded March 19, 2019); Each year since FY 2012, the U.S. Court of Appeals for the Federal Circuit has upheld MSPB rulings at least 92% of the time. Merit Systems Protection Board, *APR-APP for FY 2018-2020*, March 18, 2019, p. 14. https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=1598039&version=1603838 (Downloaded March 19, 2019)

62 "The Council of the Inspectors General on Integrity and Efficiency (CIGIE) is an independent entity established within the executive branch to address integrity, economy and effectiveness issues that transcend individual Government agencies and

aid in the establishment of a professional, well-trained and highly skilled workforce in the Offices of Inspectors General." Council of the Inspectors General on Integrity and Efficiency. https://ignet.gov/ (Downloaded March 19, 2019)

63 Whistleblower Protection Coordination Act (Public Law No. 115-192), June 25, 2018. https://www.congress.gov/115/bills/s1869/BILLS-115s1869enr.pdf (Downloaded March 19, 2019)

64 Follow the Rules Act (Public Law No. 115-40), June 14, 2017. https://www.congress.gov/115/plaws/publ40/PLAW-115publ40.pdf (Downloaded March 19, 2019)

65 Dr. Chris Kirkpatrick Whistleblower Protection Act of 2017 (Public Law No. 115-73), October 26, 2017. https://www.congress.gov/115/plaws/publ73/PLAW-115publ73.pdf (Downloaded March 19, 2019)

66 Federal Bureau of Investigation Whistleblower Protection Enhancement Act of 2016 (Public Law No. 114-302), December 16, 2016. https://www.congress.gov/114/plaws/publ302/PLAW-114publ302.pdf (Downloaded March 19, 2019)

67 An Act to Enhance Whistleblower Protection for Contractor and Grantee Employees (Public Law No. 114-261), December 14, 2016. https://www.congress.gov/114/plaws/publ261/PLAW-114publ261.pdf (Downloaded March 19, 2019)

68 Whistleblower Protection Enhancement Act of 2012 (Public Law No: 112-199), November 27, 2012. https://www.congress.gov/112/plaws/publ199/PLAW-112publ199.pdf (Downloaded March 19, 2019)

69 In a 2019 report on the Defense Department and military-service Inspectors General, the Government Accountability Office found that "DODIG [the Defense Department Inspector General] and the military service IGs have policies to protect whistleblower confidentiality, but some gaps exist. For example, DODIG guidance for protecting whistleblowers who report internal DODIG misconduct does not specify key steps investigators should take to protect confidentiality, such as not identifying complainants during interviews with case subjects. Also, Air Force, Naval, and Marine Corps IG guidance does not specify when whistleblower identities can be disclosed without consent. Without updated guidance, the IGs cannot ensure the consistent implementation of confidentiality protections." Government Accountability Office, *Whistleblower Protection: Analysis of DOD's Actions to Improve Case Timeliness and Safeguard Confidentiality* (GAO-19-198), March, 2019. https://www.gao.gov/assets/700/697337.pdf (Downloaded March 12, 2019)

70 41 U.S.C. § 4712; 10 U.S.C. § 2409

71 31 U.S.C. §3730(h)(3)

72 31 U.S.C. § 3730(h)

73 The Intelligence Community is made up of seventeen "elements": The Office of the Director of National Intelligence; the Central Intelligence Agency; the Defense Intelligence Agency (DIA); the National Security Agency (NSA); the National Geospatial-Intelligence Agency (NGA); the National Reconnaissance Office (NRO); the intelligence elements of the Army, Navy, Marine Corps, and Air Force; the Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis; U.S. Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation; the Drug Enforcement Agency's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; the Department of the Treasury's Office of Intelligence and Analysis. Office of the Director of National Intelligence, "Members of the IC." https://www.dni.gov/index.php/what-we-do/members-of-the-ic (Downloaded March 19, 2019)

74 Also remember that even if you aren't an IC employee, if your disclosure contains legally restricted (i.e. classified) information, it is likewise restricted to certain audiences.

75 Intelligence Authorization Act For Fiscal Year 2010 (Public Law No. 111-259), § 405, October 7, 2010; Intelligence Authorization Act For Fiscal Year 2014 (Public Law No. 113-126), §601, July 7, 2014.

76 50 U.S.C. § 3234 covers federal employees and contractor employees at all the IC elements, except the FBI, which has its own separate statute.

