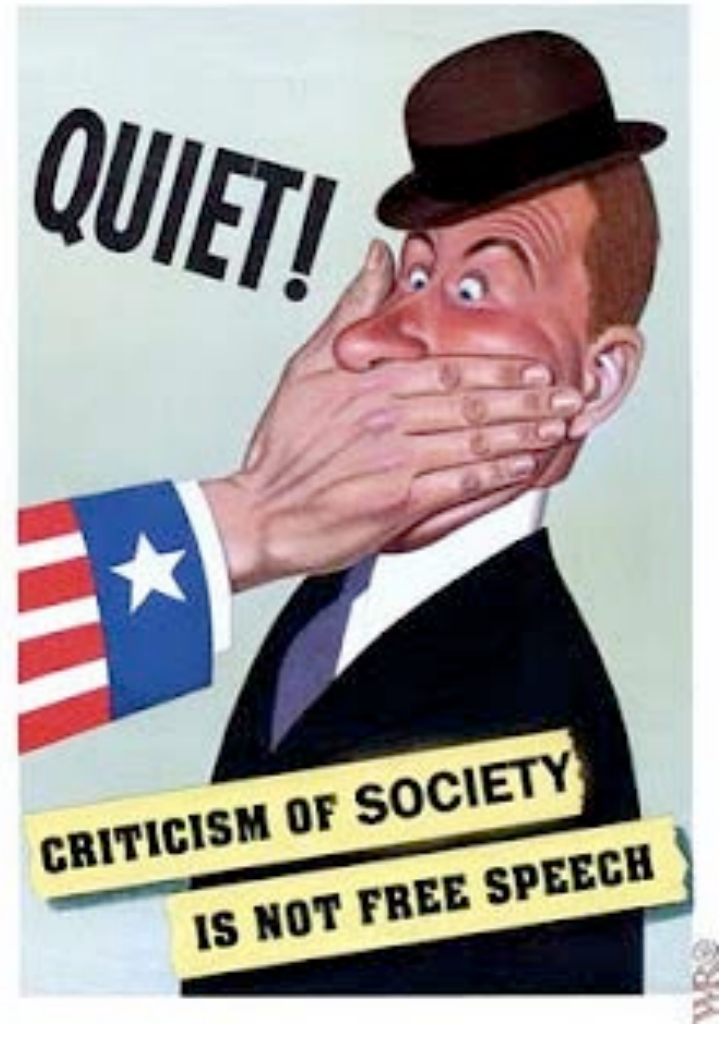
"All that is needed for evil to prosper is for people of good will to do nothing"—Edmund Burke

The Whistle

No. 78, April 2014

Newsletter of Whistleblowers Australia



Wikipedia: **Hoon** is a term used in Australia and New Zealand to refer to anyone who engages in loutish, anti-social behaviours. In particular, it is used to refer to one who drives a car or boat in a manner which is anti-social by the standards of contemporary society, that is, too fast, too noisily or too dangerously.

Why good people do nothing

Kim Sawyer

THE other night I was taking a walk in our neighbourhood. As I was crossing a road, a car came hooning around the corner and nearly removed me from whistleblowing advocacy.

I pointed at the number plate and evidently one of the two in the car saw the point. They braked, and proceeded to reverse with the intention of running me down. I removed myself to the footpath, whereupon they jumped out of the car, ran up to me and threatened to break my jaw.

Clearly, pointing at a number plate is the ultimate form of dobbing.

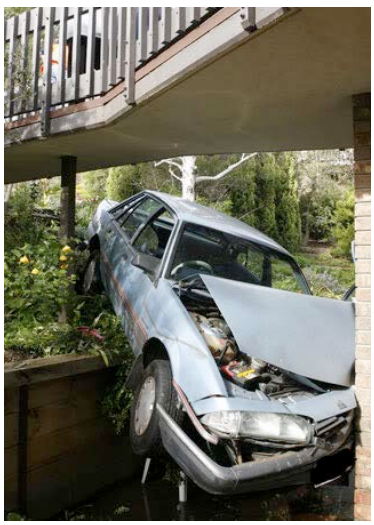
I told them to settle down, and eventually they took off. I had noted their licence number. The incident happened too quickly for me to be scared and, while I was bigger than the main hoon, twenty years of advocating non-violence have taken the fight out of me. I did not relish a punch-up in a public street at 8.30 at night.

