Chapter 12

Strategy for public interest leaking

Brian Martin

Introduction

Speaking out in the public interest – being a whistleblower – can be risky. The classic example is an employee who learns about corruption, abuse or dangers to the public and tells the boss. Such employees are often subject to reprisals, including reprimands, harassment, ostracism, assignment to onerous duties, assignment to trivial duties, referral to psychiatrists, demotion, dismissal and blacklisting. These are all-too-common responses to whistleblowing.[1] Sometimes whistleblowing is welcome; for example, when it exposes a problem that can be fixed to the organisation's benefit. But when senior managers are implicated in the problem, whistleblowers may be treated as traitors.

Many whistleblowers start by informing their bosses of the problem. Indeed, many do not even think of themselves as whistleblowers, rather as workers just doing their jobs. After receiving an inadequate response or experiencing reprisals, many then take their message to other audiences, usually watchdog bodies such as ombudsmen, auditors-general and anti-corruption agencies. Although these bodies sometimes help, a great deal of the time they do not.[2] Whistleblowers then sometimes go to the media, which provide a powerful avenue for exposing problems, although whistleblowers themselves may still pay a serious price for their actions.

Not only do whistleblowers often suffer reprisals, but in most cases speaking out does not fix the problem. Employers and agencies orient attention towards the whistleblower. During the months and years that the whistleblower makes complaints to various agencies, the original problem remains unaddressed. Furthermore, as soon as a whistleblower speaks out, managers can take action to hide evidence of the problem or of their own complicity in it.

There are, thus, quite a number of reasons why whistleblowing can be a poor strategy for addressing problems: it leads to reprisals, it alerts management so responsibility can be avoided, and it delays fostering the wider awareness that is often the only lever powerful enough to bring about change.

In this context, there are advantages to a slightly different strategy, which can be called 'anonymous whistleblowing' or 'public interest leaking'. Instead of making

his or her identity known, the employee remains anonymous, providing information and documents to outsiders. This has the great advantage of avoiding reprisals, at least so long as anonymity is maintained. Another advantage of anonymity is that the focus is more on the leaks than the leaker; in contrast, non-anonymous whistleblowers are often the centre of attention, rather than their disclosures. Finally, anonymous whistleblowers can remain on the job and continue to gather and leak information, whereas whistleblowers who reveal their identity are often immediately cut off from sources of information and are sometimes dismissed.

Public interest leaking has gained tremendous visibility due to WikiLeaks. The spectacular releases by WikiLeaks – especially the 'collateral murder' video, the Afghanistan and Iraq war logs, and the US diplomatic cables – have attracted widespread media coverage, overshadowing WikiLeaks exposés on other topics, such as Guantánamo detention camp procedures and elite corruption in Kenya. Public interest leaking drew further attention after revelations of the US National Security Agency's (NSA's) vast surveillance operations, based on documents leaked by NSA contractor Edward Snowden to *The Guardian* in 2013. However, public interest leaking is not new. The most famous pre-internet public interest leaker is Daniel Ellsberg, who leaked the Pentagon Papers, a history of US military involvement in the Vietnam War, to *The New York Times*.[3] There are many other cases, but few of them are documented, precisely because the leakers have remained anonymous and their personal stories have never been told.

The focus here is on leaking in the public interest. However, most leaking, by politicians and government officials, is to serve private interests or advance political goals. For example, politicians will tell journalists about party room discussions in order to hurt rivals, support allies or affect the public agenda. Politicians or senior bureaucrats will tell business executives about government plans to give advantages to favoured companies, sometimes reaping a political favour or pay-off. Senior bureaucrats may leak plans for new policies to test public reaction. Leaking in the public interest, in contrast, is usually by lower-level employees and serves neither the personal interests of the leaker nor the agendas of politicians and top bureaucrats.[4]

Surprisingly, there are very few studies of public interest leaking. Kathryn Flynn tells of a group of Australian government employees concerned about fraud in the national health insurance system who, knowing that their concerns would not be acted upon by senior officials or politicians, regularly leaked information to the media, generating pressure for action.[5] Her study is a reminder that leaking is not always a solo activity, but can be collective and well organised.

In the next section, five common tactics used by managers and other opponents of whistleblowing are described. Only some of these tactics are easily applied to leakers. This analysis of tactics reveals the many advantages, as well as a few weaknesses, of leaking. This analysis is then applied to the experience of WikiLeaks, showing ways in which the operation has been effective and ways in which it has been targeted, with some suggestions for an improved strategy. Following that, the experience of Edward Snowden is examined similarly. The conclusion sums up lessons for public interest leakers and their supporters.

