"All that is needed for evil to prosper is for people of good will to do nothing"—Edmund Burke

The Whistle

No. 76, October 2013

Newsletter of Whistleblowers Australia

Edward Snowden

Media watch

Why is NSA leaker Snowden demonized?

Rem Rieder
USA Today, 19 June 2013

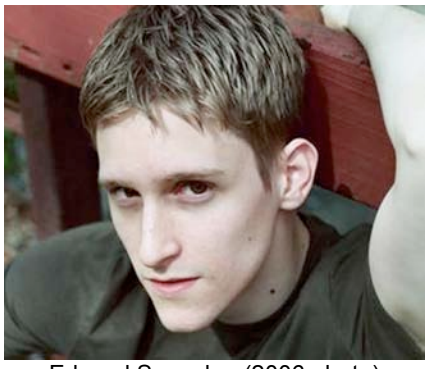
NSA LEAKER Edward Snowden is being called a traitor.

It's a classic example of "shoot the messenger."

Traitor or not, the nation needs to decide for itself the appropriate level of surveillance.

When you leak explosive government secrets to the news media, it's safe to say that you open yourself up to, among other things, harsh criticism.

So it's hardly a surprise that former vice president Dick Cheney, the hardest of the hardliners, has unloaded on National Security Agency leaker Edward Snowden, denouncing him as a "traitor" who might be working for China.



Edward Snowden (2006 photo)

But Cheney, who made his remarks over the weekend on *Fox News Sunday*, was hardly the first to use the epithet. Last week, in an interview on ABC's *Good Morning America*, House Speaker John Boehner said flatly of Snowden: "He's a traitor."

And when it comes to the name-calling and the demonizing, former and current public officials such as Cheney and Boehner hardly have a monopoly. Journalists can play that game, too.

Politico columnist Roger Simon wrote a sneering piece headlined "The slacker who came in from the cold" in which he dismissed Snowden as "29 and possessing all the qualifications to become a grocery bagger."

(An aside: Is it just me or are these constant references to Snowden being 29, as if that somehow discredits him, out of line as well as annoying? Is the idea that someone so young is incapable of doing anything worthwhile? Really?)

To former NBC anchor Tom Brokaw, Snowden is merely "a high school dropout who is a military washout." And rather than go down in history as a significant whistleblower, *Washington Post* columnist Richard Cohen wrote in a sublimely baffling outburst that he thought Snowden will "go down as a cross-dressing Little Red Riding Hood."

All of that outrage is perfectly understandable. Acts like Snowden's arouse powerful passions. To some he is a hero, a principled man whose alarm at the security state's secret surveillance compelled him to act, despite the consequences to his own life. To others he is, well, a traitor, an irresponsible, self-righteous egomaniac who placed himself above the law and put his country in great peril.

But it's important that we — the news media and society as a whole — don't get too caught up in it. While pinning labels on Edward Snowden may be a fine parlor game, it's not nearly as significant as dealing with the information he revealed.

Even White House Press Secretary Jay Carney says it's "appropriate" to have a national debate on government information gathering. But we wouldn't be having one absent Snowden's disclosures.

Maybe the government is right. Maybe the heightened security the surveillance of all those phone calls and e-mails makes possible is worth the erosion of privacy. But that's something we as a country need to decide, not the president, whichever president, acting without our knowledge. Remember, even if you trust this particular president and/or his predecessor, there's no guarantee that someday the White House won't be occupied by someone you don't want having access to all that "telephony metadata" and the like. (See Nixon, Richard.)

Even now, it's not an easy debate to have. The proceedings of the Foreign Intelligence Surveillance Court are secret. Members of Congress who are briefed on the programs are constrained about what they can say. So are the Silicon Valley powerhouses that have cooperated with the PRISM initiative. On Tuesday, Google asked the surveillance court for permission to be more forthcoming about its role.

But despite the difficulties, a conversation has begun. The federal government has mounted an aggressive defense of the programs and has begun to release information to show that they are working. Some members of Congress seem committed to trying to rein in the excesses, no matter how uphill the struggle. And we've only just begun.

That's where the primary focus should remain, not on whether or not Snowden is a duplicitous spoiled brat.

"Shoot the messenger" has been part of the lexicon for a long time, certainly since Sophocles' prime, which was way pre-Twitter. It doesn't just apply to actual old-school messengers and, as is frequently the case in this era, the news media. Ad hominem (and ad feminam) attacks are a time-dishonored way of avoiding uncomfortable subjects by beating up political opponents. And belaboring the appallingly 29-year-old slacker/traitor is a great way to change the subject.

The geeks who leak

Michael Scherer, Caroline Kelley, Zeke Miller and Jay Newton-Small
Time, 24 June 2013

THE PRESIDENT calls them a threat to national security. The Internet calls them heroes. A new wave of hacktivists is changing the way we handle secrets

The 21st century mole demands no payments for his secrets. He sees himself instead as an idealist, a believer in individual sovereignty and freedom from tyranny. Chinese and Russian spooks will not tempt him. Rather, it's the bits and bytes of an online political philosophy that attract

his imagination, a hacker mentality founded on message boards in the 1980s, honed in chat rooms in the '90s and matured in recent online neighborhoods like Reddit and 4chan. He believes above all that information wants to be free, that privacy is sacred and that he has a responsibility to defend both ideas.

"The public needs to decide whether these programs and policies are right or wrong," said Edward Joseph Snowden, the 29-year-old former National Security Agency (NSA) contractor who admitted on June 6 to one of the most significant thefts of highly classified secrets in US history. The documents he turned over to the press revealed a massive program to compile US telephone records into a database for antiterrorism and counterintelligence investigations. Another program, called Prism, has given the NSA access to records at major online providers like Google, Facebook and Microsoft to search information on foreign suspects with court approval. The secret program has been under way for seven years.

Snowden is "no different than anybody else," he claimed. "I'm just another guy who sits there day to day in the office," he said in an interview with the *Guardian,* which broke the story along with the *Washington Post.* But Snowden, who was working as an analyst for the government contractor Booz Allen, is not just another guy. He is something new. More than 1.4 million Americans now hold top-secret security clearances in the military and the shadow world of intelligence. Most do not contact reporters and activists over encrypted e-mail in hopes of publishing secrets as civil disobedience. Few are willing to give up their house, their $122,000-a-year job, their girlfriend or their freedom to expose systems that have been approved by Congress and two Presidents, under the close monitoring of the federal courts. Snowden is different, and that difference is changing everything.

A brave new world

The US National Security infrastructure was built to protect the nation against foreign enemies and the spies they recruit. Twenty-something homegrown computer geeks like Snowden, with utopian ideas of how the world should work, scramble those assumptions. Just as antiwar protesters of the Vietnam era argued that peace, not war, was the natural state of man, this new breed of radical technophiles believes that transparency and personal privacy are the foundations of a free society. Secrecy and surveillance, therefore, are gateways to tyranny. And in the face of tyranny, the leakers believe, rebellion is noble. "There is no justice in following unjust laws," wrote Aaron Swartz, a storied computer hacker and a co-founder of Reddit, in a 2008 manifesto calling for the public release of private documents. "We need to take information, wherever it is stored, make our copies and share them with the world."

Aaron Swartz

On the run in a Hong Kong hotel room, Snowden explained in a video interview the reasons for his actions, with pride and a hint of serenity, even as he described how he could be killed, secretly "rendered" by the CIA or kidnapped by Chinese mobsters for what he had done. He characterized the surveillance systems he exposed as "turnkey tyranny" and warned of what would happen if the safeguards now in place ever fell away. He hoped to force a public debate, to set the information free. "This is the truth. This is what is happening," he said of the documents he had stolen and released. "You should decide whether we need to be doing this."

Three years earlier, a 22-year-old Army intelligence analyst stationed in Iraq named Bradley Manning offered a nearly identical defense for a similar massive breach of military and diplomatic secrets. "I want people to see the truth, because without information, you cannot make informed decisions as a public," Manning wrote to a hacking friend in 2010 after he had illegally sent hundreds of thousands of classified documents to the website WikiLeaks.

Like Snowden, Manning said his worst fear was not that his actions would change the world but that they wouldn't. Both young men grew up in the wake of the security crackdown that followed the Sept. 11, 2001 attacks. They had come of age online, in chat rooms and virtual communities where this new antiauthority, free-data ideology was hardening. They identified, at least in part, as libertarians, with Manning using the word to describe himself and Snowden sending checks to Ron Paul's presidential campaign. Neither appeared to believe he was betraying his country. "Information should be free," wrote Manning before his capture, later adding that he was not sure if he was a hacker, cracker, hacktivist, leaker or something else. "It belongs in the public domain."

"We are legion"

Manning's statement is a radical one, since it directly undermines the rule of law, something both men seemed to recognize. "When you are subverting the power of government, that's a fundamentally dangerous thing to democracy," Snowden said of his actions. And in official Washington, the broad consensus is that the impulse is dead wrong and likely to cause real harm. "What this young man has done, I can say with a fair amount of certainty, is going to cost someone their lives," said Georgia Republican Saxby Chambliss, who is vice chairman of the Senate Select Committee on Intelligence. Neither the Obama White House nor the leaders of either party are much concerned about the legality or the effectiveness of the sweeping data-collection programs; both sides, however, seemed quite keen to track down Snowden and bring him to justice. The public, according to a new *Time* poll, echoed that impulse, with 53% of Americans saying Snowden should be prosecuted, compared

with just 28% who say he should be sent on his way.

But among Snowden and Manning's age group, from 18 to 34, the numbers are much higher, with 43% saying Snowden should not be prosecuted. That hacktivist ethos is growing around the world, driven in large part by young hackers who are increasingly disrupting all manner of institutional power with online protest and Internet theft. "That's the most optimistic thing that is happening — the radicalization of the Internet-educated youth, people who are receiving their values from the Internet," said Julian Assange, the founder of WikiLeaks, in an April interview with Google executive chairman Eric Schmidt. "This is the political education of apolitical technical people. It is extraordinary."

The stories show up in newspapers and courtrooms on a daily basis. Just as Snowden flew to Hong Kong with his stolen cache, a 28-year-old hacker named Jeremy Hammond pleaded guilty in New York City on May 28 to stealing e-mails, credit-card information and documents from Stratfor Global Intelligence Service, a private consulting company. Hammond expressed little remorse for working with a hacking and activist collective known as Anonymous to break the law. "I did this because I believe people have a right to know what governments and corporations are doing behind closed doors," he wrote on a website after pleading guilty. "I did what I believe is right."

In recent years, Anonymous has targeted companies like MasterCard and trade groups like the Motion Picture Association of America for the alleged crime of opposing openness. They have staged protests against the rapid-transit system in the San Francisco Bay Area, when authorities shut down cellular service, and staged rallies around the world against Scientology, to protest the religion's aggressive protection of its secrets. In 2011, hackers claiming to be Anonymous stole personal details of 77 million Sony PlayStation accounts, shutting down the network for a month, in apparent protest against a prohibition the company had imposed on installing certain features on the devices' firmware.

Others have targeted academia and the law. Swartz, who committed suicide at the age of 26 in January while under federal indictment for hacking an academic computer, downloaded and publicly released millions of federal court documents from a US court computer system in protest against a per-page fee for access. He was arrested for trying to download huge volumes of copyrighted academic articles from the costly JSTOR database at the Massachusetts Institute of Technology. "Those who have been locked out are not standing idly by," he had argued about the need to liberate information to the public domain.

These "free the files" protests are crimes under US law, but in most cases they are not crimes of a nature that the legal system was designed to prosecute. When they take the form of denial-of-service attacks, overwhelming and shutting down websites with bogus traffic, they resemble protests protected in some cases by the First Amendment. Others follow in the tradition of the country's most heralded technological revolutionaries. Facebook's Mark Zuckerberg hacked the Harvard databases of student IDs to create Facemash, the predecessor to his current multibillion-dollar site. As a teenager, Apple founder Steve Jobs sold boxes built by his friend Steve Wozniak to fool the phone company and make free long-distance calls. Microsoft's Bill Gates hacked the accounts of an early computer company to avoid having to pay to use it.

