Leaking: practicalities and politics

Brian Martin[1]

WHEN you want to reveal information in the public interest, consider leaking. To be effective, you need to be very careful and to understand both practical and political aspects.

Whistleblowing is speaking out in the public interest, for example about corruption, abuse or hazards to the public. Most whistleblowers reveal their identity, and many suffer reprisals. Therefore, in many situations it is more effective to remain anonymous and leak. This can be called anonymous whistleblowing or public interest leaking.[2]

There is a serious double standard in leaking. Many politicians and top bureaucrats leak information to the media, often for personal gain or to sound out policies. Such leaks are seldom investigated and never prosecuted even when they are illegal.[3] However, when lower-level workers leak, this is commonly portrayed as a serious transgression and sometimes investigations are undertaken to identify the leaker. One of the main purposes of such investigations is to deter other workers from becoming leakers. It may be the only reason.

The focus here is on leaking in the public interest. It can be a powerful way to challenge damaging and dangerous activities carried out in secret. There are three main reasons why it can be worthwhile for whistleblowers to remain anonymous. First, reprisals are less likely: if authorities do not know your identity, they can't take action against you. Many whistleblowers who reveal their identity are met with petty harassment, ostracism, assignment to trivial duties, assignment to onerous duties, hostile rumours (for example of poor performance, crimes, mental disorder or sexual activities), forced transfers, reprimands, referral to psychiatrists, demotions, dismissal and blacklisting. After reprisals begin, life becomes very difficult. Many whistleblowers suffer in their careers, their finances, their health and their relationships. Therefore, it is better to avoid reprisals if at all possible.

Second, remaining anonymous means you can stay on the job and continue to collect information and leak. As soon as you are identified, your access to sensitive information will be blocked. Furthermore, efforts will be made to hide or destroy information about wrongdoing.

Third, by remaining anonymous, attention is more likely to be on the issues revealed than on the person making the claims. Employers prefer to turn the spotlight on whistleblowers, including their personalities and alleged flaws, as a means of distracting attention from wrongdoing.

Even if you decide to reveal your identity, it is often worthwhile waiting for months or even years while you collect plenty of information. As a rule of thumb, you need ten times as much information as you think you do. This is because wrongdoers will try to discredit you and the information in every way possible. For example, they will deny authorship of documents, say their words were taken out of context, say the policy wasn't actually implemented, or that they were joking.

Another advantage in waiting is that you are less likely to be suspected of being a potential whistleblower.

If you decide to serve the public interest by collecting information and making it available to outsiders, you need to approach this task with great care. You are undertaking a vital activity, but it is likely that opponents will try to discredit or even destroy you. So you need to learn how to be effective.

Whistleblower protection

In Australia, there are various laws intended to protect whistleblowers when they make "public interest disclosures." In some cases, giving information to journalists or activists is legally protected. However, in practice, employers often treat whistleblowing as illegitimate, even when it is entirely lawful.

Legal protection is not a guarantee against reprisals. Furthermore, employers are almost never held to account for taking reprisals against whistleblowers, even when they are supposed to be protected legally. The lesson here is not to rely on whistleblower laws: they may give only an illusion of protection.[4] This is why remaining anonymous is often a better option.

An illusion of protection

---

[1] Vice president, Whistleblowers Australia; Professor of Social Sciences, University of Wollongong. Email: bmartin@uow.edu.au, web: http://www.bmartin.cc/.

For useful comments, I thank AJ Brown, Kathy Flynn, Simon Frew, Brendan Jones, Cynthia Kardell, Ted Mitew, Ben Morris and others who prefer to remain anonymous.

[2] This article draws on ideas in Brian Martin, *Whistleblowing: A Practical Guide* (Sparsnäs, Sweden: Irene Publishing, 2013), chapter 8. Available at http://www.bmartin.cc/pubs/13wb.html

[3] David E. Pozen, "The leaky Leviathan: why the government condemns and condones unlawful disclosures of information," *Harvard Law Review,* vol. 127, 2013, pp. 512–635, describes the US federal government's tolerance of leaking by high-level officials, especially in the area of national security.

[4] Brian Martin, "Illusions of whistleblower protection," *UTS Law Review,* No. 5, 2003, pp. 119–130.