77 Note that for contractor, subcontractor, grantee, subgrantee, or personal services contractor employees, the law requires a showing of "gross" mismanagement, an elevated standard. 50 U.S.C. § 3234(c)(1)(B).

78 50 U.S.C. § 3234(b)

79 "Presidential Policy Directive 19: Protecting Whistleblowers with Access to Classified Information." October 10, 2012. https://www.dni.gov/index.php/ic-legal-reference-book/presidential-policy-directive-19 (Downloaded March 19, 2019)

80 Section A of PPD-19 protects "any employee serving in an Intelligence Community Element." Section F defines Intelligence Community Element and specifically excludes FBI employees. However, it does not define "employee" and does not discuss contractors or members of the armed services working in an IC element.

81 Adam Zagorin, "NSA Watchdog Removed for Whistleblower Retaliation," Project On Government Oversight, December 15, 2016. https://www.pogo.org/investigation/2016/12/nsa-watchdog-removed-for-whistleblower-retaliation/

82 Patrick Eddington, "The Curious Case of Ex-NSA Inspector General George Ellard," CATO Institute, August 3, 2017. https://www.cato.org/blog/curious-case-ex-nsa-inspector-general-george-ellard (Downloaded March 15, 2019)

83 Section B of PPD-19 prohibits retaliatory revocation of security clearances. That section applies to "any officer or employee of an executive branch agency." Further, 50 U.S.C. 3341(j) lays out protections and a review process that expressly applies to federal employees and contractors who hold clearances.

84 Office of the Director of National Intelligence, "What Are My IC Protections?." https://www.dni.gov/ICIG-Whistleblower/protected.html (Downloaded March 10, 2019)

85 5 U.S.C. § 2303

86 See Federal Register Vol. 64, No. 210, November 1, 1999, p. 58782. https://www.govinfo.gov/content/pkg/FR-1999-11-01/pdf/99-27898.pdf (Downloaded March 19, 2019)

87 Federal Bureau of Investigation Whistleblower Protection Enhancement Act of 2016 (Public Law 114-302), December 16, 2016. https://www.congress.gov/114/plaws/publ302/PLAW-114publ302.pdf (Downloaded March 19, 2019)

88 Government Accountability Office, *Whistleblower Protection: Additional Actions Needed to Improve DOJ's Handling of FBI Retaliation Complaints* (GAO-15-112), January 2015, pp. 13-14. https://www.gao.gov/assets/670/668055.pdf (Downloaded March 19, 2019)

89 5 U.S.C. § 2303 and Department of Justice, "How Do I File a Claim?." https://www.justice.gov/oarm/how-do-i-file-claim (Downloaded March 19, 2019)

90 28 C.F.R. Part 27.3

91 Department of Justice, "Burdens of Proof." https://www.justice.gov/oarm/burdens-proof (Downloaded March 19, 2019)

92 28 C.F.R. Part 27.4

93 Senate Judiciary Committee, *Report to Accompany S. 2390, the Federal Bureau of Investigation Whistleblower Protection Enhancement Act of 2016* (114-261), May 25, 2016, pp. 4-5. https://www.congress.gov/114/crpt/srpt261/CRPT-114srpt261.pdf (Downloaded March 19, 2019)

94 The Justice Department states that "the case law of the U.S. Court of Appeals for the Federal Circuit and the U.S. Merit Systems Protection Board, although not binding on OARM, is instructive and looked to for guidance." Department of Justice, "Applicable Law." https://www.justice.gov/oarm/applicable-law (Downloaded March 19, 2019)

95 Michael Isikoff, "The Whistleblower Who Exposed Warrantless Wiretaps," *Newsweek,*

December 12, 2018. https://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805 (Downloaded March 15, 2019)

96 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times,* December 16, 2005. https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (Downloaded March 15, 2019)

97 Michael Isikoff, "The Whistleblower Who Exposed Warrantless Wiretaps," *Newsweek,* December 12, 2018. https://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805; Jim Gilmore, "Thomas Tamm," *PBS Frontline,* December 11, 2013. https://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-tamm/ (Downloaded March 15, 2019)