By the early 1990s, the hacktivists were organizing around larger goals, like ensuring online privacy for individuals. A hacker named Phil Zimmermann created a data-encryption program called PGP, which used a software technology that was classified as a "munition" under US law and therefore banned for export. Zimmermann responded by publishing his code in a book, via MIT Press, since the export of printed matter is protected by the First Amendment. The movement that grew up around these efforts helped give birth to WikiLeaks. Today that same defiant spirit still dominates large swaths of the Internet, informing the actions of people like Snowden, Manning and Swartz. "It's a generation of kids who have been told again and again that behaviors that seem perfectly reasonable to them are criminal," says Lawrence Lessig, a Harvard law professor who was a mentor to Swartz.

Peter Ludlow, a philosophy professor at Northwestern University who has written extensively about cyberculture, says two disparate ideas have been linked in recent years. "There was always this kind of tech-hacker ethos, which was probably libertarian, which has collided with this antiauthoritarian political impulse," he said. "You put these two things together, and it's just like wildfire."

"We are legion," runs the catchphrase of Anonymous. "We do not forgive. We do not forget. Expect us." Now the government has to figure out how to respond.

Dawn of the informer age

In the days after the Snowden disclosures, a coalition of 86 groups — including online communities like 4chan, Reddit and BoingBoing — signed on to an open petition to Congress calling the NSA programs "unconstitutional surveillance." A petition filed with WhiteHouse.gov calling on Obama to pardon Snowden reached 60,000 names in three days. Sales of George Orwell's 64-year-old

antitotalitarian novel *1984* have soared. The Progressive Change Campaign Committee, which usually raises money for liberal candidates, founded a legal-defense fund for Snowden. And a recent online video campaign — with Hollywood filmmaker Oliver Stone, actors such as Maggie Gyllenhaal and Peter Sarsgaard, and several liberal journalists — has been organizing a social-media campaign called "I am Bradley Manning," which argues Manning was nothing more than a whistle-blower who should be protected from prosecution.

Even the current corporate titans of Silicon Valley, who have long been libertarian in their politics, have not been far behind. Shortly after the Snowden leak named Google, Facebook and Microsoft as partners in the Prism program, the companies all asked the Justice Department for permission to disclose more fully their prior secret cooperation with the courts. The reason: they did not want to damage their brands, which have long embraced free experimentation and minimal regulation on the Internet. "Google has nothing to hide," the company's chief legal officer David Drummond announced in an open letter.

But what is accepted wisdom among the tech community is viewed with some skepticism with much of the American public. The *Time* poll found that only 43% of the country thought the government should "cut back on programs that threaten privacy," while 20% said the government should be doing more, even if it invades privacy. On the question of whether they approved or disapproved of the current programs revealed by Snowden, the nation was basically split, with 48% approving and 44% disapproving.

The government, meanwhile, is likely to treat Snowden as if he was a Cold War spy seeking to undermine the country he still claims to serve. The Justice Department has launched an investigation into the disclosure of classified information, a prelude to a standard espionage prosecution. Even though charges may not be filed for weeks, it is likely that prosecutors will try to extradite Snowden to the US for trial and seek a punishment of life in prison.

Perhaps the clearest summary of the federal response to this new online political activism can be found, appropriately enough, in a classified 2008 document from the US Army Counterintelligence Center, which has been leaked and posted online by hacker activists. "Websites such as WikiLeaks.org have trust as their most important center of gravity protecting the anonymity and identity of the insider, leaker, or whistle blower," the document reads. The solution, concludes the Army, is to find, expose and punish those people who leak in an effort to "potentially damage or destroy this center of gravity and deter others considering similar actions."

Already, the government may have overinterpreted that guidance. Manning, after his arrest more than three years ago, was subjected to harsh incarceration conditions, including confinement to his cell 23 hours a day, that have raised the concerns of Amnesty International, a former UN human-rights investigator and even a former State Department spokesperson, Philip Crowley, who called the conditions "ridiculous and counterproductive and stupid." Crowley resigned over those comments, but a federal judge later ruled that Manning's final sentence would be reduced 112 days to compensate for harsh pretrial treatment.

Manning has already pleaded guilty to 10 counts of misusing classified information, with a maximum penalty of 20 years in prison. He is now undergoing a court-martial at Fort Meade, Maryland, the same military base where the NSA is headquartered, on additional charges of aiding the enemy and violating the Espionage Act, with the possibility of life in prison. "The more I read the cables, the more I came to the conclusion this was the type of information that should become public," he has testified in his own defense.

After the Manning leaks, the intelligence community, the State Department and the military tried to remake their procedures to ensure that another leak could not happen. New trip wires were added to detect massive downloading of classified information, monitor military workstations and better compartmentalize secret information. Clearly, more will have to be done. "There is a belief that the total revelation of information is in the public interest," said a White House official, describing the threat. The official noted that the coming changes to classified access in response to Snowden are likely to further limit information sharing, narrowing the potential of a key reform after 2001 meant to prevent further attacks.

"I think that there's a group of people, younger people who are not fighting the war, who are libertarians mostly, who feel like the government is the problem," says Senator Lindsey Graham, the South Carolina Republican on the Armed Services Committee who helped write the laws that govern the NSA surveillance programs. Graham says he wants more internal efforts in the intelligence community to detect such people before they go public and to punish the leakers severely. "It's imperative that we catch him," Graham said of Snowden. "I don't care what we need to do. We need to bring this guy to justice for deterrence sake."

But others who monitor the intelligence world say it will not be so easy. Snowden wasn't a government official; he was a private contractor, the kind of hired help the US intelligence system has come to rely on by the thousands since 9/11. And the punishment of Manning did not dissuade Snowden, after all. If anything, it cleared the path to future celebrity and martyrdom for other, like-minded activists. "It's going to be a challenge to the intelligence community to figure out how to defend against this," says Senator Chambliss. "I don't know that you always can."

In the meantime, the threat of more leaks is likely to grow as young people come of age in the defiant culture of the Internet and new, principled martyrs like Snowden seize the popular imagination. "These backlashes usually do provoke political mobilization and a deepening of commitments," says Gabriella Coleman, a professor at McGill University

in Montreal, who is finishing a book on Anonymous. "I kind of feel we are at the dawn of it."

Gabriella Coleman

How to leak and not get caught

Jack Shafer
Reuters, 9 July 2013

IF US prosecutors ever get their hands on Edward Snowden, they'll play such a tympanic symphony on his skull he'll wish his hands never touched a computer keyboard. Should US prosecutors fail, US diplomats will squeeze — as they did in Hong Kong — until he squirts from his hiding place and scurries away in search of a new sanctuary. But even if he finds asylum in a friendly nation, his reservation will last only as long as a sympathetic regime is calling the shots. Whether he ends up in Venezuela or some other country that enjoys needling the United States, he'll forever be one election or one coup away from extradition.

Even then, he won't be completely safe.

"Always check six, as we said when I used to be a flyer in the Air Force," said NSA whistleblower Thomas Drake recently. "Always make sure you know what's behind you."

Solitary whistleblowers like Snowden, Drake and Daniel Ellsberg draw targets on their backs with their disclosures of official secrets, either by leaving a trail from the heist scene, being the most logical suspect, or because they admit their deed. Escaping prison time, such whistleblowers have learned, depends on the luck of prosecutorial overreach (Drake) or self-destruction by the state, which derailed the prosecution of Pentagon Papers liberator Ellsberg.

The solitary whistleblower, usually a career government employee, isn't really a leaker, as Stephen Hess explains in his enduring typology of leakers. Typically, the whistleblower seeks revolutionary change, not piecemeal reform. He doesn't share information with journalists to purchase their goodwill or to loft a trial balloon or to give himself an ego boost. He's motivated by principle, not self-interest or Machiavellian intrigue, and seeks to correct what he considers an intolerable wrong. And in most cases, his whistleblowing results in career suicide if not jail time.

Most leakers — mindful of the fate of the pure and solitary whistleblowers — scale the size of their leaks to avoid detection. Rather than giving the whole puzzle away to reporters, they break off pieces for distribution, in hopes that it can't be traced back to them. Or, if crafty, leakers dispense pieces of the puzzle that aren't especially revealing and therefore not precisely classified, but provide hints about the location of the next puzzle piece. Investigative reporters who excel at fitting a mosaic together benefit the most from this class of leaker.

According to plumbers, a slow leak can lead to big problems.

The best way to escape detection, however, is to leak as part of a flock, a flock that may or may not fly together. The best recent example of this kind of leaking can be found in two excellent stories about the NSA's machinations published earlier this week, the *New York Times*' "In Secret, Court Vastly Broadens Powers of NSA," and the *Wall Street Journal*'s "Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering."

I'm not privy to how the *Times* or *Journal* reported these stories, but both attribute their revelations to interviews with "current and former" officials. As identification stamps go, "current and former" officials is pretty vague. The complete *Journal* credit goes to interviews with "current and former administration and congressional officials," but that's still plenty vague. In plurality, any flocking bird will tell you, resides security. When a mass of current and former officials talk to the press about a classified story, it's harder for a government investigator to pick off one for punishment. Such vague sourcing means the government investigator would have to investigate every current and former official exposed to the classified information discussed in the story, which can often be a very long list. In our current national security reporting renaissance, with a dozen or more reporters breaking new parts of the NSA story almost daily, the number of suspected leakers quickly expands to defeat the ability of the spy cops to track all of them.

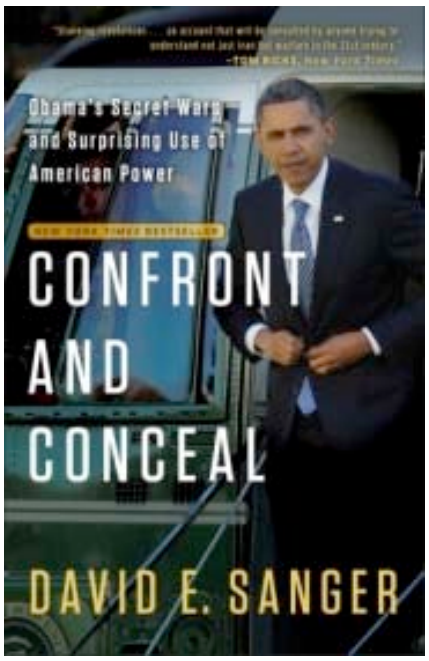
That's assuming of course, that the leakers have actually leaked classified information. As mentioned above, fitting pieces of unclassified material together mosaic style can lead a good reporter toward a mostly completed picture. At this juncture, the reporter can ask authorities direct "confirm or deny" questions about his findings. The authorities can confirm his hypothesis, beg him not to publish it, or confess a kind of defeat by confirming parts of the story (but not for attribution) while explaining why other parts of it aren't true. One thing the government can rarely afford to do is blow the reporter off, lest the government be damaged by the publication of an inaccurate story. Also, the last thing the national security state wants is to turn away reporters whose questions might cause it more grief than the less-damaging story the national security state can confirm.

The "current and former officials" formulation serves the press well in times like these, where the former officials might belong to a different party or faction. This broadening of the sourcing helps lift the story out of the

partisan realm, and helps make the reporters look more like truth-finders and less like partisans. It also provides the leakers with camouflage that makes them look less like leakers and more like think-tankers conducting a policy debate in the pages of the press, and helps dislodge the debate from the political. Sometimes the protestations of "current and former officials" is a genuine signal of a policy debate inside the government, which appears to have been the case in 2005 when *New York Times* reporters James Risen and Eric Lichtblau broke the "Bush Lets U.S. Spy on Callers Without Courts" story. Breaking convention, Risen and Lichtblau enumerated the officials yakking with them, writing that "nearly a dozen" anonymous current and former officials had discussed the story with the *Times* "because of their concerns about the operation's legality and oversight."

The New York Times and the *Wall Street Journal* aren't the only major news outlets favoring the "current and former" construction. In recent months, the *Washington Post,* the *Los Angeles Times* and Reuters have relied on it to extend anonymity to sources that may or may not have been authorized to discuss national security-related issues.

The last thing a source who doesn't consider himself a whistleblower should do if he hopes to evade detection is grandstand. According to a recent report by NBC News, the Justice Department has opened an investigation of James "Hoss" Cartwright, a four-star general and former vice chairman of the Joint Chiefs of Staff, for possibly leaking classified information about the Stuxnet virus that appeared in a June 1, 2012 *New York Times* story by David E. Sanger. That story, of course, attributed some of its findings to interviews with "current and former American, European and Israeli officials involved with the program, as well as a range of outsiders."