But what was I to do with the licence number? I did nothing. I walked away. I exhibited exactly the same indifference that I have condemned in others. I was indifferent to the hoon and to the possibility that he may re-offend or possibly worse in the future. I began to question why. After all, I have spent forty years not being indifferent, helping at road accidents, revealing a neighbour to be a burglar, disciplining cheats at universities and, of course, blowing the whistle and advocating for others who blew the whistle. An honours student once placed a note in my mailbox advising that another student had plagiarised a thesis. He stated "We knew you would do the right thing."

So why was I now indifferent? Of course, indifference is all about risk; in this case the risk that it would be my word against the word of the hoon; the risk that the hoon would target my family and I did not know his network; the risk that by taking on the hoon I would jeopardise other things more important to me in the future. But also it is about the possibility of saving oneself for more important battles that possibly can be won; and the knowledge of karma that I did not have before I blew the whistle more than twenty years ago. Twenty years ago, I thought karma was just buried in Hindu and Buddhist writings. Now I think differently. Sometimes the universe does the work.

Kim Sawyer

For once I did nothing and perhaps understood better some of the indifference I have suffered from. But it still doesn't excuse it, particularly the collective indifference we all experience as whistleblowers.



Fate of the hoons?

Australian whistleblowers provide tip-offs for US scheme amid criticism of laws at home

Criticism of laws at home comes as figures reveal dozens of Australians gave tip-offs to a US scheme rewarding whistleblowers with cash incentives.

Ruth Williams
Sydney Morning Herald (BusinessDay section), 20 January 2014

Illustration: Simon Bosch

DOZENS of Australians have contacted the US securities regulator to report suspected misconduct after it launched a scheme rewarding whistleblowers with cash bounties.

The US Securities and Exchange Commission (SEC) has received 39 whistleblower tip-offs from Australia since late 2011, when laws to "incentivise" those who exposed insider trading, market manipulation, foreign bribery and other misconduct came into force.

Figures from the SEC's Office of the Whistleblower show that Australia has been one of its top foreign sources of tip-offs, ranking at least seventh for the past two years. Canada and the UK were by far the biggest contributors.

The US scheme, introduced under the sweeping Dodd-Frank Wall Street reforms, gives whistleblowers 10 per cent to 30 per cent of any financial penalties paid by those pursued as a result of their tip-offs, as long as the fine levied is at least $US1 million ($1.13 million).

The SEC has so far received more than 6500 tips and paid rewards to six whistleblowers under the scheme, ranging from $US50,000 to the whopping $US14 million paid to an unnamed individual in October.

The SEC declined to comment on whether any Australian-sourced tip-offs led to prosecutions or current investigations, and whether the Australian tips were about US companies operating in Australia, Australian-based companies with a US presence, or companies based elsewhere with dealings in both countries.

Foreign tips accounted for almost 12 per cent of the 3238 tips the SEC received last year, 149 of which related to the offshore bribery-tackling Foreign Corrupt Practices Act (FCPA).

The FCPA's most recent scalp was Alcoa, which, along with Australian subsidiary Alumina, last week agreed to pay fines of $US384 million to settle charges that one of its units bribed officials in Bahrain.