Tactics against whistleblowers

Many whistleblowers are conscientious employees who see something that might be a problem and report it in good faith to 'higher-ups', assuming the issue will be investigated and, if necessary, fixed. However, instead of addressing the complaint, all too often management shoots the messenger, visiting reprisals against the employee. From the point of view of outsiders, there are two potential injustices involved. The first is the corruption, abuse or public hazard about which the whistleblower speaks out; the second is the reprisals against the whistleblower, which often seem unfair.

When powerful groups do something that others see as unjust – for example, censorship, bullying, massacres of peaceful protesters, torture or genocide – the perpetrators often act in ways that reduce public outrage.[6] Five tactics are commonly used:

1 covering up the action;
2 devaluing the target;
3 reinterpreting what happened by lying, minimising the consequences, blaming others or reframing the perspective;
4 using official channels to give an appearance of justice;
5 intimidating people involved.

For example, these five methods were used by the US Government to reduce outrage from the torture and abuse of prisoners by US guards at Abu Ghraib prison in Iraq, revealed to the world in 2004. Before the exposure, the action by the guards was covered up. The prisoners were devalued by being labelled criminals and terrorists, so what was done to them seemed more acceptable. After the exposure, US officials downplayed the seriousness of the treatment, calling it 'abuse' rather than 'torture', and the media went along with this framing. The prison guards were blamed so higher officials could escape responsibility. The official charges against some of the guards gave the appearance of justice, while policies and responsible senior officials were left untouched. Some of those who helped to reveal the abuse were ostracised and threatened.[7]

It is plausible that these same five methods will be used against whistleblowers and their supporters, to reduce outrage over both the activities exposed by the whistleblower – corruption, abuse or hazards – and the reprisals taken against the whistleblower.

Cover-up is the first method.[8] Wrongdoers usually keep their activities hidden. This is precisely why whistleblowing is such a threat. In addition, some reprisals, such as ostracism and petty harassment, are subtle, difficult to document and therefore hidden from wider audiences. Other reprisals are more obvious, such as reprimands at meetings, and are intended to send a warning to other employees. Leakers, if they remain anonymous, avoid reprisals, so there are no reprisals to be covered up.

The second method is devaluation. Whistleblowers are commonly labelled as traitors, troublemakers or difficult personalities. Management may encourage

spreading of rumours that a whistleblower is a poor worker, thief or sexual deviant, among other derogatory allegations. Whistleblowers are often referred to psychiatrists, serving to cause humiliation and devaluation. When whistleblowers are anonymous, general negative labels, like 'traitor' or 'troublemaker', can be applied, but making specific allegations is less credible. Maintaining anonymity reduces the potency of devaluation.

Reinterpretation is the process of changing the meaning of actions. For example, corruption can be reinterpreted as acceptable business practice that does not hurt anyone, or it can be blamed on low-level operatives. Reinterpretation is commonly applied to reprisals against whistleblowers – for example, by denying that reprisals have occurred (in other words, lying), minimising their significance or blaming someone else. Disclosures by leakers are subject to the usual array of reinterpretations, for instance by claiming that what was revealed was an unusual occurrence, was actually an instance of best practice, or was due to a mistake. When there is an investigation to discover the identity of a leaker, this is commonly said to be motivated by a concern for privacy, confidentiality, proper procedures, security or public safety – anything except a desire to exact reprisals and prevent further disclosures.

Most whistleblowers report problems through official channels, typically to their bosses, senior management or watchdog agencies, such as ombudsmen. When they suffer reprisals, they often complain to the same sorts of agencies. Unfortunately, many whistleblowers find that official channels do not help. In one key study, whistleblowers reported that 90 per cent of their approaches to agencies did not help; moreover, some approaches made things worse.[9] Official channels, including whistleblower protection laws, give the appearance of dealing with these problems, but often do not. Furthermore, most official processes are slow, focus on procedural technicalities and rely on experts such as lawyers, all of which serve to reduce the potential for public outrage. One of the unanticipated consequences of whistleblower protection laws is that they encourage workers to report concerns and reveal their identity, opening them to reprisals, rather than publicising their concerns. In many cases, most of the attention is on dealing with claims about reprisals, so that the original issue – corruption, abuse or hazards – remains unaddressed.

The alternative for whistleblowers is to take their concerns to wider audiences, for example, by going to the media. Leaking as a strategy typically avoids the traps inherent in official channels and takes the message directly to outsiders.

The fifth method commonly used against whistleblowers is intimidation. This is most obvious in the reprisals taken against whistleblowers. The threat of reprisals serves to deter other workers from speaking out about the original issue or openly supporting the whistleblower. Leakers, if they remain anonymous, can avoid reprisals. However, witch-hunts for leakers, and reprisals visited on those who are identified, can serve as a powerful deterrent to others. That said, in some cases the unfairness of reprisals can operate to inspire action by witnesses. Leaking probably has a greater potential for encouraging emulation, because a leaker's success

provides a model to others, whereas the fate of non-anonymous whistleblowers is something co-workers seek to avoid.