98 In the *Harvard Law Review*, Columbia University Law Professor David Pozen speculates that "Tamm's civil disobedience was vindicated in the court of public opinion." Pozen cites a conversation he had with a former Justice Department attorney who worked on leak cases who said the Department is unlikely to prosecute if they think the case lacks "jury appeal," in other words, if a jury finds the defendant's leaks justified. David Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review,* Vol. 127, p. 600. https://harvardlawreview.org/wp-content/uploads/pdfs/vol127_pozen.pdf (Downloaded March 15, 2019)

99 Charlie Savage, "Whistle-Blower on N.S.A. Wiretapping Is Set to Keep Law License," *The New York Times,* July 12, 2016. https://www.nytimes.com/2016/07/13/us/politics/thomas-tamm-nsa-wiretapping-law-license.html (Downloaded March 15, 2019)

100 "Report And Recommendation Of Hearing Committee One: Approving Petition For Negotiated Discipline," *in the matter of Thomas M. Tamm*, No. 16-ND-004 (D.C. Court of Appeals, Board on Professional Responsibility), July 11, 2016. http://www.abajournal.com/files/ThomasTammReport.pdf (Downloaded March 15, 2019)

101 10 U.S.C. § 1034(a)(1)

102 10 U.S.C. § 1034(b)

103 A military survey noted that 40 percent of respondents indicated they were retaliated against for reporting sexual assault. Office of People Analytics, *2016-2017 Military Investigation and Justice Experience Survey Overview Report*, January 2018, p. 75. https://www.dmdc.osd.mil/appj/dwp/rest/download?fileName=2017_MIJES_Report.pdf&groupName=pubSurSur (Downloaded March 19, 2019)

104 "Certain threats" includes threats that indicate "a determination or intent to kill or cause serious bodily injury to members of the armed forces or civilians or damage to military, Federal, or civilian property." 10 U.S.C. § 1034(c)(2)

105 10 U.S.C. § 1034(b)(2)(A); Note that unlike the Whistleblower Protection Act, the Military Whistleblower Protection Act includes retaliatory investigations as a prohibited practice. It defines a retaliatory investigation as "an investigation requested, directed, initiated, or conducted for the primary purpose of publishing, harassing, or ostracizing a member of the armed forces for making a protected communication."

106 50 U.S.C. § 3341(j)

107 *Department of the Navy v. Egan*, 484 U.S. 518 (U.S. Sup. Ct.1988)

108 Judicial Proceedings Panel, *Whistleblower Statutes for DoD: Military vs. Civilian Federal Employee Protections*, December 4, 2015. p. 1. http://jpp.whs.mil/Public/docs/03_Topic-Areas/06-Retaliation/20151211/02_Chart_WhistleblowerProtections_Military_v_FedCivEmployees.pdf (Downloaded March 16, 2019)

109 10 U.S.C. § 1034(c)(4)(A)

110 10 U.S.C. § 1034(d)

111 10 U.S.C. § 1034(e)(3)(A)

112 10 U.S.C. § 1034(c)(4)(E)

113 10 U.S.C. § 1034(e)(1)

114 10 U.S.C. § 1034(f)(1)

115 10 U.S.C. § 1034(f)(3)

116 Danielle Brian and Mandy Smithberger, "How The System Went After a War Hero: Jason Amerine Goes to Washington," *War on the Rocks*, December 10, 2015. https://warontherocks.com/2015/12/how-the-system-went-after-a-war-hero-jason-amerine-goes-to-washington/ (Downloaded March 6, 2019)

117 Jeff Stein, "Controversial Green Beret Retires Quietly with High Award," *Newsweek*, October 31, 2015. https://www.newsweek.com/controversial-green-beret-retires-quietly-high-award-389282 (Downloaded March 6, 2019)

118 Dan Lamothe, "Investigation clears Army of retaliating against Green Beret whistleblower, but scrutiny remains," *Washington Post*, September 3, 2015. https://www.washingtonpost.com/news/checkpoint/wp/2015/09/03/investigation-clears-army-of-retaliating-against-green-beret-whistleblower-but-the-scrutiny-isnt-over/ (Downloaded March 6, 2019)

119 Rebecca Jones, "Revoking Clearances on a Whim Hurts Whistleblowers—and the Rest of Us," Project On Government Oversight, September 14, 2018. https://www.pogo.org/analysis/2018/09/revoking-clearances-on-a-whim-hurts-whistleblowers-and-the-rest-of-us/

120 10 U.S.C. § 1034(h)

121 Between September 2012 and March 2016, the Defense Department Inspector General substantiated .9% of military whistleblower retaliation claims and the military branch inspectors general substantiated, on average, 5.9%. This averages to 3.4% of military reprisal claims substantiated in that time-period. Project On Government Oversight, "Table created by the for the House Oversight and Government Reform Subcommittee on National Security hearing on 'Oversight of the Department of Defense Office of Inspector General's Military Whistleblower Reprisal Investigations,'" September 7, 2016. http://www.pogoarchives.org/m/wi/pogo_testimony_appendix_a.pdf

122 The Defense Department Office of Inspector General told the Project On Government Oversight in an email that it has yet to use the authority.