Even though many employers do everything they can to discredit and undermine whistleblowers, there is considerable support in the wider community for speaking out in the public interest. By acting responsibly — for example, limiting damage to third parties — whistleblowers can maximise their credibility with co-workers and wider audiences. It is valuable to remember that whistleblowing is about serving the public interest, not personal agendas. If you are doing this, you deserve support and admiration. When your employer initiates reprisals, it is valuable to remember that you are doing the right thing.

Problems and penalties

In every part of society, there are problems that need to be addressed. They include business swindles, hazardous chemicals, abuse of people with disabilities, paedophilia in the churches (and elsewhere), harm to prisoners, tax rip-offs, nepotism, unfair tax laws, environmental damage, and a host of others. All deserve attention and action.

Perpetrators usually prefer to operate in secret. Whistleblowers, whether they are open or anonymous, can play an important role in exposing the problems. Sometimes, disclosures cause wrongdoers to halt their activities.

The risks from speaking out are much greater in some areas than others. Probably the most risky areas are organised crime, the military, the police and national security. The problems are not necessarily more serious, but the power of the wrongdoers to impose reprisals is much greater.

National security is an exceptional case, because governments have enormous power and can use it to abuse human rights and avoid accountability. Anti-terrorism laws give governments power against dissent that is far beyond what is warranted by the dangers involved. For example, some pharmaceutical drugs, with known dangers, cause tens of thousands of deaths, far more than the death toll from terrorism.[5] Yet the penalties for challenging anti-terrorism laws far exceed the penalties for speaking out about crimes by the pharmaceutical industry.

When penalties for dissent are excessive, it is all the more important to reveal problems, and to do so with the greatest care. To be effective in exposing problems, it is worthwhile learning from dissenters and opposition movements in repressive regimes.

The Australian national-security connection

In 2014, the Australian government passed draconian anti-terrorism laws with extreme penalties for whistleblowers and journalists — up to ten years in prison — who reveal information on certain national security matters. Whether these laws will actually be used remains to be seen, but they are obviously intended to deter public interest leaking and reporting. They will also enable abuses to be committed with impunity and hence make exposure even more important.

Whistleblowers in other fields seldom face such extreme penalties, but speaking out still can be risky. There is much to learn from the challenges facing dissidents in high-security areas.

Learning from challenges to repressive regimes

Many governments in the world are highly repressive. They do not allow dissent, and may harass, arrest or even kill opponents. Despite the dangers, courageous citizens take action in support of political freedom. It is possible to learn from these challenges to repressive regimes.[6]

Repressive regimes often provide some official means for citizens to express discontent. It is possible to write to the government, though this seldom has any effect. Often there are elections, but these are rigged. Often most of the mass media are controlled by the government, or limited in what they can say. Information about alternatives is restricted. Trying to change the system by lobbying or voting is fruitless.

The most effective challenges to such governments involve a wide range of non-standard methods of action, such as rallies, strikes, boycotts and occupations. Campaigns relying on such methods are more effective than armed struggle.[7] There are several features of such campaigns worth noting.

Protesters in Peru, 2011

Widespread participation in actions is important. Mass rallies are one example. However, when joining a rally is too risky, there are other options. In Turkey in 1997, at the initiative of the Citizens Initiative for Constant Light, at a particular time in the evening people turned off their lights as a symbol of resistance. In Poland under military rule, the government's official news was broadcast at 7pm. To express their opposition in a safe way, many citizens went for a walk at this time, some with their televisions in prams. The more repressive the regime, the more important it is to find methods of opposition that involve only a small risk, so many people can join.

It is also important that many different sectors of the population participate. If the opposition is based on a single group, such as students or workers, it cannot easily build into a mass movement. Involving different groups also brings in more ideas about resistance, making the movement more flexible and creative.

Campaigns against repression need to be resilient: they need to be able to survive government attacks. One implication is not to depend too much on leaders, who can be discredited, arrested or even killed. A decentralised, network-based system for decision-

[5] Peter C. Gøtzsche, *Deadly Medicines and Organised Crime: How Big Pharma Has Corrupted Healthcare* (London: Radcliffe, 2013).

[6] See "Resisting repression: resources for defending Australian freedoms," www.bmartin.cc/dissent/documents/rr/.