In summary, employers have many more opportunities to exact reprisals when the identity of the whistleblower is known. Leaking, by this analysis, has many advantages. However, it is important to note several circumstances that make anonymity inadvisable or unfeasible.[10] First, in many cases, an employee is already known for speaking out, and thus is an obvious suspect when a leak occurs. This is the situation for many who do not initially think of themselves as whistleblowers: they raise an issue of concern, expecting it to be investigated and addressed, and discover to their dismay that they have become the target of attack. These are employees who thought they were just doing their job and inadvertently discovered or exposed something highly sensitive.

Second, if inside information is known only to a few individuals, leaking is risky because the source of the leak can be readily identified. Third, some individuals are not suited for covert operations. Being an effective leaker requires a capacity to keep a secret, cover one's tracks, disguise one's emotions, and sometimes to lie (in a good cause). If this causes great discomfort or is exceedingly difficult to carry out and maintain, then leaking may not be a suitable option. Fourth, some individuals are well protected from reprisals, so it may be better to speak openly and gain the extra credibility this sometimes entails. Often, this means they have obtained a new job in safe circumstances. Having a new job also means there are no further opportunities for leaking in the previous one. In such circumstances, the advantages of leaking are fewer and the benefits of being open can be greater.

These considerations suggest that leaking is unlikely to become the prime option for more than a minority of whistleblowers. Nevertheless, because it is such a potent method, with the possibility of ongoing action, it has the potential for much greater impact. With this background on the tactics relevant to leaking, it is useful to examine the experience of WikiLeaks, to show the relevance of this analysis to the world's most prominent formal system for public interest leaking.

WikiLeaks tactics

WikiLeaks was the first, and remains the most prominent, system for anonymous whistleblowing through a web interface. It is important to distinguish between leakers (who submit items to WikiLeaks) and WikiLeaks itself, which is more akin to a traditional editor and publisher.[11] Julian Assange, who set up WikiLeaks and is its most visible figure, is not himself a whistleblower. The most well-known person who has leaked information via WikiLeaks is Chelsea Manning (formerly Bradley Manning), whose identity became known not via WikiLeaks, but via another person, and who has received both condemnation and praise.

Analysing the tactics used in relation to WikiLeaks involves looking at methods used for and against Manning, Assange and the WikiLeaks operation. The five methods for reducing outrage from injustice are cover-up, devaluation, reinterpretation,

official channels and intimidation. It is useful to begin with intimidation because it has played such an important role in the story.

Manning has been subject to the most ferocious reprisals, including arrest, imprisonment and torture via solitary confinement and suicide-watch procedures.[12] As well as serving as punishment of Manning for her acts against the US state, these reprisals serve two other important functions. First, they send a signal to other potential leakers about the fate that awaits them. Second, they distract attention from the information that Manning revealed, including the 'collateral murder' video that exposed the casual killing of Iraqi civilians and the vast archives of war logs and diplomatic cables.[13] In the extensive media coverage of Manning's arrest, imprisonment and trial, the information exposed often is secondary to Manning's own story.

Assange is alleged to have committed rape in Sweden, and has been threatened with arrest and criminal prosecution in the US, with some US politicians calling for him to be assassinated. Then, there are the attacks on WikiLeaks as an operation. Internet service providers, including Amazon, withdrew services for WikiLeaks, and financial institutions – including Visa, Mastercard, PayPal and Bank of America – denied services to WikiLeaks, thereby making it difficult for members of the public to financially support WikiLeaks, a not-for-profit organisation largely funded by donations.[14] The US Department of Justice issued subpoenas to Twitter for all records concerning several people associated with WikiLeaks.[15]

Intimidation is a tool of direct attack and a method of reducing the expression of outrage over acts that might be considered unfair. In the case of WikiLeaks, some US Government intimidation has discouraged the expression of outrage. For example, financial institutions such as Visa seem to have been deterred from speaking out. On the other hand, intimidation itself can be a source of outrage, and this has been the case especially in the case of Manning, who has become a martyr in the eyes of many supporters.

Cover-up is a tactic commonly used to reduce outrage over injustice: if people do not know about something, they will not be upset about it. It is a primary means of curtailing awareness of criminal or disreputable US military and diplomatic activities. Cover-up commonly operates in layers, with a few core individuals having full information, others knowing less and yet others, further away from the core, knowing little or nothing or believing falsities. The outer layers normally rely on mass media coverage, so if the information is restricted to specialist outlets, a significant level of cover-up is achieved.[16]

In relation to stories broken by WikiLeaks, based on leaks by Manning, the US Government was unsuccessful in cover-up: the collateral murder video, war logs and the diplomatic cables were widely publicised via mass media collaborating with WikiLeaks. It is reasonable to presume that US agencies covertly pursued a wide range of methods of disrupting or shutting down the WikiLeaks operation. Overall, the role of cover-up in the attack on WikiLeaks was variable: some methods of attack were hidden, some were known in limited circles and some became more widely known.