We can and should presume the innocence of Cartwright, but in a piece for Slate, my friend and former colleague Fred Kaplan sketched some of the circumstantial evidence that might have led investigators to the general. Given his military position, he was certain to know all about Stuxnet. Kaplan noted that Cartwright is also quoted by name in Sanger's book, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, from which the *Times* article was adapted. And the general had a reputation inside of the Pentagon of being a "lone wolf," wrote Kaplan, who did things his own way and by himself, and lone wolves often pay a price for their independence.

"If the Justice Department continues its probe and winds up indicting Cartwright for violating his security oath, it's unlikely that any officers will leap to his defense in this crisis either," Kaplan wrote. "It's a fair guess, in fact, that some of those officers may have pointed prosecutors in his direction."

If you hope to leak national security information and avoid prosecution, don't do it solo, as Snowden (and perhaps Cartwright) did. Bring a posse of like-minded leakers with you to muddy your tracks. And forget the fire hose: A drip irrigation system might take forever to drench the press but it's a lot less conspicuous.

From patriot to pariah

Peter Munro
Sydney Morning Herald, 13 July 2013

IN an era where technology has made it easier to smuggle data, governments are determined to demonise whistleblowers.

Deep Throat would meet journalist Bob Woodward in an underground car park at 2am, their meetings arranged through the signal of a red flag in an old flower pot or codes circled in the newspaper. Four decades later, Bradley Manning lip-synced to Lady Gaga while downloading hundreds of thousands of classified documents from military servers.

The diminutive, low-ranking army private, now on trial for "aiding the enemy," is in many ways the antithesis of the well-connected Watergate whistleblower, chain-smoking while spilling state secrets. Hell, Manning doesn't even look old enough to smoke.

More Americans believe Snowden is a whistleblower than a traitor — a mood that might win the day.

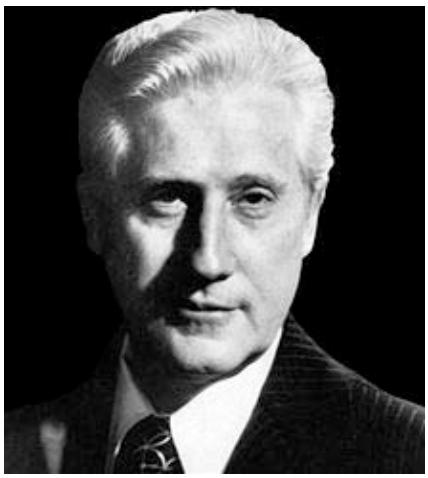
Classmates recalled the intelligence analyst as a "funny little character," often teased for being a geek. He joined the army in 2007 after drifting through low-paid jobs, yet three years later casually carried out what he called "possibly the largest data spillage in American history," all the while singing along to *Telephone*.

The appearance of 30-year-old Edward Snowden — lean, bespectacled and pale, with a fuzz of facial hair — is similarly disarming. The fugitive former intelligence contractor was a high school dropout whose first job at America's National Security Agency was as a security guard, before moving up the ranks. As online magazine *Slate* noted, the man accused of being a traitor for leaking details of pervasive snooping by the US is not a seasoned FBI or CIA investigator. He's the IT guy.

The Obama administration has accused him of threatening US national security. But its grip on control seems to be slipping, particularly in relation to data in the digital age.

Whistleblowing is faster and easier than ever. Today, potential leakers do not need a dark car park so much as a good grasp of digital technology.

Former FBI deputy director Mark Felt was lionised by many Democrats, in 2005, when he outed himself as Deep Throat. Former Bill Clinton adviser Dick Morris said Felt should have been awarded the Medal of Honour for helping *Washington Post* reporters uncover the Watergate scandal that brought down President Nixon.



Mark Felt

In 2008, presidential nominee Barack Obama was lip-syncing from the same song book, hailing the "courage and patriotism" of whistleblowers. Yet since taking office, Obama has presided over an unprecedented crackdown on whistleblowers and leakers.

Five years after saying whistleblowing "should be encouraged rather than stifled," the Obama administration has the dubious record of having prosecuted more leakers under the World War I-era Espionage Act than all other administrations combined.

Sections of the US media have been lately complicit in this crackdown. In 2002, *Time Magazine* applauded three whistleblowers as its "people of the year." Just over a decade later, self-described whistleblower Snowden is instead gutless, a coward and traitor, according to Fox News. No surprises there, perhaps.

More telling is the capitulation of *The Washington Post*, which ironically scored a major scoop based on Snowden's documents. In June the paper that led perhaps the most significant leak-based investigation in US political history declared in an editorial that "the first US priority should be to prevent Mr Snowden from leaking information."

As online publication *Salon* wrote, it was the equivalent of the newspaper in 1972 insisting the Nixon administration's first priority should be to prevent Deep Throat from leaking more information.

Snowden, who has been stripped of his passport, reportedly remains stranded inside the transit zone of a Russian airport. His likely final destination is the Venezuelan capital of Caracas, which is "the world's murder capital."

Snowden never expected to be met by US authorities with open arms. But his case is an insight into the way whistleblowers have gone from patriots to pariahs under Obama. The fugitive former security contractor has been charged with espionage for leaking details of America's extensive surveillance network, which extends to four facilities in Australia.

Former NSA executive Thomas Drake was charged similarly under the Espionage Act in 2010 for leaking information about financial waste and bureaucratic dysfunction within the NSA. His charges were later downgraded to a single misdemeanour for "exceeding the authorised use of a computer."

"I actually had hopes for Obama," Drake told *The New Yorker* in 2011. "But power is incredibly destructive. It's a weird, pathological thing. I think the intelligence community co-opted Obama because he's rather naive about national security. He's accepted the fear and secrecy."

Drake's first full day at work happened to be on September 11 — the legacy of which remains strong today. The fear and secrecy that spilled from the US terrorist attacks has seen the emergence of a vast security bureaucracy. The extent of such snooping is extraordinary. Snowden's documents include revelations the US bugged the European Union headquarters. Brazil's government, meanwhile, has said it might contact Snowden over allegations the US monitored phone calls and emails there.

"You can't have 100 per cent security and also then have 100 per cent privacy and zero inconvenience," Obama told a Californian crowd last month.

The growing ease of whistleblowing, in part, has prompted this punitive response from authorities, desperate to stay in control. Within the whistleblowing community such crackdowns are called "mobbings": the whistleblower is surrounded like a foreign virus in the body and attacked and isolated until expelled.

The "intensity and extremity" of this punitive pursuit reflects the times we live in, says Griffiths University's Professor A.J. Brown, an expert on whistleblowers. "It's almost as if it reveals the desperation of institutionalised national security interests to try to keep control over information in an era where that is inherently becoming more and more difficult."

Drake has described the attacks on Snowden as a distraction from a greater concern. "The government is desperate to not deal with the actual exposures, the content of the disclosures. Because they do reveal a vast, systemic, institutionalised, industrial-scale Leviathan surveillance that has clearly gone far beyond the original mandate to deal with terrorism — far beyond."

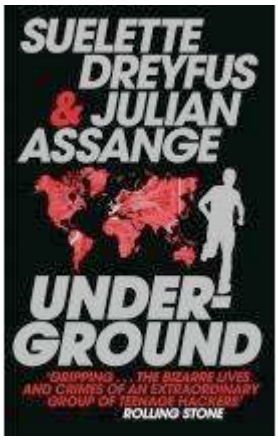
The new documentary *War on Whistleblowers* catalogues the casualties of this pursuit of perceived enemies from within. Marine Corps senior science adviser Franz Gayl lost his security clearance and work prospects after exposing the Pentagon's delays in getting armoured vehicles to

US troops in Iraq. Michael DeKort lost his job at Lockheed Martin for exposing flaws in the ships the contractor was building for the US Coast Guard.

In both cases, the nature of what they revealed offered no respite from prosecution. Gayl's actions saved the lives of many US soldiers. DeKort exposed the sheer absurdity of fitting Coast Guard boats with non-waterproof radios.

Mainstream media can be bypassed in this process. DeKort posted a video on YouTube revealing his concerns. Snowden, meanwhile, is being assisted in his flight by WikiLeaks.

Melbourne University's Dr Suelette Dreyfus, the author of *Underground*, a book about a group of hackers including a young Julian Assange, says technology has changed the game for every player.



While digital tools — such as encryption programs — have made whistleblowing easier, authorities are turning the same technology inward to spy on employees and to plug leaks. Some investigative journalists complain fewer whistleblowers are coming forward for fear of being tracked down.

Snowden, ever the idealist, reckons "draconian responses simply build better whistleblowers." "Citizens with a conscience are not going to ignore wrongdoings simply because they'll be destroyed for it: the conscience forbids it."

But inadequate whistleblower laws across the globe are a disincentive, says Dreyfus. "One whistleblower I interviewed said: 'Sometimes I see these guys and it's like all they have left in their lives are the boxes of documents they have taken with them. They end up living in a caravan, isolated, left without spouse or house, and hiding from people wanting to harm them. All they have left are these boxes'."

What might we call Snowden? A whistleblower is someone who reveals inside information or the internal workings about serious wrongdoing within an organisation.

Manning faces a possible life sentence for allegedly "aiding the enemy," by providing secret material to WikiLeaks. Yet that included video of a US air strike in Afghanistan that killed dozens of civilians — a brutal case of serious wrongdoing.

Snowden, meanwhile, has revealed details of a secret surveillance system operating in the US and abroad without any of the apparent checks and balances essential in a democracy. A new poll in the US has found more Americans believe he is a whistleblower than a traitor — and the public mood might win the day.

The term whistleblower originally meant to stop foul play, as on the sports field. In the 1930s in the US the term took a negative turn — becoming the equivalent of a "snitch" — before growing in public esteem over subsequent decades.

In Australia, whistleblowers have rarely found favour with the public or authorities. Federal independent MP Andrew Wilkie quit his job with the Office of National Assessments, in 2003, to publicly question the government's justifications for the Iraq War. He says whistleblowers here are and have always been treated appallingly. "Maybe whistleblowers are seen to be dobbing on their mates or letting the team down."

An online survey in 2012, commissioned by Griffith and Melbourne universities, found 81 per cent of those surveyed consider it more important to support whistleblowers for revealing serious wrongdoing in organisations than to punish them. Yet only 53 per cent of respondents saw it as "generally acceptable" for people to speak up about serious wrongdoing if it meant revealing inside information.

The dogged pursuit of Allan Kessing reflects such a culture, in part. The former customs officer was convicted under the Crimes Act in 2007 for leaking two damning reports on lax security at Sydney Airport.

Kessing, who maintains he did not leak the reports to *The Australian*, was given a nine-month suspended sentence. That his revelations prompted an inquiry and a $200 million upgrade in airport security has not convinced the Labor government to pardon him, despite speaking in his favour while in opposition.

It is hoped the passage of new whistleblower protection laws by the Federal Parliament, in June will offer greater security to future whistleblowers. But the exclusion of intelligence agencies and some politicians from its ambit means the fate awaiting many whistleblowers here remains up in the air.

Meanwhile Snowden sits somewhere in a 1.6-kilometre airport transit corridor, wondering when his flight will end. He has not been seen in many days. That Sheremetyevo Airport boasts a new counselling service for passengers suffering pre-flight jitters is little consolation. For now, at least, he is going nowhere.

On Bradley Manning and America

Richard Falk
blog, 22 August 2013

I am posting on this blog two important texts that deserve the widest public attention and deep reflection in the United States and elsewhere. I would stress the following:

— the extraordinary disconnect between the impunity of Bush, Cheney, Rumsfeld, Yoo, and others who authorized and vindicated the practice of torture, were complicit in crimes against humanity, and supported aggressive wars against foreign countries and the vindictive rendering of "justice" via criminal prosecutions, harsh treatment, and overseas hunts for Snowden and Assange, all individuals who acted selflessly out of concern for justice and the rights of citizens in democratic society to be informed about governmental behavior depicting incriminating information kept secret to hide responsibility for the commission of crimes of state and awkward diplomacy; a perverse justice dimension of the Manning case is well expressed in the statement below of the

Center of Constitutional Rights "It is a travesty of justice that Manning who helped bring to light the criminality of U.S. forces in Iraq and Afghanistan, is being punished while the alleged perpetrators are not even investigated." And "We fear for the future of our country in the wake of this case."