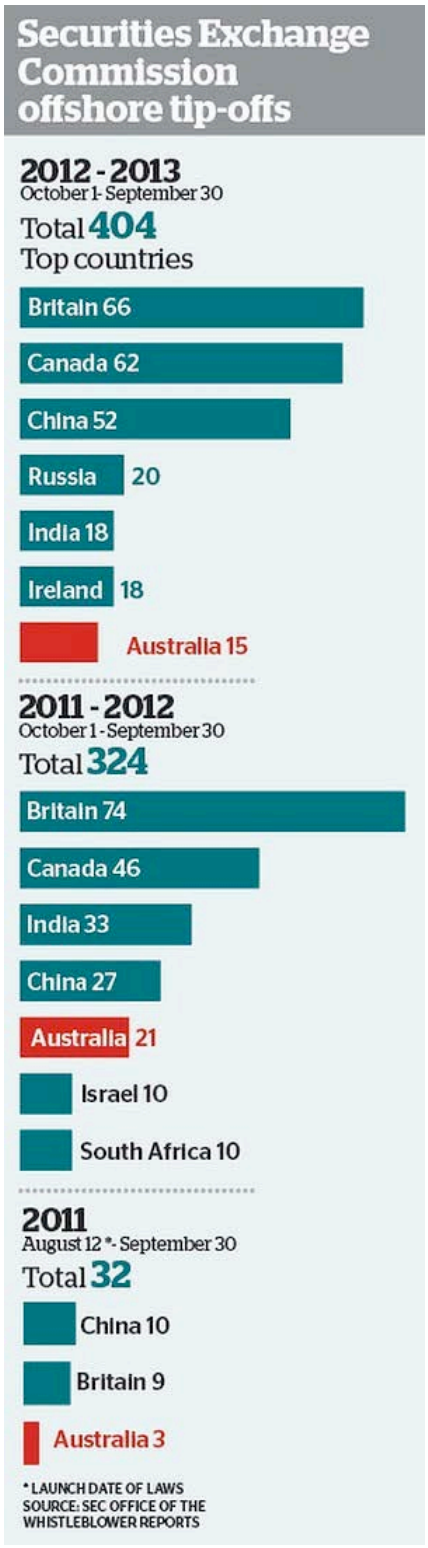
The response to the US scheme comes amid criticism of Australia's own whistleblowing laws and how the corporate regulator, the Australian Securities and Investments Commission (ASIC), has dealt with whistleblowers.

An ongoing Senate inquiry into ASIC's performance was launched last year after revelations the regulator took 16 months to act on a 2008 whistleblower tip-off alleging serious misconduct inside the Commonwealth Bank's financial planning arm. The bank later paid $51 million in compensation to impacted clients.

Experts are now calling for a major review of Australia's private sector whistleblower laws, dubbed "poorly regarded" by the Governance Institute of Australia, including whether US-style rewards should be offered.

The Governance Institute has urged that a "targeted" review of whistleblower laws be launched, and AJ Brown, from Griffith University's Centre for Governance and Public Policy, said it was a "logical" time to review private sector whistleblower protections, after laws impacting government workers and contractors were reformed last year.

Describing Australia's whistleblower laws as "patchy, limited and far from international best practice," Professor Brown said a review should include a "serious look" at whether Australia should adopt a reward scheme similar to those in place in the US.



The long-standing US False Claims Act — a Lincoln-era law beefed up by the Reagan and Obama administrations

— rewards whistleblowers that report companies defrauding the government in a similar way to the SEC-run Dodd-Frank scheme.

The False Claims Act has proved lucrative for the US government and whistleblowers alike, recouping $US3.8 billion in fines and penalties for the US government in 2012–13 as whistleblowers shared $US354 million in bounties.

Independent Senator Nick Xenophon and groups including the Australian Federal Police Association and the Tax Justice Network have called for Australia to consider whistleblower laws similar to those in place in the US, arguing they could help tackle fraud and better protect and compensate whistleblowers.

Senator Xenophon has flagged plans to introduce legislation into the Senate modelled on the US laws, and told BusinessDay he was planning to release the draft legislation in coming months. He was preparing to travel to the US at his own cost to research its whistleblower laws.

BusinessDay revealed last year that the federal Attorney-General's department is researching the US laws. "We are still considering the merits of an Australian scheme and will continue to work with the private sector on this," a spokesman said this month.

Whistleblowers, including one of those at the centre of the CBA scandal, have complained that the system in Australia leaves them vulnerable to victimisation and financial and emotional stress, and in the dark about progress on their complaints.

Decade-old laws protect corporate whistleblowers who contact ASIC from being sacked and from criminal and civil liability, for example for breach of confidentiality or defamation. But the laws only apply to a narrow group, including current employees — preventing, for example, former employees, business partners and anyone wishing to act anonymously from claiming protection.