Next is the tactic of devaluation: when a person or organisation is seen as low status, disreputable, criminal or deviant, then actions taken against the person or organisation do not seem as serious as they might otherwise. Although in principle 'murder is murder', most people are more upset by the murder of a respected physician than the murder of a paedophile. Therefore, the devaluation of targets of attack is predictable.

Devaluation is the most obvious tactic used against Manning, Assange and WikiLeaks. Manning has been called a traitor; Assange has been called a terrorist. As well as the outpouring of words by opponents of Manning and Assange, actions taken against them have served to demean and discredit them. Manning, by being held in a high-security prison, is implicitly portrayed as a terrorist; by being treated as suicidal, she was portrayed as unstable. Assange was devalued by the rape claims made against him; although his sexual activities in Sweden had no significant connection with his work with WikiLeaks, the allegations served to discredit him as a person.

Reinterpretation is a process of creating or fostering meanings, in this case to make the actions taken against Manning, Assange and WikiLeaks seem understandable, even virtuous. Four important methods of reinterpretation are: lying about what happened; minimising the impact of actions taken; blaming others; and framing events in a favourable manner. An example of lying is the claim that Manning's treatment in prison was for her own safety. An example of minimising was the claim by US officials that the treatment of Manning in prison did not amount to abuse or torture. The most important framing process was to present leaking, and the publishing of leaks, as a threat to national security and as putting named individuals in danger. All of these types of reinterpretation challenged or weakened the alternative interpretation – that WikiLeaks is a valuable contribution to society because of its exposure of corruption, abuse and government perfidy.

Official channels, such as grievance procedures, ombudsmen and courts, are supposed to be fair. People expect them to provide justice. However, when powerful groups are transgressors, official channels often give only the appearance of justice, with little or no substance.[17] Therefore, they can serve to dampen public outrage with minimal impact on the status quo. Whistleblowers commonly seek action via official channels, often trying one after the other, usually with little success.

In the case of WikiLeaks, no substantive action was taken about the problems revealed, for example by the collateral murder video. Outrage apparently was not great enough to stimulate official inquiries into the abuses revealed. Instead, official channels were used as a means of attack; Manning received a 35-year sentence, and Assange was sought for extradition over a rape claim. These actions would have had little credibility if not for their status as operations of the criminal justice system. Manning and Assange were treated as criminals, while the actions they exposed were exempted from proceedings. Official channels in this case gave the stamp of approval for processes of devaluation and intimidation.

To summarise this case study, the US Government and its allies, in their campaign against WikiLeaks, used all five methods of reducing outrage. Although the full extent of cover-up remains to be revealed, it is plausible that covert methods have been used. Devaluation has been a prominent technique, with attempts to discredit Manning, Assange and WikiLeaks more generally. The technique of reinterpretation, including lying, minimising, blaming and framing, has been used to suggest WikiLeaks revelations are a source of danger (for example, to individuals named in leaked documents), thereby diverting attention from the crimes revealed by the leaks. One of the most significant achievements of the anti-WikiLeaks campaign has been to frame the issue around WikiLeaks itself, rather than around the matters exposed by the group; many members of the public hear more about Assange and WikiLeaks than about the documents hosted on the site. Official channels, especially the courts, have been used to make the attacks on WikiLeaks seem more justified. Finally, Manning, Assange and others involved in WikiLeaks have experienced serious intimidation.

The attack on WikiLeaks should not be seen in isolation. There is, after all, a long history of reprisals against whistleblowers, as well as pressures against media outlets considering reporting on government crimes, often due to leaks. Highlights of this history include Ellsberg's leaking of the Pentagon Papers, delayed for many months by media timidity; reprisals against A. Ernest Fitzgerald, a US Defense Department employee who exposed billion-dollar cost overruns;[18] and a recent upsurge in whistleblowing by current and former employees of the US national security apparatus.[19] The attack on WikiLeaks has been accompanied by plans to deal with the 'insider threat' – namely to track down public interest leakers.[20]

Manning, Assange and WikiLeaks supporters have many ways to respond to attacks. To better understand the dynamics of outrage management, it is useful to classify responses into five categories:

1 expose attacks (countering cover-up);
2 validate the target (countering devaluation);
3 interpret the attacks as unfair (countering reinterpretation);
4 avoid or discredit official channels – instead, mobilise support (countering official channels);
5 resist intimidation.

Expose attacks

The attacks on WikiLeaks have been widely publicised. For example, the blocking of funding for WikiLeaks was revealed in various media accounts.