[7] Erica Chenoweth and Maria J. Stephan, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (New York: Columbia University Press, 2011).

making and action is better for survival. Large organisations, with investments in facilities, staff positions and official credibility, have more to lose and can more easily be harassed.

Alliances are crucially important. Governments often use divide-and-rule techniques. They demonise certain sectors of the population, such as trade unionists, religious minorities or students, sometimes labelling them terrorists or subversives, and attack them directly or via proxies. Other sectors of the population, rather than support the targeted group, instead look to the government for protection, thereby cementing its power.

In this context, whistleblowers can play a valuable role. Those who are inside the government apparatus, for example in the police, military or security services, can provide information to opposition groups. Useful sorts of information include evidence of government abuses, plans and methods. For example, when opposition groups know about government plans to infiltrate and discredit them, they can better prepare their actions and systems.

Dissent is risky

In a repressive regime, speaking out can be very risky, potentially leading to arrest and imprisonment or worse. In less repressive places, there is greater tolerance for free speech and political protest. Yet speaking out can still be risky. The greatest danger is from employers.

Large organisations, such as government departments, corporations and churches, are usually structured on the principles of hierarchy and division of labour, in a form that sociologists call bureaucracy. The military is a classic bureaucracy, with a rigid line of command. In a bureaucracy, workers are interchangeable cogs.

Large organisations like this are undemocratic.[8] There is little or no free speech. Leaders are not accountable through elections, and opposition movements are often not allowed. Basically, a large bureaucratic organisation is similar to an authoritarian state.[9] This helps explain why whistleblowing is so risky. A whistleblower is similar to a lone political dissident in a repressive regime, which is why whistleblowers can learn from techniques for political dissent.

Imagine standing alone against a dictator — it's brave, but seldom a good strategic move. It's usually more effective to be part of a movement for change. When you have allies, you are safer and there's a better prospect of success. There is strength in numbers, and also many more skills, resources and contacts.

If there is an organised opposition movement within your workplace, this is a good place to seek allies. If not, then look outside the organisation, for example to action groups on the environment, health, honest government, human rights, social justice or whatever is most relevant.

If you are on the inside, with information, and others are on the outside, with resources and capacity to take action, you can contribute most by linking up with those on the outside. By remaining anonymous, you can provide information on an ongoing basis.

When leaking is not a good idea

Leaking is only possible and suitable in certain circumstances.

• If you've already spoken out, and especially if you've already suffered reprisals, you have limited opportunities for obtaining inside information and leaking it anonymously. So being public might be better.

• If you are the only person with certain information, you probably won't be able to remain anonymous: you will be identified immediately. So it might be better to gather more information before leaking, or first obtain a new job.

• To be an effective leaker, you need to be an actor: you need to behave like you do normally. If there is a witch-hunt for the leaker, you need to pretend that you are not the leaker, and to tell lies if necessary. If you're not able or comfortable doing this, leaking may not be for you. To be really effective, you may need to join the search for the leaker and even contribute ideas to how to track down the leaker.

• Sometimes leaking may put you and others close to you in serious danger. In such situations, you need to balance benefits and costs, and consider different strategies.

Strangely enough, when the danger is high, it may be safer to reveal your identity, because more people will know you have spoken out and will be aware if anything is done to you. For example, sometimes witnesses to crimes by criminal syndicates are put in supposedly safe locations under police protection. But if the criminals have infiltrated the police, then your life can be in danger and no one will know. If you are a public face, you might actually be safer.

Who can receive leaks

There are several potential recipients: journalists, activists, WikiLeaks and similar services, and the public directly.

Journalists can use your information to write stories and publicise problems. You can remain completely anonymous by sending material by email or post, or you can talk via a safe phone, or you can agree to meet. How much personal contact you make with the journalist depends on several factors, including how much you trust the journalist, how risky it is for you to have your identity known to anyone, and how much you want to build a relationship for ongoing leaks.

The best sort of journalist to contact is one who has a good reputation and a track record of exposing problems. It is important to remember that journalists

[8] Bruce Barry, *Speechless: The Erosion of Free Expression in the American Workplace* (San Francisco: Berrett-Koehler, 2007); David W. Ewing, *Freedom Inside the Organization: Bringing Civil Liberties to the Workplace* (New York: Dutton 1977).