ASIC itself, in its submission to the Senate inquiry, called for changes to the current laws — including that they be extended to cover former employers, company advisers such as accountants and unpaid workers such as interns and volunteers. It said it had reworked its approach to whistleblowers, including putting in place a central tracking system for whistleblower reports, and providing "prompt, clear and regular" communication with whistleblowers.

ASIC's submission revealed that it received 845 "potential whistleblower reports" last financial year, 129 of which were referred to ASIC's compliance, investigation or surveillance teams for further action.

In response to questions from BusinessDay, ASIC declined to say how many of these qualified as protected whistleblowers under the current laws, citing confidentiality requirements.

Professor Brown, whose submission to the inquiry called for wide-scale reforms, said pressure was building for stronger whistleblower protection laws in the private sector, but warned that without a co-ordinated approach, a "proliferation" of complex rules could result — adding costs to business and government.

"Everybody knows that [whistleblowing] happens … but people are just on the edge of acknowledging how important it really is," he told BusinessDay. "People are [afraid] that it's a bit of a Pandora's box to facilitate or encourage whistleblowing."

The previous Labor government launched a review of corporate whistleblower laws in 2009, with then corporate law minister Chris Bowen saying the current regime had "fundamental shortcomings." He revealed at the time that just four whistleblowers had used the protections to provide information to ASIC.

But despite taking submissions, the project was abandoned, with the former government saying last year that the consultations "did not reach consensus on the need for or form of further reforms."

In its submission to the current Senate inquiry, the Governance Institute, formerly Chartered Secretaries Australia, "strongly recommended" a separate review of whistleblowing laws "which recognises the involvement of multiple regulators in the process of investigating and prosecuting corporate and private whistleblowing."

The Institute's national policy director Judith Fox said that while there were concerns about how ASIC managed whistleblowers, "ASIC's not in this alone," pointing to ASIC's need to liaise on criminal matters with the Commonwealth Director of Public Prosecutions and the Australian Federal Police.

Attorney-General George Brandis was unavailable for comment.

Bills in Congress crack down on whistleblowers

Maxwell Abbott
posted on *PR Watch*
20 December 2013

PRESIDENT Obama was elected on a platform that included promises for increased transparency and openness in government. Despite this rhetoric, Obama has prosecuted more whistleblowers than any administration in history and overseen the massive growth of the NSA's surveillance apparatus. In November, the Senate (S. 1681) and House (H.R. 3381) Intelligence Committees each released their own version of the "Intelligence Authorization Act for Fiscal Year 2014."

This was an opportunity for Congressional leadership to address one of the defining issues of our time and either take a stand for increased transparency or continue down an Orwellian path of pervasive secrecy. A review of each chamber's proposed legislation demonstrates that *1984* is the future.

Stopping "insider threats"

The bills contain provisions which will intensify efforts to stop whistleblowers or "insider threats," no doubt inspired by Edward Snowden and his release of sensitive NSA documents. The House version of the funding bill provides $75 million of increased funding specifically for classified information protection. According to Tom Devine, Legal Director of the Government Accountability Project, "the 'insider threat' program is a cover for a witch hunt of whistleblowers."

In a purported effort to demonstrate support for the principles of openness and transparency, the House and Senate Intelligence Committee bills will provide protections for "legitimate" whistleblowers. But the committees

believe legitimacy in whistleblowing is not due to the accuracy of the information disclosed, how much harm it spares the American people, or how much it benefits the democratic process, but rather whether or not the information is reported to proper authorities, such as "lawmakers, inspectors general and intelligence community leaders."

Notably missing from this list is the media, and history shows that whistleblowers who do use "proper channels" first are rarely rewarded.

Media is a legitimate conduit for whistleblowers

What the Intelligence Committees propose to protect in this legislation is a watered-down version of whistleblowing. The Government Accountability Project created a composite definition of whistleblowing based on state, federal and international cases, which states that "whistleblowers speak out to parties that can influence and rectify the situation. These parties include the media, organizational managers, hotlines, or Congressional members/staff, to name a few."