Validate the target

Manning and Assange have received endorsements from numerous journalists and prominent individuals, not to mention thousands of bloggers. Indeed, the attempt

to discredit them seems to have triggered a counter-movement to portray them as martyrs to a noble cause. Demonising or glorifying them may not provide an accurate representation of Manning and Assange as individuals, but these responses do reflect the struggle over the value of their acts, cast as evil by detractors and, in defence, as justified and needed by supporters. Underlying the attention to the worthiness or otherwise of Manning and Assange is the more basic issue of the value of WikiLeaks and other online leaking operations.

Interpret the attacks as unfair

In the face of the reinterpretation techniques of lying, minimising, blaming and framing, WikiLeaks supporters have emphasised the unfairness of shooting the messenger, namely attacking leakers and WikiLeaks rather than addressing the problems they have exposed.

Avoid or discredit official channels – instead, mobilise support

The official channels involved in the attacks, which give greater legitimacy to them, have received considerable criticism. The best example is the sceptical reception given to the Swedish legal system by Assange supporters, with many commentators seeing the claims about rape as a process being misused for political purposes. This has made many people sympathetic to Assange's refusal to go to Sweden to face questioning. Normally, a legal system in a well-respected liberal democracy is assumed to function fairly; the discrediting of the Swedish legal system is thus a sign of the power of the campaign to support Assange.

There is ample evidence for outpourings of support for Manning, Assange and WikiLeaks. Where this campaign has a weakness is in not providing an easy opportunity for more direct challenge to the laws and techniques used against WikiLeaks. An analogy would be the McLibel campaign challenging legal action against authors of the leaflet 'What's wrong with McDonald's?'. Supporters distributed the leaflet, itself an action that directly challenged the McDonald's defamation action, vastly increasing the circulation of the information the company was trying to suppress.[21] A possible parallel action in support of WikiLeaks would be for numerous employees in a company all to leak the same document. However, there is no immediately obvious action like this that members of the public can join.

Resist intimidation

Manning, Assange and WikiLeaks supporters have resisted, each in their own way. Manning's calm and considered defence of her actions, in the face of charges against her, revealed thoughtfulness and courage that can be an inspiration to others, although few would be willing to make equivalent sacrifices. The hacker movement Anonymous responded by attacking companies that withdrew credit

facilities from WikiLeaks. The actions of Anonymous certainly show a willingness to resist, but most members of the public can only be second-hand witnesses to hacking exploits. Anonymous operates as a vanguard network, undertaking actions in which participation is impossible for most, and thus is not a model for a wider campaign that can involve a broad cross-section of the population in forms of resistance.

Julian Assange, as the founder and public face of WikiLeaks, has received extraordinary visibility. Whether he has used his support to maximum advantage is another question. As is well known, he refused to go to Sweden to be questioned over rape allegations, first fighting the extradition order in court and then seeking asylum in the Ecuadorian Embassy in the UK. Another option would have been for Assange to go to Sweden and take the risk of being extradited to the US to face charges. If this had happened, he could have become even more of a cause celébrè, generating enormous sympathy and support. A case against him in the US would have been a contemporary equivalent to the possibility of charges against Daniel Ellsberg, who leaked the Pentagon Papers 40 years earlier. Ellsberg could have been charged and gone to prison, but he was so prominent that he was left alone. On a global scale, Assange is even more well-known than Ellsberg ever was; a case against him on the grounds of running a leaking operation could possibly backfire on the US Government, just as the McLibel case backfired on McDonald's. This assessment is hypothetical, of course. The point is that actions taken by key players can open or foreclose opportunities for support actions. Leakers and their supporters need to keep this in mind.

The Snowden story

In June 2013, Edward Snowden, a contractor for the NSA, leaked a massive trove of top secret NSA documents to *The Guardian.*[22] These documents revealed that the NSA, for years, had been undertaking widespread surveillance of electronic communications around the world. The ongoing revelations from the leaked documents caused a worldwide furore. It could be said that Snowden is the world's most successful public interest leaker. Therefore, it is worth examining Snowden's experience to see whether and how he and his supporters avoided or countered the tactics used to reduce outrage over the abuses revealed by his disclosures.

Snowden, like Manning, had great technical skills that he used to obtain, order and explain NSA documents. However, in some ways this was not the greatest challenge he faced. He sought a media outlet that would give his material the visibility he believed it deserved and that would not capitulate to the US Government. Therefore, he did not approach mainstream US media giants, such as *The New York Times,* instead choosing the UK-based *Guardian,* which has a small US operation.

Snowden did not approach just anybody: he wanted to make contact with Glenn Greenwald, a *Guardian* freelance columnist who had taken strong stands critical of US Government surveillance. Snowden initially sent anonymous emails to Greenwald using secure channels, asking him to install encryption software, but Greenwald was too busy to make this a priority. So Snowden tried an indirect

route, approaching journalist Laura Poitras, a fierce critic of the US security state, and a victim of it, who worked closely with Greenwald.