— the vindictive punishment of Bradley Manning, a historically stiff imprisonment for the unlawful release of classified documents, a dishonorable discharge from military service that is a permanent stain, a demotion to the lowest rank, and imprisonment for 35 years;

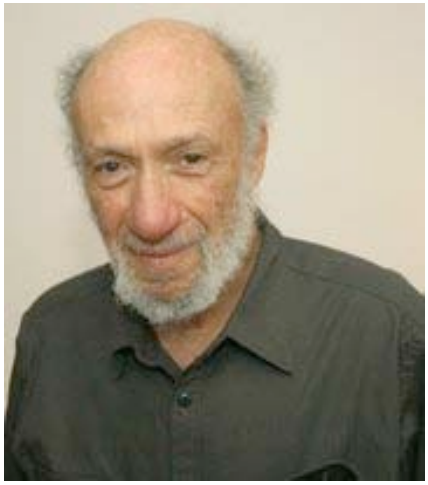
— the failure of the prosecution or the military judge or the national leadership to acknowledge the relevance of Manning's obviously ethical and patriotic motivations and the extenuating circumstance of stress in a combat zone that was producing observable deteriorations in his mental health;

— an increasingly evident pattern of constructing a national security state that disguises its character by lies, secrecy, and deception, thereby undermining trust between the government and the people, creating a crisis of legitimacy; it is part of the pattern of "dirty wars" fought on a global battlefield comprehensively described in Jeremy Scahill's book with that title;

— the mounting challenge directed at President Obama to grant Manning's request for a presidential pardon, and to reverse course with respect to the further authoritarian drift that has occurred during his time in the White House; ever since Obama's Nobel Prize acceptance speech when he claimed American adherence to the rule of law, it has been evident that such a commitment does not extend to high level governmental violators at home ("too important to prosecute") or to the sovereign rights of foreign countries within the gunsights of the Pentagon or the CIA or to the crimes of America's closest allies; international law is reserved for the enemies of Washington, especially those who resist intervention and occupation, or those who dare to be whistle-blowers or truth-tellers in such a highly charged atmosphere that has prevailed since the 9/11 attacks; the opening of Manning's statement below suggests the relevance of such a context to the evolution of his own moral and political consciousness;

— the noted author and public intellectual, Cornel West, offered a salutation to Manning relating to his announcement about his/her gender identity shift that I wholeheartedly endorse: "My dear brother Bradley Manning — and from now on sister Chelsea Manning — I still salute your courage, honesty and decency. Morality is always deeper than the law. My presence at your trial yesterday inspires me even more!"

— read Bradley Manning's statement and ask yourself whether this man belongs in prison for 35 years (even granting eligibility for parole in seven years), or even for a day; imagine the contrary signal sent to our citizenry and the world if Manning were to be awarded the Medal of Freedom! It is past time that we all heeded Thomas Jefferson's urgent call for "the vigilance" of the citizenry as indispensable to the maintenance of democracy.



Richard Falk is an international law and international relations scholar who taught at Princeton University for forty years. Since 2002 he has lived in Santa Barbara, California, and taught at the local campus of the University of California in Global and International Studies and since 2005 chaired the Board of the Nuclear Age Peace Foundation. He initiated this blog partly in celebration of his 80th birthday.

Statement by Bradley Manning on being sentenced

The decisions that I made in 2010 were made out of a concern for my country and the world that we live in. Since the tragic events of 9/11, our country has been at war. We've been at war with an enemy that chooses not to meet us on any traditional battlefield, and due to this fact we've had to alter our methods of combating the risks posed to us and our way of life.

Bradley/Chelsea Manning

I initially agreed with these methods and chose to volunteer to help defend my country. It was not until I was in Iraq and reading secret military reports on a daily basis that I started to question the morality of what we were doing. It was at this time I realized in our efforts to meet this risk posed to us by the enemy, we have forgotten our humanity. We consciously elected to devalue human life both in Iraq and Afghanistan. When we engaged those that we perceived were the enemy, we sometimes killed innocent civilians. Whenever we killed innocent civilians, instead of accepting responsibility for our conduct, we elected to hide behind the veil of national security and classified information in order to avoid any public accountability.

In our zeal to kill the enemy, we internally debated the definition of torture. We held individuals at Guantanamo for years without due process. We inexplicably turned a blind eye to torture and executions by the Iraqi government. And we stomached countless other acts in the name of our war on terror.

Patriotism is often the cry extolled when morally questionable acts are advocated by those in power. When these cries of patriotism drown out any logically based intentions [unclear], it is usually an American soldier that is ordered to carry out some ill-conceived mission.

Our nation has had similar dark moments for the virtues of democracy — the Japanese-American internment camps to name a few. I am confident

that many of our actions since 9/11 will one day be viewed in a similar light.

As the late Howard Zinn once said, "There is not a flag large enough to cover the shame of killing innocent people."

I understand that my actions violated the law, and I regret if my actions hurt anyone or harmed the United States. It was never my intention to hurt anyone. I only wanted to help people. When I chose to disclose classified information, I did so out of a love for my country and a sense of duty to others.

If you deny my request for a pardon, I will serve my time knowing that sometimes you have to pay a heavy price to live in a free society. I will gladly pay that price if it means we could have country that is truly conceived in liberty and dedicated to the proposition that all women and men are created equal.

Statement of the
Center for Constitutional Rights
21 August 2013

Today, in response to the sentencing of Pfc. Bradley Manning, the Center for Constitutional Rights issued the following statement.

We are outraged that a whistleblower and a patriot has been sentenced on a conviction under the Espionage Act. The government has stretched this archaic and discredited law to send an unmistakable warning to potential whistleblowers and journalists willing to publish their information. We can only hope that Manning's courage will continue to inspire others who witness state crimes to speak up.

This show trial was a frontal assault on the First Amendment, from the way the prosecution twisted Manning's actions to blur the distinction between whistleblowing and spying to the government's tireless efforts to obstruct media coverage of the proceedings. It is a travesty of justice that Manning, who helped bring to light the criminality of U.S. forces in Iraq and Afghanistan, is being punished while the alleged perpetrators of the crimes he exposed are not even investigated. Every aspect of this case sets a dangerous precedent for future prosecutions of whistleblowers — who play an essential role in democratic government by telling us the truth about government wrongdoing — and we fear for the future of our country in the wake of this case.

We must channel our outrage and continue building political pressure for Manning's freedom. President Obama should pardon Bradley Manning, and if he refuses, a presidential pardon must be an election issue in 2016.

Manning pays price of embarrassing US

Paul McGeough
The Age, 23 August 2013, p. 15

COMPARED with the vastly shorter sentences dealt to other leakers, and taking into account that he might not be released until 10 years after the documents he leaked are declassified, WikiLeaks source Bradley Manning is being harshly punished — 35 years in a military prison.

In 1985, the first government worker to be jailed for leaking to the media was a former US Navy intelligence officer who gave classified satellite photographs to Jane's Defence Weekly. He went down for just two years.

More recently, under the Obama administration, an FBI linguist went away for 20 months; a National Security Agency employee got off with a year on probation and community service; and a guy from the CIA went away for 30 months.

Given that Washington has failed to substantiate its claims of gross damage to the US, its employees and their sources, the Manning sentence seems way out of line with just 10 years for the ringleader in the Abu Ghraib prison scandal — who was released after serving just 6½ years.

Ben Wizner, director of the American Civil Liberties Union's speech and technology project, told reporters: "When a soldier who shared information with the press and the public is punished far more harshly than others who tortured prisoners and killed civilians, something is seriously wrong with our justice system."

It was hard not to conclude after military judge Colonel Denise Lind took just two minutes to dispatch Manning on Wednesday that the 25-year-old was being so severely punished not so much because he damaged the US government as because he embarrassed it.

Sitting on a mountain of classified material, he figured leaking it would spark a useful public debate about Iraq and Afghanistan.

He showed the world the callousness of a US helicopter crew killing civilians — and the callousness of Washington in denying the existence of the video to the Reuters news agency, which employed two of the dead.

Manning revealed the abuse of detainees by Iraqi officers — as US minders turned a blind eye. And he showed that civilian deaths in the Iraq war probably were much higher than official estimates.

After a brief meeting with Manning and some of his family after the decision, defence lawyer David Coombs told *The Guardian*: "The only person that wasn't emotional was Brad — he looked to us and said, 'It's OK, I'm going to move forward and I'm going to be all right'."

Next week, there will be a plea to the White House for a pardon. The lawyer read from a personal message to Barack Obama that will be included: "If you deny my request for a pardon, I will serve my time knowing that sometimes you have to pay a heavy price to live in a free society."

Manning has Buckley's chance if he thinks he can turn Obama, who ran for office as a champion of whistleblowers but now presides over an aggressive campaign to lock them up.

Canada's invisible government

Katherine Jaconello

IN 2010, I was sued for libel and conspiracy. It was a legal action that fits into the category of Strategic Lawsuits Against Public Participation — SLAPPs — that are designed to deter citizens from speaking out on matters of public interest.

I am writing this in the hopes that I can console those who endure this type of horrible experience and the after-effects, which are considerable. It is only now — three years later — that I am capable of working on the projects I was doing before the deadly day when I received the Notice of Libel.

In August 2010, the Honourable Kevin Daniel Flynn, Member of the Provincial Parliament of Ontario, presented a document to the Speaker of the Legislative Assembly of Ontario with these words:

> Your Select Committee on Mental Health and Addictions has the honour to present its *Final Report* entitled *Navigating the Journey to Wellness: The Comprehensive Mental Health and Addictions Action Plan for Ontarians* and commends it to the House.

With these noble words, he put into the hands of the government the plan to administer to every unhappy man, woman and child, experimental psychiatric drugs, electroconvulsive shock and brain surgery by psychiatrists who, in their own medical journals, admit their body of knowledge is unworkable. Their treatments are falsely promoted as safe and effective by their associations.

Perhaps the process of polling 230 presenters and reviewing 300 submissions seems workable. It is not. I know from one little corner of the universe that it is not.

Buried in the back pages of that report are the presenters. One of those presenters sued me and nine others for libel and conspiracy on the very day they met with the Select Committee on Mental Health. We ten people had one thing in common — we knew the truth about what psychiatric community centres *really* do to kids. All of us were silenced with a "cease and desist order."

I was charged with being the founder of a movement to stop the drugging of children. Strangely enough, I guess I was. Eight years before, I had typed up a little flyer on my computer calling for a movement to stop the drugging of children with psychotropic drugs. Though I only gave out one or two of those flyers, the concept ended up on the Internet and was catching on. I knew a young fellow, John, who so passionately hated the place where he had been involuntarily committed as a child that he seized upon the idea to find the kids who had been drugged against their will.

John had been forced to take Ritalin and Concerta as a child, prescribed by a paediatrician. When he had side effects, he was involuntarily committed to this psychiatric hospital for children. According to him, he was tranquillised and restrained, eventually discharged with an inconsolable hatred of the place. Over the years, he got himself off the drugs. When the school gave him an ultimatum — "Ritalin or no school" — he quit school. He busied himself with a website using the name of this psychiatric hospital, exposing their human rights abuses. With Facebook and other social media, he obtained a following of children who had similar upbringings. On his website, he would include names of people who helped him. I was one of those people. The kids made it known that they wanted the place shut down.

The directors of this private psychiatric hospital, in preparation for appearing before the Select Committee on Mental Health, alleged a "conspiracy" among those listed on the website and filed the SLAPP against them. Once they had cleared the way for their appearance, they promoted their private hospital as a "holistic centre" for kids in order to get more money and power. They already receive $16 million a year from three levels of government.

I had been reporting on conflicts of interest of psychiatrists for 10 years — since psychiatrists nearly destroyed my mother with their lethal drugs. My job at our medical centre is to read the medical journals. I had done so for 28 years. I had been privy to the "bling" era of ghostwriting for the promotion and sale of dangerous psychiatric drugs, shock and brain surgery as "safe and effective." I reported instances of fraud and ghostwriting to the Investigations Committee of the College of Physicians and Surgeons of Ontario. I was constantly labelled "vexatious."