123 391 U.S. 563 (U.S. Sup. Ct. 1968)

124 Public Employees for Environmental Responsibility, "State Watch.". https://www.peer.org/state-federal-watch/state-watch/ (Downloaded March 19, 2019)

125 The Occupational Safety and Health Act, as amended. 29 U.S.C. Ch. 15 § 651 et seq.

126 Workplace Fairness, "Environmental Whistleblowers – Occupational Safety and Health Act." https://www.workplacefairness.org/environmental-whistleblowers#2 (Downloaded March 3, 2019)

127 Sarbanes-Oxley Act of 2002 (Public Law No. 107-204), July 30, 2002. https://www.govinfo.gov/content/pkg/PLAW-107publ204/html/PLAW-107publ204.htm (Downloaded March 19, 2019)

128 FDA Food Safety Modernization Act (Public Law No. 111-353), January 4, 2011. https://www.govinfo.gov/content/pkg/PLAW-111publ353/pdf/PLAW-111publ353.pdf (Downloaded March 19, 2019)

129 The Consumer Product Safety Improvement Act (Public Law No. 110-314), August 14, 2008. https://www.govinfo.gov/content/pkg/BILLS-110hr4040enr/pdf/BILLS-110hr4040enr.pdf (Downloaded March 19, 2019)

130 *Mt. Healthy v. Doyle School District,* 429 U.S. 274 (U.S. Sup. Ct. 1977)

131 403 U.S. 388 (U.S. Sup. Ct. 1971)

132 462 U.S. 367 (U.S. Sup. Ct. 1983)

133 5 U.S.C. §2302(b)(12)

134 547 U.S. 410 (U.S. Sup. Ct. 2006)

135 42 U.S.C. § 1983, commonly referred to as "Section 1983."

136 *Van Ee, Jeffrey v. EPA, et al*, 202 F.3d 296 (D.C. Cir. 2000) https://law.justia.com/cases/federal/appellate-courts/cadc/99-5147/99-5147a-2011-03-24.html (Downloaded March 14, 2019)

137 *Van Ee, Jeffrey v. EPA, et al*, 202 F.3d 296 (D.C. Cir. 2000) https://law.justia.com/cases/federal/appellate-courts/cadc/99-5147/99-5147a-2011-03-24.html (Downloaded March 14, 2019)

138 *Van Ee, Jeffrey v. EPA, et al*, 202 F.3d 296, 302 (D.C. Cir. 2000) https://law.justia.com/cases/federal/appellate-courts/cadc/99-5147/99-5147a-2011-03-24.html (Downloaded March 14, 2019)

139 Public Employees for Environmental Responsibility, "Federal Employees 'Un-Gagged'," *PEEReview,* Spring 2000, p. 5. https://www.peer.org/assets/docs/PEEReview_Spring_00.pdf (Downloaded March 14, 2019)

Notes

DECIDING TO BLOW THE WHISTLE ON WRONGDOING CAN BE THE SINGLE MOST IMPORTANT PROFESSIONAL DECISION YOU MAY EVER HAVE TO MAKE.

Brave individuals who have exposed abuses of power have changed the course of history with their disclosures. They have saved lives, prompted lasting government reforms, and strengthened our democracy.

WHISTLEBLOWING, HOWEVER, IS RISKY AND DIFFICULT. History also shows it is an act usually best done while attempting to keep your identity anonymous to your workplace and the public at large.

This survival guide covers what federal sector employees should consider before potentially blowing the whistle.

A COLLABORATION OF

PROJECT ON GOVERNMENT OVERSIGHT
GOVERNMENT ACCOUNTABILITY PROJECT
PUBLIC EMPLOYEES FOR ENVIRONMENTAL RESPONSIBILITY