By initially sending a few NSA documents as 'tasters', Snowden captured the interest of Poitras and then Greenwald, enough to entice them, as part of a *Guardian* team, to a meeting in a Hong Kong hotel. Snowden took extraordinary precautions to maintain security, for example, having *The Guardian* visitors put their phones in the freezer, in case they were bugged. Snowden proceeded to pass over the documents and provide an informed explanation of what they meant, given that many were highly technical.

The Guardian decided to go ahead and, in the usual fashion, asked for comment from US officials, who responded with a combination of blandishments and threats. United States media probably would have pulled back at this point, but *The Guardian* went ahead with publication, causing a storm on mainstream and social media throughout the world. After obtaining and leaking the NSA files, Snowden did not want to remain anonymous. A few days after the first *Guardian* stories, he revealed his identity, providing calm explanations of why he had leaked the NSA documents. In going public, Snowden gave greater credibility to the material.

The tactics involved in the Snowden saga fit the same pattern as with WikiLeaks. First, consider the methods used by the US Government to reduce outrage over the NSA's massive surveillance operation. Prior to Snowden's leaks, the NSA's primary tactic had been cover-up: relatively few members of the public knew much about the surveillance, and the mass media did little to pursue the story. Those who tried to expose the problem were devalued: attempts were made to discredit Snowden – for example, calling him variously a 'shithead', traitor, narcissist and Chinese agent.[23] The government reinterpreted its spying operation as protection of the population against terrorism, and attempted to shift attention to Snowden and away from his disclosures. The official channels for addressing the problem were only a facade; the secret court that assessed NSA requests was a rubber stamp. Finally, there is the tactic of intimidation. Under the Obama administration, treatment of state security whistleblowers was especially harsh,[24] as Manning's experience revealed to Snowden.[25]

The same sorts of tactics were used to reduce outrage over methods used to pursue Snowden. There is an overlap here between methods to reduce outrage over NSA surveillance and those to reduce outrage over pursuit of Snowden because, obviously, Snowden provided information to expose the surveillance.

First, cover-up: the US Government used a range of means to snare Snowden, but most of these were unknown to the general public. For example, US officials applied pressure on the Hong Kong and Chinese governments to relinquish Snowden. Later, after Snowden was in Moscow, the US Government induced European governments to refuse permission for an aircraft carrying Bolivian president Evo Morales to use their airspace because of an incorrect suspicion that Snowden was on board. This extraordinary use of power received little media attention. Most of the public knew little about the sustained efforts of US officials to hunt down and capture Snowden.[26]

Second, devaluation: politicians, government officials and media commentators made various derogatory comments about Snowden. Glenn Greenwald,

a key media interpreter of Snowden's disclosures, was also subject to sustained denunciation.[27]

Third, reinterpretation: US officials tried to frame the issue as Snowden violating the confidentiality agreements he had signed, and being disloyal, rather than recognising him as a whistleblower.

Fourth, US Secretary of State John Kerry, among others, said Snowden should return to the US and let the courts deal with him, in other words, to trust in official channels.[28] This was an appeal in principle to official channels, rather than an actual use of them.

Fifth and finally, intimidation: Snowden could predict, from what happened to Manning, his likely fate. In the prospect of torture (through sensory deprivation) and a lengthy jail sentence, there was a combination of techniques. United States officials had partially hidden the harsh treatment of Manning, which blunted public awareness. Snowden knew very well what he faced, yet many members of the public did not, and might have been taken in by US Government statements (using techniques of reinterpretation, including lying and framing) about obtaining a fair trial.

Despite all this, Snowden was highly effective, arguably the most effective leaker in history. The actual impact of his disclosures on policy remains to be seen,[29] and will be limited by various processes, but in terms of popular awareness, the leaks had a tremendous impact. So what did Snowden do to make this possible? First is the tactic of exposure. Of course, this is the essence of whistleblowing, but Snowden sought disclosure to the public via journalists, rather than using internal paths as most whistleblowers do. Second is validation: Snowden calmly and carefully explained his motivations, showing himself to be a sober, socially concerned person. He had no obvious skeletons in his past that could be used to discredit him, and he recruited *The Guardian*, and through it other media outlets, adding credibility to his claims. Third is reinterpretation: Snowden and *The Guardian* stayed on message about the importance of addressing threats to privacy and freedom. Fourth is avoiding official channels and instead mobilising support: Snowden did not pursue formal processes within the NSA, but instead aimed at bringing on board first the journalists Laura Poitras and Glenn Greenwald, then additional *Guardian* workers, and through them a wider constituency. Fifth is standing up to intimidation: Snowden knew his opponents and the risks he faced, yet he continued with calm and courageous commitment to his principles.