On the SLAPP, I was charged with founding a movement to stop the drugging of children, with opposing psychiatric drugs for children and with reporting on psychiatrists. Mostly, the people charged did not know each other so we did not cooperate. I think that was a mistake as the lawyers for the directors of this hospital insisted on ignoring the truth and treating us as one, so no one was let off unless all agreed on a settlement. I would say to anyone charged with conspiracy — work together.

At this difficult time, I turned to my government. My Member of Provincial Parliament, my Member of Parliament, the Attorney General and the Premier all closed their doors. The Premier told me to go to the Law Society. There, I was referred to a lawyer who wanted a $20,000 retainer, told me I was in trouble, that the directors would attach my assets, that my children would never get an inheritance and that it would drag on for ten years. She met me in a coffee shop by the courthouse and charged me $250 for the advice. I was terrified and could not eat or sleep. I thought I had ruined my family's life.

I called the lawyers for this psychiatric institution and asked if we could meet and get the website taken down. The lawyer consulted with his clients who told him "no concessions."

I found my own lawyer on the Internet — a nice fellow who guided me by email first, then charged me a $5,000 retainer and tried not to spend my money. He was a young lawyer starting out.

I helped to research my own statement of defence and in doing so, found the notes recorded by the Ontario Legislature from the date of the SLAPP's beginning. That's how I found out that those men were in front of the Select Committee on that day. Then I knew there was corruption. I was told by my lawyer to forget about proving anything. These men got away with lying in court documents because it would have cost me $200,000 to prove otherwise. I would advise anyone going through this to work hard on researching your own case. Don't trust anyone else.

When the SLAPP came down, it had the "cease and desist order" which meant we all had to be silent. We thought we would end up in jail if we stated the truth. This was the summer of the G8 meeting in downtown Toronto, and the massive protests against it, when hundreds of people were being tried for trumped up conspiracies and put in jail. It made the whole thing much more frightening.

One consoling fact was that the Attorney General's office had an Anti-SLAPP panel looking into these bullying lawsuits. Our suit was reported to them. It is only thanks to the writings of Professor Brian Martin at the University of Wollongong in Australia that I even learned what a SLAPP was. Once again, research on the Internet helped me. Somehow, our SLAPP ended up being immortalised on Wikipedia.

Note from Brian Martin: here is an extract from the Wikipedia entry on "Strategic lawsuit against public participation," 26 September 2013:

• In May 2010, Youthdale Treatment Centres of Toronto, Ontario filed a defamation suit against various former patients, parents of former patients, and other persons, claiming C$5,000,000.00 in damages.[citation needed] The lawsuit, filed on May 5, 2010 on behalf of Youthdale by Harvin Pitch and Jennifer Lake of Teplitsky, Colson LLP claimed that these persons were involved in a conspiracy to, among other things, have Youthdale's licence to operate revoked. Youthdale also claimed their reputation was damaged as a result of various actions by the named defendants, which Youthdale alleged included the creation of websites and blogs containing complaints against Youthdale, including alleged accusations of unlawful administration of psychotropic medications. A notable left-turn for Youthdale occurred in July 2010, when Youthdale became the subject of a Toronto Star investigation, in which it was found that Youthdale had been admitting children to its Secure Treatment Unit that did not have mental disorders.[47] The case is still ongoing against some of the named defendants.

The actual "claim" has 58 pages and 165 paragraphs. These detail the workings of the place and take each person charged separately. It basically outlines the statements on John's website, saying that they are false and injurious. Unfortunately for them, a local newspaper dedicated several issues to exposing the abuses of this place in the summer of 2010. That newspaper was not sued for libel. My opinion is that the directors of that psychiatric hospital thought I was involved in the production of that newspaper's expose. I was not.

How did it end? When the Select Committee disbanded and put out its report in the fall of 2010, they dropped the suit and paid half my lawyer's fees. The psychiatrists bought John's website. They also registered the title of the flyer that I wrote eight years ago as a domain on the Internet. I have gone on to dedicate my time to researching the abuses of psychiatry and writing about it to create a public outcry. John is in college, studying law to take on the abuse of children by psychiatry and Children's Aid. Another woman heavily promotes human rights for youth. I don't know what happened to the others.

The psychiatric community centre got what it wanted from government and continues to publish slick reports to get clients.

Though I have contacted many government departments, political leaders and humanitarians about the flawed action of the Select Committee on Mental Health, not one has been interested. The only exception is a professor of ethics at the University of Minnesota. Of course, I never mention the name of this hospital as I was forced to sign a paper saying that I would never say anything bad about this place.

Here we have a legal document — *Navigating the Journey to Wellness* — enshrined in Ontario's legislature whose "truths" were the truths of vested interests with millions to spend on legal actions to silence knowledgeable people and to effectively, legally and with full support of the Attorney General terrorise helpless individual citizens.

I learned through this SLAPP that government operates mainly as a public relations department. It is powerless and not interested in the operation of this invisible government. It is, on the contrary, heavily invested in their actions and in the development of psychotropic drugs and, come hell or high water, they want their payback.

This invisible government — psychiatry — has used public funds to shift public opinion to support a medical/psychiatric public and mental

health movement that will drug them with dangerous, experimental and unworkable psychiatric drugs, that will shock them with electroconvulsive shock to destroy brain tissue and that will operate on them with operations they state to be "safe and effective" such as DBS (deep brain stimulation) and anterior capsulotomy (heated wires inserted into the brain through holes in the skull to burn brain tissue and create a lesion). All this will be supported by a system of informants, access to private medical information, easier involuntary commitment and court orders.

The naivety and ignorance of the entire world concerning the dangers of psychiatry is a frightening fact. Who would ever believe what they do? *They do it. They are doing it. They will do it to you.*

Though this happened in Canada, by Canada's invisible government, it should be of concern to everyone who has someone they care about. The only solution is public understanding.

BOOK REVIEW

Willful blindness

reviewed by Brian Martin

Whistleblowers see a problem and speak out about it. But what about the people who know there's a problem but say nothing? What about those who can't even see there's a problem?

If you're wondering about these questions, get a copy of Margaret Heffernan's book *Willful Blindness.* She surveys the evidence about how and why people turn away from unwelcome information, often to their own detriment.

She starts with a very personal issue: being oblivious to the shortcomings of those closest to us. She married a man who, due to a heart condition, had a short life expectancy. But she ignored this — because she was in love. She provides heart-wrenching stories of other relationships that continue despite abuse and betrayal.

Many people who use sun beds to acquire a tan become angry when confronted with evidence about their harmful effects on health. Many who are deeply in financial debt are completely oblivious to their plight. Heffernan:

> We know — intellectually — that confronting an issue is the only way to resolve it. But any resolution will disrupt the status quo. Given the choice between conflict and change on the one hand, and inertia on the other, the ostrich position can seem very attractive. (p. 96)

Not wanting to know about problems, or doing nothing about them, occurs in all sorts of situations. Major engineering disasters, such as the collapse of levees that devastated New Orleans during Hurricane Katrina in 2005, can be traced to bureaucratic systems in which warnings were repeatedly ignored. In German-occupied Europe in the early 1940s, there were many who knew about Nazi atrocities, but turned away.

Margaret Heffernan

There's quite a lot of research that helps explain this very human failing. One factor is conformity. Solomon Asch did pioneering experiments in the 1950s in which subjects assessed which of three lines was the same length as a reference line. When others in the room — confederates of the experimenter — chose the wrong line, even though it was obviously wrong, many subjects conformed and denied the evidence of their own eyes. Going against the group can indeed be uncomfortable.

Then there were Stanley Milgrim's experiments on obedience to authority, in which subjects willingly gave electric shocks to another person (an actor who wasn't actually shocked) up to highly dangerous levels, with no more than an experimenter with a white coat to urge them on.

In a corporation or government department, these two influences come together. When the boss expresses a view, most subordinates will acquiesce, and when most others acquiesce, many of them literally cannot see any problem: they deny the evidence of their senses. This helps explain the giant corporate disasters such as Enron.

Reflective military officers know from experience that blind obedience can be damaging, and even contribute to war crimes. However, many business executives do not understand this.

> … business colleagues seemed to envy what they imagined to be the military model of obedience — just do as you're told — and were unaware that the model is dangerous and out of date. That the military itself doesn't regard blind obedience as an admirable goal should give any executive pause. Some of the gravest mistakes in both the business and the political world have been caused by eager executives, keen to please, hungry for reward, and convinced that blind obedience was their path to success. Who is more willfully blind: the executives who believe this, or their leaders who allow them to? (pp. 123–124)

Then there is the problem of taking responsibility. If experimental subjects are put in a room doing some mundane task, and smoke gradually starts filling the room, nearly everyone will raise the alarm — if they are doing the task on their own. If there are several subjects in the room at the same time, they are likely to continue with the task until they can hardly see. Each individual thinks, "the others aren't doing anything, so I shouldn't worry." One implication is that in the case of an emergency, it's better to ask an individual to help than to ask an entire group. Heffernan comments: "The experiment indicated that the larger the number of people who witness an emergency, the fewer who will

intervene. Collectively, we become blind to events that, alone, we see readily." (p. 148)

In some cases of apparent neglect, when people turn away, they literally do not register what is happening. Studies show no brain activity to correspond with sensory inputs. When people say they didn't see or hear something, they can be quite sincere: it didn't register in their conscious mind.

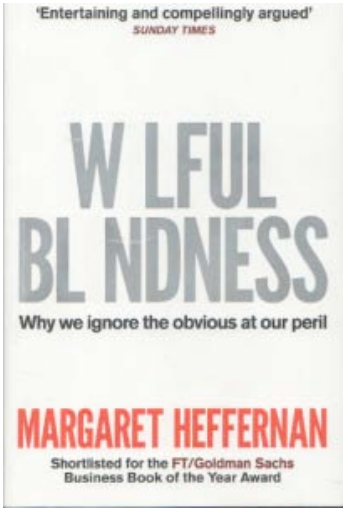
Willful Blindness is an engaging treatment of these issues. Heffernan interviewed psychologists, business people and many others to provide personal commentary about the issues. She tells numerous stories about the disastrous effects of remaining unaware of serious problems.

> You only have to mention the words *willful blindness* to hear the same story about a different industry: how beverage companies ignored the advent of vitamin drinks; packaged goods businesses don't think it matters whether products are environmentally sound; pharmaceutical companies don't pay attention to off-label prescribing; and gun manufacturers still pretend a secondary market (selling to kids and criminals) has nothing to do with them. The knowledge is there, spoken or unspoken, but the executives do nothing. (p. 155)

What to do? Heffernan gives pride of place to whistleblowers and dissidents, giving many stories of heroic intervention. She also offers suggestions for better practice, for example advising bosses not to let subordinates know their views before discussion proceeds. She tells about a time when she was the boss and couldn't attend a meeting: that was the time when her team came up with the best ideas, because they could acknowledge problems and change their minds without loss of face. She says "In fact, of course, being a truly good team player involves having the confidence to dissent — but this is rarely what's involved in this trite accolade" (p. 138).

The implication is that whistleblowing is valuable, but is only part of the solution. As well, society needs systems that overcome the human tendency to ignore looming problems due to conformity and obedience. Last, and not least, money is part of the problem.

> All the other organizational forces of willful blindness — obedience, conformity, bystander effects, distance, and division of labor — combine to obscure the moral, human face of work. Money keeps us very busy, often too busy, to see clearly and work thoughtfully. It keeps us silent, too, fearful lest debate or criticism jeopardize salaries. Money reinforces and often appears to reward those core, self-identifying beliefs that blind us to alternatives and to argument. You could say that if we are just obeying orders, fitting in, diffusing responsibility for people who are a long way away and, anyway, may not be our concern at all — then money is the final incentive to keep looking away. The fact that money tends to be addictive — the more we have, the more we feel we need — merely ensures that the cycle is rewarded and perpetuated. To paraphrase Edmund Burke, all that evil needs to flourish is for good people to see nothing — and get paid for it. (p. 194)



Margaret Heffernan, *Willful Blindness: Why We Ignore the Obvious at Our Peril* (New York: Walker & Company, 2011)

Brian Martin is editor of *The Whistle*. Thanks to Anu Bissoonauth-Bedford and Ian Miles for helpful comments on a draft of this review.