[9] Deena Weinstein, *Bureaucratic Opposition: Challenging Abuses at the Workplace* (New York: Pergamon, 1979)

and their editors seek stories they judge newsworthy, for example involving conflict, personalities, local relevance and current events. If your material is too old, too technical, too complicated or too risky — risky because it might open the news outlet to legal or government reprisals — then there may be no story, or only an inadequate one. Look at what other stories have been run to see whether your material fits the usual mould.

An inexperienced or careless journalist may compromise your identity. Many journalists are seriously overloaded and therefore may not have the time to give your story the attention, care and security precautions it deserves.

If you have an ongoing relationship with a journalist, you should arrange codes and communication systems in case of danger, for example to cancel meetings at short notice or even to shut down contact altogether. Multiple methods of contact, for example email accounts in different names, can be useful.

Journalists should copy printed documents received and destroy originals, and similarly transform electronic files to eliminate identifying information, for example by putting them into plain text. Journalists should not keep files on site that can be obtained through a search warrant.

In Australia, anti-terrorism laws may deter journalists from covering some national security stories. One alternative: go to international media. Or go to activists, use leaking sites or publish the material yourself.

Activists can use your information in several ways. By providing insights into how your organisation works, they can better plan their campaigns. For example, if they know there are differences of opinion, or discontent, in your organisation, activists may be able to propose options or design protests more effectively. Especially important to activists is information about the impact of their campaigns.

What sort of activist group? It depends on where you work. There are groups concerned about education, human rights, environment, labour, peace, welfare and a host of other issues. However, sometimes there's no suitable group.

Activists are less likely to be familiar with using leaked information. They may not have good systems to protect your identity. Proceed cautiously. It's probably better to approach an individual with a lot of experience, and someone with a reputation for maintaining confidentiality.

Remember that most people like to gossip. Knowing about a leaker may be a secret that is too hard for some to keep to themselves. If in doubt, don't reveal your identity. You can be an effective leaker by sending messages from an anonymous email account or putting documents in a mailbox.

Remember also that activists may be suspicious of you. They may worry that you are a government agent trying to mislead or entrap them. So proceed gradually, and provide information to establish your credibility. Or try one of the other options.

Leaking sites are a good option if you have important documents. A well-designed leaking site, like WikiLeaks, provides strong protection that your identity will not be revealed. Not all sites do this, so check out the site carefully. Another well established leaking site, predating WikiLeaks, is Cryptome.

Leaking sites may or may not give your material wider visibility. Too often, material just sits on the site and no one notices. So you may need to contact journalists or activists to let them know about the documents.

Direct publication: you can post material online. You can set up a website, a Facebook page or a blog, or you can put documents on a site like Scribd. Then you can notify journalists or activists or go directly to your target audience. For example, if you have email addresses, you can send messages to members of an organisation. The advantage of posting material — documents or written commentary or both — is that you control exactly what you want to say, without relying on journalists or activists as intermediaries.

Choose recipients of your leaks very carefully. You may need to take as much care in selecting and cultivating journalists or activists as you do gathering material to give to them. Edward Snowden gathered a vast quantity of data about the US National Security Agency's spying operations, but that was the easy part. He carefully selected the journalist he wanted to receive the documents and then spent months trying to interest him in the story. His efforts paid off in the biggest stories imaginable. The lesson is to be selective in choosing recipients and to be patient and persistent in building a relationship with them.[10]

Remaining anonymous

Leaking may seem dangerous because we read about leakers who were exposed, most famously Daniel Ellsberg and Chelsea Manning. Most leakers, however, remain anonymous as long as they want to — so we never hear about them.[11]

---

[10] Brian Martin, "Learning from Snowden," http://comments.bmartin.cc/2014/06/26/learning-from-snowden/. For informative accounts of Snowden's experience, see Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (London: Hamish Hamilton 2014); Michael Gurnow, *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal* (Indianapolis: Blue River Press, 2014); Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (London: Guardian Books 2014).