In summary, the Snowden saga reveals the usual set of tactics and countertactics found in most struggles between employers and whistleblowers. In this highly unequal struggle between the US Government and a single individual, Snowden fared remarkably well, getting his message to huge audiences around the world. In doing this, he used the tactics of exposure, validation, interpretation, mobilising support (and avoiding official channels) and resisting intimidation. However, it is important to recognise that Snowden did not do all this on his own. Mobilising support implies others playing a role and taking risks. Many individuals working for *The Guardian* were ingenious in gathering and verifying the stories and courageous in standing up to intimidation; others in media outlets, government

departments and elsewhere played crucial roles in protecting Snowden and ensuring his revelations received the publicity they did.[30] The message here is that, just as secrecy is multilayered, challenging secrecy requires a multilayered effort.

Conclusion

Most whistleblowers speak out without taking any precautions against reprisals. Many do not think of themselves as whistleblowers: they are employees just doing their jobs. Others trust in the system, and therefore initially make reports to bosses, senior management and outside watchdog agencies, such as ombudsmen. For too many whistleblowers, this approach is disastrous. They are subject to reprisals and little or nothing is done about the matters they raise. Indeed, by reporting matters internally, they alert wrongdoers to the need to cover their tracks, for example, by destroying evidence and creating false stories. By revealing their identity, whistleblowers make it possible for perpetrators to initiate reprisals and prevent access to any more incriminating information.

Anonymous whistleblowing – leaking in the public interest – is often a far more effective option. It reduces the risk of reprisals, keeps attention on the information leaked rather than on the person revealing it, and enables the whistleblower to remain on the job, collect more information and leak again. Public interest leaking has been occurring for decades, but has had far less visibility than conventional non-anonymous whistleblowing, in part because most news stories based on public interest leaking focus on the information, not on the person who has revealed it. Journalists, who are prime recipients of leaks, often make extraordinary efforts to avoid revealing their sources, sometimes even going to jail rather than acquiescing to court orders.

The attention on Chelsea Manning, Julian Assange and WikiLeaks has served, among other things, as a distraction from the documents that WikiLeaks has enabled to become public, including both those leaked by Manning and by others from around the world. The crimes exposed through WikiLeaks should be the centre of attention, but few of them are known to the public.

Even so, the attack on WikiLeaks has had a significant positive impact: it has made leaking far more prominent as an option for whistleblowers. Leaking directly to WikiLeaks is a possibility, but for most whistleblowers there are other leaking options, often more effective, most commonly through contact with local journalists (professional or citizen journalists) or action groups or by directly circulating or posting information anonymously. Edward Snowden took the route of leaking to journalists he carefully selected as recipients, thereby amplifying the impact of his disclosures.

In some ways, then, WikiLeaks need not exist as an actual operation to provide an inspiration for more leaking. Others can set up operations similar to WikiLeaks, learning from the experience of WikiLeaks to be more effective in defending against attack, liaising with mass media and providing a service to whistleblowers. For employees who observe wrongdoing and want to do something about it, the WikiLeaks story is a pointer to a different option: remaining anonymous.

The lessons from the experiences of whistleblowers, WikiLeaks and Snowden are straightforward:

- If possible, keep your identity secret.
- Win allies for publicising leaked material, such as the media and action groups.
- Be very careful about what is leaked, to prevent damage to others, to communicate well to outsiders and to minimise the risk of detection.
- Be prepared for a witch-hunt for the leaker.

Finally, there is a certain irony in recommending anonymity – a type of secrecy – in order to be more effective in exposing secrets.

Notes

1 C. Fred Alford, *Whistleblowers: Broken Lives and Organizational Power* (Cornell University Press 2001); David W. Ewing, *Freedom Inside the Organization: Bringing Civil Liberties to the Workplace* (Dutton 1977); Myron Peretz Glazer and Penina Migdal Glazer, *The Whistleblowers: Exposing Corruption in Government and Industry* (Basic Books 1989); Geoffrey Hunt (ed.), *Whistleblowing in the Health Service: Accountability, Law and Professional Practice* (Edward Arnold 1995); Geoffrey Hunt (ed.), *Whistleblowing in the Social Services: Public Accountability and Professional Practice* (Edward Arnold 1998); Nicholas Lampert, *Whistleblowing in the Soviet Union: Complaints and Abuses under State Socialism* (Macmillan 1985); Marcia P. Miceli, Janet P. Near and Terry Morehead Dworkin, *Whistle-blowing in Organizations* (Routledge 2008); Terance D. Miethe, *Whistleblowing at Work: Tough Choices in Exposing Fraud, Waste, and Abuse on the Job* (Westview 1999).

2 William De Maria, *Deadly Disclosures: Whistleblowing and the Ethical Meltdown of Australia* (Wakefield Press 1999); William De Maria and Cyrelle Jan, 'Behold the Shut-eyed Sentry! Whistleblower Perspectives on Government Failure to Correct Wrongdoing' [1996] 24 *Crime, Law & Social Change*, 151.