The increasing appeal of Lincoln's Law

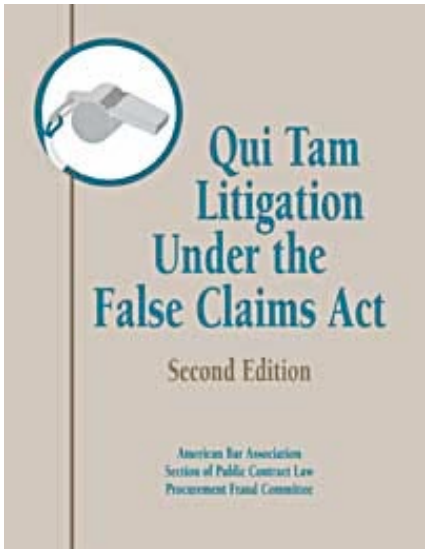
Kim Sawyer

In recent months, there has been increasing public support for a False Claims Act (FCA) for Australia. Articles have appeared in several newspapers advocating the introduction of an FCA, paralleling the US model, including Ben Allen, "Pay the piper and we may end public fraud" (*Sydney Morning Herald,* 7 May), Noel Towell and Markus Mannheim, "Fraud spotters fees could save billions" (*Canberra Times,* 7 May), Ruth Williams and Ben Butler, "Push to give whistleblowers a cut" (*Sydney Morning Herald,* 5 June). The United States FCA allows individuals to litigate on behalf of the US Government to prosecute those who falsely claim on the Government. The FCA was an old law which had become dormant until 1986 when legislators realised that inside information was required to combat a culture of non-compliance in government contracting. The FCA depends on whistleblowers with access to specific information unravelling anomalies in contracting. The whistleblower is compensated as part of the process. There are now many advocates for an Australian FCA, including the Australian Federal Police, the Tax Justice Network, various law firms, and a number of legal academics — and of course whistleblowers themselves. Apparently, the time for an Australian FCA has arrived.

As one who has advocated for a FCA since 1996 when at the Whistleblowers Australia conference in Melbourne I first suggested this should be considered in Australia, I am puzzled as to why there has been a sudden realisation that Lincoln's Law, as it is termed in the US, is now appropriate for Australia. My puzzlement is in part attributable to the fact that advocacy for a FCA has not always been so favourably received. In January 2004, I wrote an opinion article in the Melbourne *Age* entitled "How Australia should fight white collar crime." In that article, I argued for the introduction of a False Claims Act, citing its effectiveness in both the recovery of fraud and the protection of whistle-

blowers. I cited the cumulative fraud recovery in the US at the beginning of 2004 as totalling $6 billion. Today that cumulative recovery exceeds $40 billion. Two days after my opinion article, *The Age* editorialised with the headline "Protect, not pay, whistleblowers." They commented "Enticing whistleblowers by monetary rewards seems morally repugnant and runs the risk of attracting maliciously based information or tainted evidence of suspect credibility." Unfortunately, this argument has been the customary rejoinder to many of the articles and submissions I have made on the subject since 1996. In Australia, there has been an aversion to compensation for whistleblowers, even by strong proponents of whistleblowing reform. As recently as December 2008 on the ABC's "Law Report," I argued for the introduction of a FCA; yet on the same program, Dr AJ Brown, a leading advocate for whistleblowing reform, stated

> … in fact offering rewards for that is something that isn't necessarily going to encourage any more reporting than should occur. Potentially sends some bad messages in terms of encouraging reports that otherwise wouldn't occur than being made for pecuniary motives.



I should note that I have used the term compensation in relation to the FCA, not reward or bounty, because the FCA represents compensation for the risk of blowing the whistle. Compensation for risk is the principle which underpins our economic system. It is the principle which underpins investment. It is the principle which underpins insurance. And it is the principle which should underpin whistleblowing.

The response of *The Age* showed whistleblowers to be in a special category. It is doubtful that *The Age* would have so editorialised if I had been a member of another minority group advocating for better protection against discrimination. But then again I was a whistleblower. Whistleblowers are in a special category. They can advocate, but not fully. They are listened to, but not fully. Their submissions are read, but not fully. Their arguments are accepted, but not fully. It is the price they continue to pay for their whistleblowing. It is their loss of credibility for blowing the whistle.

So why now the increased support for an Australian FCA? There are four reasons as I see it. First, the overwhelming evidence of the effectiveness of the False Claims Act in combatting fraud is difficult to ignore. As the Taxpayers Against Fraud Center in Washington have noted

> Since 1987, False Claims Act lawsuits have returned over $40 billion to federal and state Governments. Of this sum, over $31 billion has been recovered to the federal government as a consequence of civil settlements and judgments. An additional $4 billion has been returned to the states as a consequence of False Claims Act-initiated Medicaid settlements, and an additional $5 billion has been collected by the federal government in criminal fines associated with False Claims Act-initiated actions.

Hence it is not surprising that criminal justice authorities are advocating an Australian FCA. In a bulletin dated 12 November 2012, the Australian Federal Police Association (AFPA) wrote

> During the 2010 federal election, the AFPA sought a commitment from the major political parties to consider the introduction of a Qui Tam False Claims Bill for Australia to address fraud on the Commonwealth, in particular. Both major parties committed to consider the AFPA proposal. After the 2010 federal election, the AFPA met with the then Attorney-General Robert McClelland and at his invitation, the Attorney-General's Department, to discuss our proposal. The AFPA received a positive response.

As an aside, I note that over the years I requested to meet with four different federal attorneys-general to discuss an Australian FCA, but have never been granted that privilege. But, then again, I am a whistleblower.

"It's that pesky fellow Kim Sawyer again, wanting a meeting. Just say no."

The second reason why an Australian FCA is on the agenda is the advocacy of law firms and legal academics. As US practice has shown, the FCA constitutes a public-private partnership: theoretically a partnership between the whistleblower and the government, in reality a partnership between a whistleblower, the government and a law firm which shares the proceeds of the litigation. There are many US law firms that specialise in *qui tam* actions, as FCA legal actions are called; they are listed at the top when you Google FCA. An Australian FCA would open a new frontier for law firms, and I expect many to seek a first mover advantage. The 12 November AFPA bulletin cited above referenced a federal government workshop held at the ANU College of Law in October last year to "investigate aspects of the US FCA that could be incorporated into government legislation for Australia." The conference was a

> by invitation only workshop with 40 people from federal government departments, the Australian Law Council, AFP, Law Societies, the Insurance Industry, the ANU, offices from the US Department of Justice,

and private False Claims "relator" firms and the AFPA.

But evidently no whistleblowers. If the FCA is to be a partnership, it has to be a real partnership.

The third reason why an Australian FCA is likely is because the US FCA is increasingly regarded as a deficit reduction act. For governments searching for ways to close the gap between revenue and expenditure, the FCA is an obvious mechanism. The Australian federal government deficit currently exceeds $40 billion or 3% of GDP. In my paper "Lincoln's Law, an analysis of an Australian False Claims Act," I showed that the federal government could expect to recover over the next decade more than $1 billion from implementation of an FCA, and possibly as much as $8.5 billion. Furthermore, I showed that an FCA could deter as much as $30 billion of fraud against the federal government. Estimates of this magnitude cannot easily be ignored, even by the most profligate of governments.

There is a final reason for the increased support for an Australian FCA, and that involves whistleblowers. It is now 20 years since Senator Jocelyn Newman first proposed what became the Senate Inquiry into Public Interest Whistleblowing, yet the first comprehensive legislation is only now proceeding through the federal parliament. The current legislation is less than that envisaged by Senator Newman's committee. But an FCA would be a great leap forward, and annul much of the obfuscation of the last 20 years. In "Lincoln's Law, an analysis of an Australian False Claims Act", the advantages to whistleblowers are summarised.

1. Specific protection against any form of discrimination in the terms of employment, including restitution to previous employment status, compensation for any damages resulting from discrimination and any litigation costs.
2. As a civil law statute, the FCA operates under the lowered evidence standard of preponderance of evidence.
3. *Qui tam* actions reverse the *onus of proof*. The plaintiff is the whistleblower, the defendant the false claimant.
4. When the Department of Justice intervenes, the whistleblower's litigation costs are met by the government.
5. The whistleblower is guaranteed a share of the government's recovery of fraud in a successful prosecution. Payments to *qui tam* plaintiffs average more than 16% of the proceeds of the actions.

Australian whistleblowers are owed an FCA for 20 years of government inaction. I look forward to a newspaper editorial of the future headed "Protect, compensate, but not overcompensate whistleblowers." Then I would understand that others understand.

Kim Sawyer worked for many years in economics and finance at RMIT and Melbourne University. He is now attached to Historical and Philosophical Studies at Melbourne University. He is a whistleblower and a longstanding supporter of whistleblowers and whistleblower law reform.

Whistleblowing: a practical guide

While I was president of Whistleblowers Australia in the late 1990s, I talked to many whistleblowers. Most of their stories were similar, and hence I often provided the same sort of advice. To avoid having to say the same thing over and over, I decided to write a book, *The Whistleblower's Handbook,* published in 1999.

A few years ago, after the book had sold out, I was able to put it on the web. Quite a few whistleblowers have told me how much they learned by reading it.

This year, I had the opportunity to prepare a revised edition. As well as updating and revising the text, I've added two new chapters, one on low-profile operations — bringing about change without speaking out — and leaking.

The new edition is titled *Whistleblowing: A Practical Guide.* It is published by Irene Publishing, based on Sweden. You can purchase copies at http://lulu.com for about $40. A free online version will be available on my website later on.

Brian Martin

Extract from *Whistleblowing: a practical guide,* chapter 8, "Leaking"

Most whistleblowers are open about who they are and what they are saying. They report a problem to the boss or make a complaint to an agency or contact the media. Because they are open, they often become targets for reprisals.

Another option is to reveal problems without revealing your identity. This means you are anonymous. Your boss and your co-workers may know or believe that someone has revealed information to outsiders — but they don't know it's you.

> Alana worked for an insurance company and discovered documents showing that top managers were changing the policies for customers living in risky areas without clearly informing them. She saved copies of these documents, electronically cleaned them of identifying information and, from a cybercafe across town, sent them to a citizens' group concerned about insurance company abuses.

Advantages of leaking

The risk of reprisals to whistleblowers is significant: their identity is known, hence they can be easily targeted. Leaking reduces these risks, sometimes greatly reduces them. The main risk is that you will be tracked down as the leaker. The better you are able to avoid detection, the greater the advantage of leaking.

Another major advantage of leaking is that you remain in the job and can collect more information and, if appropriate, leak again to reveal problems. If you speak out and bosses know who you are, they will make sure your access to damaging information is cut off. If bosses don't know it's you, you may continue to have access and be able to leak on future occasions. You might even be put in charge of finding the leaker!

An open whistleblower often has just one chance to expose a problem. After that it is downhill, with reprisals and exclusion from sensitive information. An anonymous whistleblower can have many opportunities to expose a problem. This means the chance of making a difference is much greater. Furthermore, with leaks the attention is more on the issue and less on the person who disclosed information.

These are very big advantages. If you're thinking of speaking out about a problem, you should carefully consider whether it's possible to do so without revealing your identity.

Cynthia Kardell comments

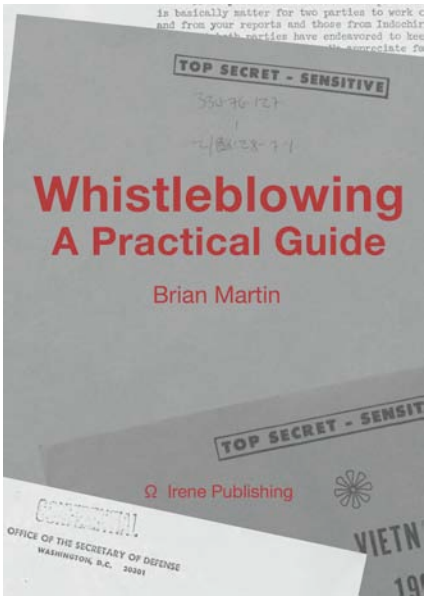
Leaking is often seen as being a bit sneaky, not being upfront and honest. Ignore all that, as it is usually the sort of thing your detractors say to undermine and pull you down. Why make yourself a target when you don't need to?