Accountability will not result if whistleblowers only have recourse to their superiors within the government. Providing information to the media and watchdog groups outside the government bureaucracy must be a viable option for whistleblowers to expose government misconduct.

Regarding Edward Snowden's decision to forego internal reporting channels and release classified NSA documents directly to the media, the Government Accountability Project commented, "By communicating with the press, Snowden used the safest channel available to him to inform the public of wrongdoing. Nonetheless, government officials have been critical of him for not using internal agency channels — the same channels that have repeatedly failed to protect whistleblowers from reprisal in the past."

Whistleblowers betrayed by "legitimate channels"

Looking back to some of the more notable cases of whistleblowers who tried to use these "legitimate channels," it becomes apparent that the protections for whistleblowers will not result in corrections of mismanagement or greater respect for civil liberties.

Thomas Drake

Former NSA employee Thomas Drake worked on the data collection program ThinThread, which was minimally invasive to American's privacy and was cost efficient. ThinThread was an NSA counter-terrorism program developed during the 1990s for surveillance of phone and email that featured automatic encryption mechanisms in order to protect privacy rights. The encryption features would hide sensitive email and phone data from NSA analysts until a threat was identified, at which time the information would be decrypted. ThinThread was never used by the NSA because NSA Director Gen. Michael V. Hayden chose a more invasive and expensive program named Trailblazer instead. This program also monitored phone and email data, but did not include the same privacy protection features as ThinThread.

Alarmed about the damage that Trailblazer would do to the 4th Amendment, Drake reported his concerns to various superiors within the government, including his direct superiors at the NSA, the NSA Inspector General, the Defense Department Inspector General, and both the House and Senate Intelligence Committees.

Despite these efforts, Drake's concerns were ignored and development of Trailblazer continued for several years, until it was cancelled when Hayden admitted that the program was far too expensive. In return for doing his duty and protecting the rights of Americans to be free from unwarranted surveillance, Drake was marginalized and transferred to work on menial projects.

At this point, Drake felt he had no option but to disclose unclassified information to *Baltimore Sun* reporter Siobhan Gorman regarding the data collection programs. President Obama and Attorney General Eric Holder responded by investigating Drake for violations of the Espionage Act, which was created to prosecute spies, not those who report government misconduct.

Pfc. Chelsea Manning

In 2010, Pfc. Chelsea Manning (formerly known as Bradley Manning) was working as an intelligence analyst in Iraq. He was tasked with helping the Iraqi police find insurgents attempting to destabilize the fragile government and attack American forces. In the course of his work, he came across "anti-Iraqi literature" that resulted in the detention of several Iraqis. He discovered that it was not the work of terrorists, but a scholarly critique of the corruption in the Al-Maliki government.

Manning brought his concerns to the attention of his superiors, but was told to keep quiet and help the Iraqi police find more people who had committed similar "crimes." In his chat logs with Adrian Lamo, the hacker who turned him over to the US authorities, Manning described his concern for innocent Iraqis and his frustration with his superiors' dismissive attitudes as a primary motivation for leaking diplomatic cables to Wikileaks.

Shamai Leibowitz

Also in 2010, Shamai Leibowitz, a translator with the FBI, released classified documents to blogger Richard Silverstein. The documents were mostly transcripts of wiretaps from the Israeli Embassy in Washington. Leibowitz believed that Israel was too aggressive in its efforts to push the American government toward military action against Iran. He claims he

brought his concerns to his superiors, "who did nothing about them."

Gina Grey

After witnessing appalling delinquency at Arlington National Cemetery, including mishandled remains and mismarked graves, Defense Department Contractor Gina Grey registered her complaints using the proper internal channels. She was fired two days after reporting these problems to the commanding general of the Military District of Washington. Despite findings by the Pentagon Inspector General that the Army "elected to terminate her, rather than make a reasonable effort to address public affairs policy issues that she raised," her termination was upheld by Army Secretary John McHugh, and she received no compensation. She told the *Washington Post*'s Dana Milbank, "I went all the way up the channels … This is what happens when you do that."