3 For his own account, see Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers* (Viking 2002).

4 David E. Pozen, 'The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information' [2013] 127 *Harvard Law Review*, 512 provides evidence of government tolerance of high-level leaking, namely leaking by those who do not think of themselves as whistleblowers. Pozen's analysis is restricted to the US federal government, and national security issues in particular; he notes the different response to what is called in this chapter 'public interest leaking'.

5 Kathryn Flynn, 'Covert Disclosures: Unauthorized Leaking, Public Officials and the Public Sphere' [2006] 7 *Journalism Studies*, 256; see also Kathryn Flynn, 'The Practice and Politics of Leaking' [2011] 30 *Social Alternatives*, 24. Other treatments include *The Art of Anonymous Activism: Serving the Public While Surviving Public Service* (Project on Government Oversight; Government Accountability Project; Public Employees for Environmental Responsibility 2002) especially 7–16; Nicky Hager and Bob Burton, *Secrets and Lies: The Anatomy of an Anti-environmental PR Campaign* (Craig Potton 1999) 240–7.

6 Brian Martin, *Justice Ignited: The Dynamics of Backfire* (Rowman & Littlefield 2007). For many other sources see 'Backfire Materials' <http://www.bmartin.cc/pubs/backfire.html> accessed 14 September 2014.

7 Truda Gray and Brian Martin, 'Abu Ghraib' in Brian Martin, *Justice Ignited: The Dynamics of Backfire* (Rowman & Littlefield 2007).

8 Cover-up is closely related to secrecy, and indeed these terms can be used as synonyms. 'Cover-up' in this context suggests hiding information about wrongdoing as opposed to a general system of secrecy, which can apply to a range of activities.
9 De Maria (n. 2).
10 Brian Martin, *Whistleblowing: A Practical Guide* (Irene Publishing 2013) 133–5.
11 On the relationship between WikiLeaks and mainstream media – which themselves are in rapid transition – see Charlie Beckett with James Ball, *WikiLeaks: News in the Networked Era* (Polity 2012).
12 Chase Madar, *The Passion of Bradley Manning* (OR Books 2012).
13 Dawn L. Rothe and Kevin F. Steinmetz, 'The Case of Bradley Manning: State Victimization, Realpolitik and WikiLeaks' [2013] 16 *Contemporary Justice Review*, 280.
14 It is uncertain whether these companies were responding to pressure from the US Government or acting on their own to please the government.
15 See, for example, 'Note on the Various Attempts to Persecute WikiLeaks and People Associated with It' in Julian Assange with Jacob Appelbaum, Andy Müller-Maguhn and Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet* (OR Books 2012) 13–19.
16 The idea of layers of secrecy is addressed by David E. Pozen, 'Deep Secrecy' [2010] 62 *Stanford Law Review*, 257, who elaborates on the distinction between shallow secrets, in which the existence of a secret is known but not its content, and deep secrets, in which the existence of a secret is unknown to wider audiences. A similar idea, related to the tactics for reducing outrage outlined here, is censorship of censorship; that is, reducing awareness that censorship has occurred: see Sue Curry Jansen and Brian Martin, 'Making Censorship Backfire' [2003] 7(3) *Counterpoise*, 5. For a related concept, see Thomas Mathiesen, *Silently Silenced: Essays on the Creation of Acquiescence in Modern Society* (Waterside Press 2004).
17 For the case of the US legal system, see Thane Rosenbaum, *The Myth of Moral Justice: Why Our Legal System Fails to Do What's Right* (HarperCollins 2004).
18 A. Ernest Fitzgerald, *The High Priests of Waste* (Norton 1972).
19 For one account, see Sibel Edmonds, *Classified Woman: The Sibel Edmonds Story. A Memoir* (Sibel Edmonds 2012).
20 Andy Greenberg, *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information* (Dutton 2012) 176–225.
21 John Vidal, *McLibel* (Macmillan 1997); see also Fiona J. L. Donson, *Legal Intimidation: A SLAPP in the Face of Democracy* (Free Association Books 2000).
22 For informative accounts, see Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton 2014); Michael Gurnow, *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal* (Blue River Press 2014); Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Guardian Books 2014).
23 Greenwald (n. 22) 222–6; Gurnow (n. 22) 76–7; Harding (n. 22) 317.
24 Edmonds (n. 19).
25 Harding (n. 22) 147.
26 Gurnow (n. 22) gives considerable detail.
27 Greenwald (n. 22) 210–22.
28 For the contrary view, see Daniel Ellsberg, 'Snowden Would Not Get a Fair Trial – and Kerry is Wrong' *The Guardian* (London, 30 May 2014) <http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act> accessed 14 September 2014.
29 For one account, see Simon Davies (ed.), *Security Services Reform: Sound and Fury, Signifying Nothing? A Global Analysis of the Impact of the Snowden Revelations* (Privacy Surgeon 5 June 2014).
30 Harding (n. 22).