Anonymous leaking is better than making a confidential disclosure to an investigative body, because it removes the temptation for the investigative body to cast you as the villain.

Leaking is entirely sensible and reasonable, particularly on politically sensitive issues, because all the protections promised by legislation and investigative bodies are only ever useful after you've suffered reprisals.

When leaking is not suitable

• If you've already spoken out, it's too late to be anonymous.
(However, your co-workers could leak — and blame it on you. If that's okay with you, encourage them. If not, then make sure you have convincing evidence that you're not the leaker.)



• If you're easily identifiable, then trying to be anonymous may be futile.

Maybe you're the only person, aside from the boss, with access to particular documents or information. Maybe the key documents are things you personally compiled or wrote. (However, you could "accidentally" leave them around for someone else to obtain and then leak.) Maybe the workplace is so small that you can't hide. Maybe you have the reputation as the person to be blamed for any exposure.

If you are easily identifiable, it may be better to be open in speaking out, thereby giving your statements more credibility, for example if you obtain media coverage.

• Sometimes you don't need to be anonymous.

If you've resigned, found another job, written articles and a book, and are speaking with politicians and regulators, then anonymity is unnecessary, maybe even pointless.

• Sometimes you need to interact with the recipient of your leaks.

You might leak some documents, but those who receive them often want to know more, for example additional evidence, how credible you are, and where the evidence comes from. They may need more information before taking action, or use your anonymity as a pretext to avoid doing anything.

Good investigative agencies, including some media, can set up secure and anonymous communication channels so you can interact with them without revealing your identity. However, the more you interact, the more likely someone will figure out who you are. You might start off being anonymous but end up being known to some people. Think through what might happen to your disclosures and be prepared.

• Sometimes leaking puts you or others in danger.

In some high-risk situations, for example relating to organised crime or some police and military cases, leaking may increase danger. If criminals are involved, they may take reprisals against whoever they think might be the leaker: you and others might be targeted. In such circumstances, leaking can be risky. Curiously, revealing your identity can give greater safety, because if there are serious reprisals — you are assaulted, for example — then others will know who did it and why. If you are anonymous, you can be assaulted without as much public concern, which makes it more likely.

For this reason, witness protection schemes run by police sometimes are better avoided. The idea is good: hide and protect the witness — someone who has seen a crime — so they can't be assaulted, threatened or otherwise prevented from giving testimony. The trouble is that the police running the witness protection scheme may have links with criminals, and you could be at greater risk. If you are open about your identity and location, attackers will know that anything they do will be widely publicised.

In high-risk situations, it's vital to carefully consider options, including not revealing anything. If you're going to leak information, try to assess the ramifications and figure out the best time and methods. This applies to any leaking, but is even more important when lives are at stake.

A whistleblower's guide to journalists

Brendan Jones

I'M a whistleblower, and I wanted media coverage of my story. But how? When my initial efforts were unsuccessful, I decided to find out more about how the media operate. Here's what I learned, drawing on contacts with many journalists and whistleblowers, some of whom are quoted here.

For many whistleblowers, the greatest benefit of going to the media is vindication that a journalist looked at their claim independently and found it was true. This is very powerful, since even politicians take their cue from journalists before taking action or asking questions in parliament.

However whistleblowers need to be realistic. Publication won't put their life back to normal. Abuse against them will continue, and publication only solves a problem 10% of the time.

But the greatest shock to the whistleblower is the discovery that despite the popular image of reporters elbowing each other for scoops, no one will touch their story. It may be too complicated, too difficult to verify, too hot, not significant enough or too old. The biggest problems are lack of time, and that there are far easier stories out there.

Journalists need solid and confirmed leads

The last thing a journalist wants to do is spend time on a story that goes nowhere.

Your story must be solid and confirmed, but this isn't always possible. Corrupt officials tightly control information, so leads can be weak. Fitzgerald inquiry whistleblower Nigel Powell recently said:

> Now, what was I saying then — had I actually seen corruption take place? No. Had I had actual evidence of money crossing hands? No. I had my suspicions, which no longer sounds like it would be enough to make a (CMC) complaint.

To convince a journalist whistleblowers must provide compelling evidence, but that's hard if they're inexperienced, and it may expose them to more danger.

Oral evidence or suspicions are only useful if they lead to documentary evidence, but this can be very hard to get. The public service can sit on Freedom of Information requests for years, and public servants who help journalists risk imprisonment. Google is, however, extremely useful. It can reveal a lot about people, identifying potential conflicts of interests through their relationships. It can familiarise you with the law, and even though corrupt officials will hide many documents, they can't hide all of them. You will be amazed what you can turn up. Find other witnesses, but vet them carefully.

Be warned: journalists cannot tell your story while you have a lawsuit. Lawsuits can drag on for years.

Stories must be fresh and interesting (to people besides you)

Stories are best told fresh, so ideally the whistleblower should approach the journalist right after the incident has taken place. However whistleblowers inevitably first try internal complaints units that stonewall complaints and can sit on them for years. Commonwealth whistleblowing laws force public servants to use these. By that time the story has lost its appeal, and is history, not news.

Stories stand the best chance if they are of "popular interest." Journalist Evan Whitton recommends aiming at the hip pocket nerve: quantify corruption in dollar values, or increased street crime. Stories affecting small groups don't pass the "popular interest" test, but when a face is put to them can be of human interest. Leslie Cannold says: "Stories move emotion and change things for people in the way that abstract arguments and reason do not."

Journalist Wendy Bacon says

> The biggest criterion is probably how closely a story is linked to the news agenda. It is up to the skills of the journalist to find a way to link it with current issues.

Jason Whittaker of Crikey says

> As much as journalism is a public service, there's no point writing it if nobody reads it. We have to make decisions on what is most interesting and beneficial to readers, but we're always happy to talk to anyone that has information they believe is in the public interest. Crikey does have a dedicated "tips" section for information that is perhaps not of broad interest but may interest smaller groups.

Too hot to handle

Australia has exceptionally harsh defamation laws. "A lot of work is required to prepare and check articles that are potentially defamatory." These are difficult stories to write. Eddie Obeid told investigative journalist Kate McClymont: "I tell you what, you put one word out of place and I will take you on again. You are a lowlife. I will go for you, for the jugular."

Wendy Bacon

Defamation may become an issue later on, but a journalist who says up-front they can't do your story because of defamation is fobbing you off. Wendy Bacon warns

> Some journalists may blame defamation for not doing stories when really the problem is lack of time, too busy, lack of sympathetic editorial environment or lack of will to do the hard word necessary. Mostly you can publish something — with some adjustments to get around tricky points.

Evan Whitton agrees "Libel laws can also be an excuse for a reporter's sloth."

Although the "truth" is a defence to defamation, lawsuits are time consuming and expensive to defend. It's also possible to tell the truth and still lose, so a wealthy or powerful person can shut down a story merely with the threat of a defamation action.

This isn't the case in the US where the *Public Figure Doctrine* allows journalists to report corruption by public officials in a timely manner. All journalists interviewed for this article support law reform to protect journalists covering public interest stories.

Time and cost

Wendy Bacon says

> The biggest difficulty for the whistleblower is finding a journalist who has the time to do the work. Even with people who can mentally package a large amount of information, you need to have lots of time at a stretch to do complicated stories. This requires a huge amount of focus and there are simply not mainstream employers prepared to do that now, except on the rare occasion. It was always difficult but it was better.

Sue Spencer says expense does not deter "4 Corners", though they only have a limited number of episodes.

Even if a journalist wants to do a story, their editor or producer must approve it. They will weigh up how much work the story requires, budget, editorial space (a major factor) and what more promising stories the journalist could be working on that better fit the news agenda.

It's not just a matter of getting a journalist to pick your story. It's a matter of getting them to pick yours from all the alternatives.

Section 70

Section 70 of the *Crimes Act* is used to prevent the public from learning about Commonwealth corruption and maladministration. Public servants reporting it to the media risk two years jail. The courts are unsympathetic.

Public servants leaking anonymously can still be caught. I don't believe anyone acting in the public interest should have to risk jail. Government departments — even Health and Ageing — have warrantless access to your communications so corrupt officials and the Australian Federal Police (who prosecute whistleblowers) can see which journalists you are talking to. Phones can be tapped.

Journalists can make it safer for whistleblowers by offering anti-spying technology such as Strongbox or PGP encrypted e-mail. Whistleblower Edward Snowden said "It should be clear that unencrypted journalist-source communication is unforgivably reckless."

Sue Spencer says *Section 70* and risk of defamation can cause "4 Corners" to not proceed with stories.

Section 137

Section 137 of the *Criminal Code* makes it an offence to supply false and misleading information to a public official. Don't fall into the trap of denying a question they already know an answer too. See a lawyer first.

What to look for in a journalist

Only deal with experienced investigative journalists with demonstrable track records.

Look at their stories and at other stories in their publication. Avoid journalists who have ridiculed or lumped whistleblowers in with the corrupt officials they are reporting. Beware some who take digs at whistleblowers to "balance" their articles. Avoid those who largely echo reports from institutions without adequately questioning statements or assumptions. Do not assume a journalist is trustworthy just because they present well on TV or radio.

Andrew Hooley warns "Avoid 'hack' journalists who publish often and without substance as they go after the easy grab story irrespective of the potential damage."

Avoid "daily" journalists expected to produce articles quickly with very little research. They don't have the time, experience or editorial support to do an in-depth story. These include most journalists in TV news and current affairs.

Avoid "beat" journalists too. They focus on a particular sector or institution, building a network of people to provide them with a steady flow of information so they can publish frequently.

Favours such as tips or an exclusive interview can create a strong sense of mutual obligation in a journalist. Just meeting a man, shaking hands and exchanging pleasantries can disincline a journalist from publishing information which could destroy his career, or even just make him cross.

A reporter who relies on a source for easy information must look the other way when the source is involved in dubious practices. Evan Whitton calls such a journalist "a prisoner of the source" which is why for example "investigative reporting into police has got to be done from outside traditional police reporting."

It's worth noting that the story of endemic corruption within the Commonwealth Public Service was not broken by a Canberra journalist, but by an investigative journalist in Sydney.

Although the government publicly attacked the credibility of his reports, there was no follow-up or support from Canberra-based journalists. Labor Minister for the Public Service Gary Gray appeared to drive a wedge when he said:

> This week *The Canberra Times* referred to a number of allegations about fraud, corruption and misconduct in the public service, which were previously reported in the *Sydney Morning Herald*. *The Canberra Times* rightly pointed out that there is no evidence of endemic corruption, or a culture of complacency, in the APS [Australian Public Service]. Correctly, *The Canberra Times* argued that sufficient anti-corruption systems exist and acknowledged that there is no need for an independent corruption commission like those that exist in

New South Wales and Western Australia.

Steve Davies of Ozloop says:

> I am perplexed at the degree of passive reporting by *The Canberra Times*. In my opinion, much reporting is effectively a rehash of the APS "party line." The media needs to understand criticising the public service is not the same as criticising the government. Self-censorship damages all these institutions.

Don't fixate on TV. Often newspaper is a better medium.

Journalists don't share information, so speak to all reputable investigative journalists to touch base and see if anyone is already on the story. Given a choice, choose the journalist with the most drive. Be aware that they will drop the story if their initial sniffing doesn't quickly bear fruit. If they drop the story, they will not tell you. Once a journalist looks at a story, however briefly, they won't look at it again, even if new evidence emerges.

Andrew Hooley of Victims of CSIRO says "Always choose a journalist who has a reputation as an outstanding person in their field as they have far more regard for their reputation and will be more professional in their approach to the story."

Talking to journalists

Time is valuable to investigative journalists. Get straight to the point.

Position your message to slot into the journalist's mind. Evan Whitton says "Reduce what you want to tell the reporter to three or four words, as on a huge billboard on the side of the road."

Evan Whitton

Write a summary of your story in no more than 400 words. Condense that into one or two sentences. The latter becomes what business people describe as your "elevator pitch." Write a separate chronology describing very briefly what happened on what date. Organise your documentation.