Gina Grey

In each of these instances, employees within the government saw serious violations of legal codes and basic human rights. They were motivated not by a desire to destroy the American government, but by a desire to help it abide by its own laws. However, the institutional pressures on their superiors resulted in dismissive attitudes and retaliation instead of the investigations and remedies that whistleblower protection requires. They were only driven to divulge important information of government misconduct after the "legitimate channels" were exhausted.

These House and Senate versions of the Intelligence Authorization Act are currently under consideration by each chamber. This history of failure to protect legitimate whistleblowers indicates that it is time to increase protections for whistleblowers — who need to provide information to the media and watchdog groups as a last resort — not pull the rug out from under them.

Crushing Thomas Drake

Andy Greenberg

An extract from *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hactivists Aim to Free the World's Information* (New York: Dutton, 2012), pages 220–225

Editor's note *Andy Greenberg, a journalist, interviewed individuals across the globe in writing his book* This Machine Kills Secrets, *an engaging account of the movement to enable access to information whose secrecy is not in the public interest. Greenberg "sought out the history and future of an idea: digital, untraceable, anonymous leaking." The book contains revealing discussions of devious plans in the US to stem the "insider threat," which means the threat to powerholders from public interest leakers.*

The individuals tasked with rooting out leaks … tend to compare their targets to Robert Hanssen and Aldrich Ames, spies who sold uncountable secrets to foreign empires for millions of dollars. In fact, the archetypal leaker is often more like one NSA [National Security Agency] analyst named Thomas Drake: a conscientious whistleblower repaid only with crushing legal retribution.

Drake, a thin and severe-looking man with a wisp of brown hair, has the hard stare of someone who has dealt in serious affairs and seen them go very badly. Drake's troubles began on his first full day of work at the National Security Agency: September 11, 2001.

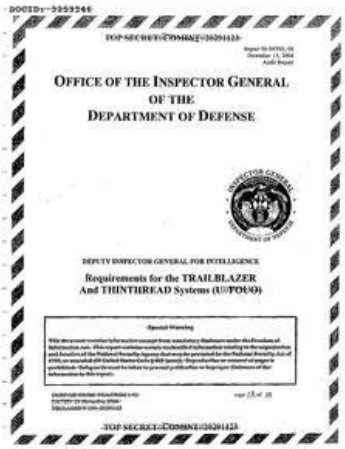
To the NSA, the horrors of that day represented its gaping inadequacies in the new millennium. The agency had intercepted but ignored phrases in the hijackers' communications including "Tomorrow is zero hour," and "The match begins tomorrow." The digital world's vast and messy flood of information had diluted those key warnings into insignificance. The NSA was drowning in data. Drake's first position at the agency, after a career in air force signals intelligence, was on a project code-named Jackpot. Jackpot aimed to analyze the agency's software to sniff out bugs and inefficiencies. One piece of code came to Drake's attention: a data-sifting algorithm known as Thinthread. The program had been built by the agency's brilliant mathematician Bill Binney to address the Internet's deluge of digital information, and Drake assessed it as a highly effective, scalable, and elegant tool, one that might have caught the needles in the digital haystack that represented 9/11 if it had only been implemented in time.

Before September 11, Thinthread had been dismissed as too invasive of Americans' privacy. Binney had responded by altering the program to encrypt all its results so that they would only be made available with a court order. But after 2001, the landscape had changed: In the bureaucratic handwringing that followed America's worst-ever terrorist attack, the NSA's leadership was looking for a solution to match the size of its problems, not a single, simple program. It launched a new project called Trailblazer with nine-figure resources aimed at funding private contractors to build new data-combing tools.

Drake would come to see the decision to pursue Trailblazer instead of Thinthread as a corrupt, negligent, and wasteful move. "Trailblazer became a corporate solution," he said when we met in the Washington, D.C., office of the Government Accountability Project, a whistleblower advocacy group. "We disregarded the traditional strength of the NSA, solving problems with the best minds of the private sector and the government, and instead turned the entire project over to industry. You always have to look at alternative options. They chose not to."