[11] On leaking, see *The Art of Anonymous Activism: Serving the Public While Surviving Public Service* (Washington, DC: Project on Government Oversight; Government Accountability Project; Public

Remaining anonymous is possible, but it takes care, especially if you work in a sensitive area where security is taken seriously. Because each situation is different, there are no general rules about how cautious you need to be. What is important is to think through how others might track you down. Imagine that your boss, a workmate or an outside investigator were given the task of finding the leaker. What would they do? Or imagine that you were assigned the task of finding a leaker. How would you proceed? By thinking through steps likely to be taken, you have a better chance of avoiding traps.

Suppose the investigator goes into your computer and checks all your files and goes into your email account and checks all your messages. That means you shouldn't leave any trace of your activity on your computer or email. So pay cash to buy a cheap computer, for example a tablet or netbook. Make sure it is not connected to the web, disable GPS and do all your writing on it.

Buy a cheap tablet.

Go to a public computer (in a library or cafe) far from your home, taking along a USB from your separate computer, and send emails from a new email account. Or use free wifi in a busy place.[12] Avoid using social media during this time, as it can compromise your anonymity.

If you plan to send files, avoid standard word-processing software; use secure open-source software instead, or put text into the body of emails. If you want to be ultra-cautious, hand-write your message and key it in at a public computer. Avoid locations where your presence can be recorded on closed-circuit TV monitoring and avoid carparks where your car's licence number might be recorded. If you're not sure about the location of security cameras, you can reduce risk by wearing sunglasses and a hat — as long as this doesn't make you more conspicuous. If you're having an ongoing conversation with a journalist, use a different public computer each time.

Suppose you've made a major leak and there's a massive hunt for the leaker. The police go into your house and take all your electronic devices — phones and computers. By this time you should have deleted all incriminating files from your computer, using a secure-delete function so even an expert cannot recover files. Even better, after deleting the files, you dispose of the separate computer entirely. Your regular home computer should never contain material relevant to your leaking.

Suppose the investigator obtains telephone company records and looks for a record of a call to a journalist or other recipient. You need a phone connection that can't be linked to you. So use public phones or arrange to use a secure open-source messaging system — not Skype — from a public computer (voice or text message only). Even safer is to avoid calls altogether, instead sending quick emails so your time online is limited.

If you want to copy documents, you need to be careful. Some photocopiers can be set up so that every copy has an identifying mark. So use a public photocopier, or make multiple copies using several different photocopiers.

Even more devious is a process sometimes used for highly sensitive documents. Each recipient's copy has a slight difference in the text — for example, an insignificant word is replaced by a synonym — so that if the document is leaked, the leaker can be identified. This level of monitoring is unusual.

Usually you will not have to deal with sophisticated defences against leaking. At some national security offices, security is so lax that it's possible to obtain paper or digital files with ease.[13]

Very few police dogs are trained to detect USB drives.

A more common problem you will face is avoiding making simple mistakes. Many leakers are caught because they leave pages in the photocopier or leave their computer monitors open to confidential documents, or send emails from their work computer. If you avoid simple mistakes, you are pretty likely to be safe.

The same principle applies to online precautions: use methods with which you are familiar and comfortable, because you are less likely to make mistakes. If you've never used encryption, VPN or open source software, don't start just before you begin leaking. Instead, learn how to use these techniques well in advance, or just use something you've used before. Meeting a contact face-to-face, away from electronic devices, remains a dependable way of avoiding surveillance; arranging such meetings is the hard part.

Often it is better to leak information bit by bit, over a period of time, rather

Employees for Environmental Responsibility, 2002), especially pp. 7–16; Kathryn Flynn, "The practice and politics of leaking," *Social Alternatives,* vol. 30, no. 1, 2011, pp. 24–28; Nicky Hager and Bob Burton, *Secrets and Lies: The Anatomy of an Anti-environmental PR Campaign* (Craig Potton, 1999), pp. 240–247. All available at http://www.bmartin.cc/dissent/documents/rr/.

[12] For even greater security, use a live USB-only operating system such as Tails (https://tails.boum.org/) and, for continuous posting, a VPN that doesn't collect data logs.

For keeping Internet activity anonymous, you can use Tor (https://www.torproject.org/) and use an anonymous email site such as hushmail (https://www.hushmail.com/), not including any personal information. Spies can use network analysis to track the source of ongoing communication, so be careful about this approach for more than occasional use.