It's best to make initial contact via a short phone call. If you e-mail, keep it short, using your elevator pitch. Don't attach any documents or letters. This is counterintuitive, but the more documentation you send, the less likely they will do your story. They will only reply if they're interested. If they don't, look elsewhere.

Think carefully about what you want to achieve from approaching a journalist. When you talk keep your answers brief. If you can't make a point in 15 to 30 seconds, you risk losing them. Long explanations can't be communicated to the public anyway. Avoid jargon. Don't pile documents on them, or set them reading assignments. They'll simply decide your story is too much work.

Describe what the corrupt officials have done. There's no need for name-calling. Andrew Hooley advises

> Always be impartial, emotionally detached in interviews as emotional comments often come across as "this person is obsessed" and discredit you. One of the fastest ways to shut down a whistleblower is to attack their personal interests, so always refer to the issue at the centre rather than "me."

Don't exaggerate or hide anything; make sure the journalist knows all relevant information. Don't get sidetracked by themes not relevant to the story, such as politics or chit-chat. Don't harp on or repeat themes the journalist shows no interest in; they will see you as a time-waster.

Investigative journalists will initially talk to you "off the record" to rapidly cover the entire subject without you needing to "lawyer" every sentence. Before the story runs they will ask you for quotes. Beware of disreputable journalists who encourage you to talk "off the record," then quote you anyway.

Whistleblower Dr. Kim Sawyer advises "Try to 'control' the story as much as possible, and that includes the headline. The headline and first two paragraphs are key."

Anticipate the likely response to the allegations and prep the journalist beforehand. When the story is published take the day off to monitor it and rebut counterclaims in real-time. Use Twitter.

A journalist who has promised to investigate your story will ask for exclusivity. Give it, but beware it may encourage them to sit on a story in the hope it writes itself. The false reassurance of imminent publication can lure a whistleblower to put in more work and expose themselves to more danger to get the story over the line. The best guide is, if the journalist isn't asking questions, they're not working on it. Put the hard word on them, and if you don't hear back (or if you do but nothing still happens), look elsewhere.

Some journalists, despite having evidence, will sit on stories indefinitely. There is no point pushing a reluctant journalist to do a story. Look elsewhere.

Anonymity

Although you've done nothing wrong, the reality is if you are publicly identified you will be harmed. Blow the whistle anonymously, as should the sources backing your story. However, journalists prefer to name their sources, so you must explain to them your reasons for anonymity. Reputable journalists will protect your identify. Andrew Hooley warns "Disreputable journalists will not, since they never expect to contact you again after the initial story has run." Unfortunately you might still be exposed by an accidental leak or because it's obvious from the story who you are.

Other avenues

Often you will find still no journalist will cover your story. What then?

While a story carried by a major newspaper will be seen by more people, smaller publications read by officials' peers can be more effective: Andrew Hooley said "Getting our story printed in *Nature* magazine created far more of a reaction from CSIRO than even material published in the *Canberra Times* or *Sydney Morning Herald*." Likewise Crikey is reportedly the most widely read publication in Parliament House. My own article in Crikey elicited a response from an attorney-general who had until then ignored me.

Wendy Bacon says:

> If you can't find an experienced journalist, look for a highly motivated final year student or recent graduate who can arrange mentoring through their university. Universities do some very good investigative journalism, but you need access to experience.

Consider writing your own story (as Allan Kessing did for Crikey) or your own opinion piece (as I did for Crikey). The most important skill here is to write efficiently; take that 12-page letter and reduce it to 800 words. Write tightly and don't repeat anything. The shorter something is, the more people will see and read it. Watch the News Agenda for openings.

Consider the independent media, but choose a publication which does investigative reporting, not just political or social commentary.

Consider publishing on your own website or blog. These are never as popular as media web sites, but they attract others whose stories may lead to media coverage. This strategy has worked very well for Victims of CSIRO whose website has had 50,000 unique visits and now one hundred members.

Read up on defamation law. Be warned that Ozloop, Victims of CSIRO and Victims of DSTO have all found that departments regularly scan their websites.

Sending private letters of complaint to officials is useful because it documents they knew of and permitted corruption, but without publicity they will ignore you. US Supreme Court Justice Louis Brandeis said sunlight is the best disinfectant. Use widely distributed public open letters cast their deeds into full view. Find other interested parties on Google and copy them on your letters.

The limits of your relationship

Journalists can publish your story, but they can't protect you from ongoing harm, advocate for you or give advice.

Wendy Bacon says "Whistleblowers need good legal and non-legal community support more than they need journalists. They need people to support and advise them even through the ordeal of trying to deal with the media."

Unfortunately that leaves nobody. Whistleblowers Australia is poorly resourced, and very few lawyers give whistleblowers advice pro bono. To get specific advice the whistleblower must pay a lawyer $230–$500 per hour to read all their material. (Something that may change this are US-style *False Claims* laws which give lawyers a financial incentive to help whistleblowers.)

A journalist warned "Lawyers are never better partners unless pro bono. They tell the client not to contact media because media can resolve the thing more efficiently, but lawyers' business model is to ensure a protracted dispute." A lawyer warned: "The only people who win out of these things are the lawyers."

Dr. Kim Sawyer warns:

> Consider the risks. Approaching a journalist is risky. Be prepared for the negative perceptions of an article. Most readers do not identify with the issue, only the scandal. Most journalists do not understand corruption, the long-term effects or the correlation across the various types of corruption. They are not interested in systemic issues, only the short-term story.

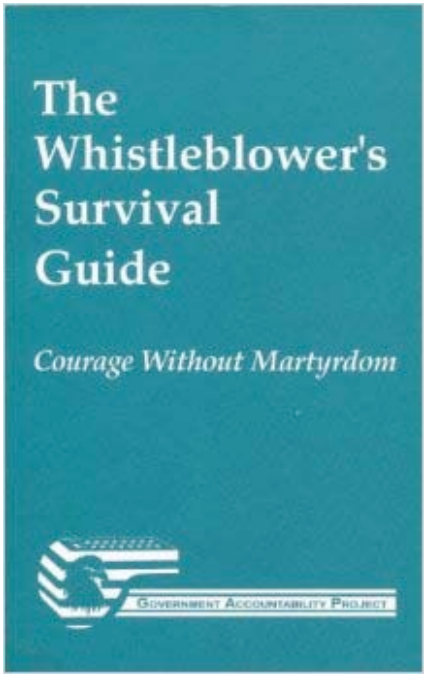
Conclusion

Only deal with experienced investigative journalists with a demonstrable track record. Write up your story in 400 words or less. Don't waste a journalist's time. Understand most stories are rejected, and that even if a story is published the abuse and the problem will most likely continue.

Thanks to all those who contributed to this article, with special thanks to Andrew Hooley and Wendy Bacon.

Recommended reading

Courage without martyrdom: A survival guide for whistleblowers by Tom Devine. This is a US book, but pages 84–94 contain good general information about working with the media. Available for free download via http://fairwhistleblower.ca/books/books.html



More information

A version of this article is available online, with over 100 footnotes containing sources and additional comment.
See http://www/bmartin.cc/dissent/documents/Jones13.html

Whistleblowers Australia

"All it needs for evil to flourish is for people of good will to do nothing"- Edmund Burke

2013 National Conference

Saturday 23rd November 2013
8.15am for 9am

Speakers include: Queenslander Jo Barber, who blew the whistle on the failings of the QLD Medical Registration Board; **NSW Detective Chief Inspector Peter Fox**, who was the catalyst for the current Federal Royal Commission of Inquiry into institutional cover-ups; **Victorian Brian Hood**, who blew the Reserve Bank, NPA, Securency bribery scandal wide open last year, **Professor David Vaux**, molecular biologist and Deputy Director of the Walter and Eliza Hall Institute in Melbourne on 'Researchers behaving badly' and the **Assistant Ombudsman, George Masri** on the workings of the new federal whistleblower protection laws.

Book launch: "Whistleblowing: A practical guide" by well known author & scientist Dr Brian Martin, Professor of Social Sciences at the University of Wollongong and Vice President of Whistleblowers Australia Inc.

2013 AGM > talkfest to follow

Sunday 24th November 2013
8.15am for 9am

Venue: Uniting Church Ministry Convention Centre on Masons Drive, North Parramatta, Sydney NSW

Non member: $65 per day: includes lunch & morning/afternoon tea. Optional $25 extra for dinner onsite 6pm Saturday night

Member: $45 per day or $80 for two days. (Note member discount also applies to students & concession cardholders). Optional dinner $20 extra for dinner onsite 6pm Saturday night.

Bookings: notify full details to treasurer Feliks Perera by phone on (07) 5448 8218 or at feliksfrommarcoola@gmail.com or president Cynthia Kardell (for phone / email see below under enquiries).

Payment: Mail cheque made payable to Whistleblowers Australia Inc. to treasurer, Feliks Perera at 1/5 Wayne Ave, Marcoola Qld 4564, **or** pay Whistleblowers Australia Inc by deposit to NAB Coolum Beach BSB 084 620 Account Number 69841 4626 **or** by credit card using PayPal to account name wba@whistleblowers.org.au.

Low-cost quality accommodation is available at the venue: Book directly with and pay the venue. Call 1300 138 125 or email service@unitingvenues.org

Enquiries: ring national president Cynthia Kardell on (02) 9484 6895 or email ckardell@iprimus.com.au

Whistleblowers Australia contacts

Postal address PO Box U129, Wollongong NSW 2500
Website http://www.whistleblowers.org.au/

New South Wales
"Caring & sharing" meetings We listen to your story, provide feedback and possibly guidance for your next few steps. Held by arrangement at 7.00pm on the 2nd and 4th Tuesday nights of each month, Presbyterian Church (Crypt), 7-A Campbell Street, Balmain 2041. Ring beforehand to arrange a meeting.
Contact Cynthia Kardell, phone 02 9484 6895, ckardell@iprimus.com.au

Wollongong contact Brian Martin, phone 02 4221 3763. *Website* http://www.bmartin.cc/dissent/

Queensland contacts Feliks Perera, phone 07 5448 8218, feliksfrommarcoola@gmail.com; Greg McMahon, phone 07 3378 7232, jarmin@ozemail.com.au

South Australia contact John Pezy, phone 0433 003 012

Tasmania Whistleblowers Tasmania contact, Isla MacGregor, phone 03 6239 1054, opal@intas.net.au

Schools and teachers contact Robina Cosser, robina@theteachersareblowingtheirwhistles.com

Whistle
Editor: Brian Martin, bmartin@uow.edu.au
Phones 02 4221 3763, 02 4228 7860
Address: PO Box U129, Wollongong NSW 2500
Associate editor: Don Eldridge
Thanks to Cynthia Kardell for proofreading.

Whistleblowers Australia conference

See previous page for details

Annual General Meeting

Whistleblowers Australia's AGM will be held at 9am Sunday 24 November at the Uniting Conference Centre, North Parramatta (Sydney). See previous page.

Nominations for national committee positions must be delivered in writing to the national secretary (Jeannie Berger, PO Box 458, Sydney Markets NSW 2129) at least 7 days in advance of the AGM, namely by Sunday 17 November. Nominations should be signed by two members and be accompanied by the written consent of the candidate.

Proxies A member can appoint another member as proxy by giving notice in writing to the secretary (Jeannie Berger) at least 24 hours before the meeting. No member may hold more than five proxies. Proxy forms are available online at http://www.whistleblowers.org.au/const/ProxyForm.html.

Whistleblowers Australia membership

Membership of WBA involves an annual fee of $25, payable to Whistleblowers Australia. Membership includes an annual subscription to *The Whistle*, and members receive discounts to seminars, invitations to briefings/ discussion groups, plus input into policy and submissions.

To subscribe to *The Whistle* but not join WBA, the annual subscription fee is $25.

The activities of Whistleblowers Australia depend entirely on voluntary work by members and supporters. We value your ideas, time, expertise and involvement. Whistleblowers Australia is funded almost entirely from membership fees, donations and bequests.

Send memberships and subscriptions to Feliks Perera, National Treasurer, 1/5 Wayne Ave, Marcoola Qld 4564. Phone 07 5448 8218, feliksfrommarcoola@gmail.com