[13] For a revealing account, see Sibel Edmonds, *Classified Woman: The Sibel Edmonds Story. A Memoir* (Alexandria, Virginia: Sibel Edmonds, 2012).

than in one giant batch. When journalists or other recipients write stories, the publicity may encourage others to confirm information or leak new material, so the area of suspicion is diffused and investigators are confused. Furthermore, a drip-by-drip leaking strategy can lead to greater publicity, as stories continue to appear. Snowden's revelations had a greater impact because they were gradually revealed over weeks and months.

Another way you can be identified is through your words and behaviour. Ask an honest friend how good you are at keeping confidences. Chelsea Manning, who obtained and leaked one of the biggest collections of documents in history, may never have been caught except for talking about it. The lesson is to never tell anyone that you are the leaker — except maybe years or decades later when there is no risk.

After you have leaked, you need to pretend that you are not the leaker. You need to behave just as you would if you hadn't been the leaker. This is a form of acting. Contrary to popular opinion, research shows that most people can lie convincingly and that few people can detect lies, so you can probably do it well, especially if you believe in what you are doing.[14] It is legitimate to lie in a good cause, for example in occupied Europe during World War II when Nazis came to people's houses asking whether there were any Jews inside.

Pinocchio hides his revealing nose

Think through in advance how you would behave if you were told that someone else had leaked information from your section. (Maybe they did!) Then be prepared to act in the same way if you are the leaker. If you are convincing, you might even be put in charge of finding the leaker! Be careful. Sometimes workers suspected of being leakers are sent material or given tasks as a means of trapping them, or sending them a warning.

If you are discovered

If your identity as the leaker becomes known, you are likely to be subject to reprisals. If you are in a dangerous area, such as organised crime, police or military, you might be at risk of assault, frame-ups and imprisonment.

If you expect reprisals to be severe, it is often better to get out and go public. Accept that your career is over, leave the job (and avoid immediate reprisals), let everyone know you are a whistleblower and seek public visibility.

Andrew Wilkie worked for the Office of National Assessments. In March 2003, he publicly questioned the Australian government's rationale for joining the invasion of Iraq. Wilkie didn't bother complaining to his bosses or making an official disclosure. Instead, he went straight to the media with his message, resigning from his job. Wilkie was courageous in speaking out, sacrificing his career. He had maximum impact and avoided reprisals inside ONA. He could have been charged with a crime and gone to prison. Because he became well known — and gained many supporters — the government decided not to prosecute him.

Andrew Wilkie

The lesson from Wilkie's experience is that to have maximum impact and reduce reprisals, resign and seek publicity and public support.[15] Don't rely on protection from whistleblower laws. They seldom work and often serve to reduce exposure of problems.

Many Australian public servants are afraid of speaking out because of the harsh laws against unauthorised disclosures, but these laws are hardly ever used. They serve mostly to scare workers into silence. You may be safer than you realise.

Conclusion

Secrecy is justified as protecting the public, but often it serves to protect powerful groups from scrutiny, and sometimes is a cover for crimes and abuse. In such circumstances, exposure is a public service.

If you're going to expose problems, leaking can be the best option, especially when you can remain in the job and continue to leak. To leak effectively, you need to be cautious and patient, perhaps waiting months or even years after collecting information. You need to choose your recipients very carefully. You need to continue in your job just as you would if you were not the leaker. You need a plan to minimise potential damage to the recipient of your disclosures in case of discovery. If you are discovered, you need to be prepared to resign and go public.

As a leaker through all this, you will obtain no recognition — no praise from bosses or co-workers, and no personal publicity. You need to be satisfied in your mind that you are doing the right thing. Sometimes that is the greatest reward.

Postscript

This is a work in progress, and is likely to become out of date in light of technological developments. If you have comments on how to improve this document, please let me know (see footnote 1). You are welcome to circulate it, especially to potential leakers. A separate pdf is available at www.bmartin.cc/dissent/documents/rr/ in the section on leaking.

[14] Paul Ekman, *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage* (New York: Norton, 2009).

[15] Brian Martin, "Bucking the system: Andrew Wilkie and the difficult task of the whistleblower," *Overland,* No. 180, Spring 2005, pp. 45–48, www.bmartin.cc/pubs/05overland.html.