Over the next years, Trailblazer doled out massive contracts: Hundreds of millions went to the contractor SAIC, which had hired a former NSA director and formerly employed the NSA deputy director at the time, what Drake describes as "a revolving door refined to an art form." But even as it overran its budget, Trailblazer ran into endless delays and dead ends. By the time the project was canceled in 2006,

it had become a $1.2 billion boondoggle.



OFFICE OF THE INSPECTOR GENERAL
OF THE
DEPARTMENT OF DEFENSE

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Requirements for the TRAILBLAZER
And THINTHREAD Systems (U//FOUO)

Department of Defense, Office of the Inspector General, report on Trailblazer and Thinthread

Drake says he could see the monumental waste in Trailblazer from the start. "It didn't matter if Thinthread was better. They just wanted to spend a lot of money over many years. Corruption had become normalized," he says. "It still chaps my lips today to think about it: the amount of money wasted that never contributed to national security, and no one has ever been held accountable."

In the early days of the program, Drake and three other NSA officials approached one of the agency's budget overseers on the House Intelligence Committee to alert her to the project's overblown costs and ineffectiveness. She passed on the criticisms to others on the committee and even Supreme Court Justice William Rehnquist, but no one acted to rein in the program.

In 2005, Drake faced the last resort of so many ignored internal whistleblowers: anonymous digital communications with the press. He signed up for an account with Hushmail, an encrypted e-mail service, and, using a proxy to disguise his IP address, began sending messages about Trailblazer's alleged corruption to Siobhan Gorman, a reporter at *The Baltimore Sun*. His pseudonym: "The Shadow Knows." With the paranoia of an NSA analyst, Drake took a certain amount of caution in those missives. He installed four layers of firewalls on his home network and used a 256-character password on his encrypted e-mail account, the longest the service would accept.

Siobhan Gorman

Even then, Drake eventually decided physical meetings would be more difficult to eavesdrop, and trusted Gorman enough that he believed meeting her in person would be safer. "There is no absolute anonymity electronically," says Drake. "There are means that make it more difficult to identify you. But there's always a digital trail."

Drake says he made certain to never share classified documents in his dealings with Gorman, only testifying to Trailblazer's fiscal waste. In early 2006, as Trailblazer was collapsing, the *Sun* published an award-winning series of articles about the NSA's problems, including one that focused on Trailblazer.

But by then, the agency was concerned about a leak of far larger proportions. A few months before, *The New York Times* had published its story detailing how the NSA had engaged in widespread, illegal spying on Americans. In the post-9/11 era, the privacy concerns that had shelved Thinthread were now an anachronism. According to the *Times'* story, a new project was now hoovering up phone conversations and Internet traffic without the encryption and court-order protections that Thinthread had implemented: warrantless wiretapping. "Every line was crossed," says Drake. "They had turned the U.S. into a foreign nation electronically."

The Bush administration, which had pleaded with the *Times* not to publish the story, was humiliated and furious. A Department of Justice witch hunt set out to find the newspaper's sources.

Drake had participated in official protests against Trailblazer and also provided classified information to Congress during its investigation of intelligence failures before September 11. Those two actions were easily enough to pull him into the Justice Department's dragnet. In November 2007, a team of armed FBI agents arrived at his home.

Drake sensed that the agents had no interest in Trailblazer, and he believed that his communications with Gorman were both legal and insignificant compared to the leak that had exposed the warrantless wiretapping program. So he decided on the spot to come clean, and spent the day sitting with the agents at his kitchen table, debriefing them on his whistleblowing activities to avoid any confusion with their investigation. He gave the investigators full access to his computers, and they carted away boxes full of his papers.

Eventually, the FBI would identify Department of Justice lawyer Thomas Tamm as at least one source for *The New York Times'* expose. But Tamm was never prosecuted, likely for fear that his trial would expose too many details of the secret surveillance program that have yet to come to light.

Instead, they indicted Drake.

Drake was accused of illegally taking classified papers from his office to his home under a section of the Espionage Act, the same spy-hunting law used to indict Daniel Ellsberg and Bradley Manning. He faced ten felony charges and thirty-five years in prison, and his case was pursued for more than two and a half years without a trial. The prosecutor in the case argued that Drake should be used to "send a message to the silent majority of people who live by secrecy agreements."

Finally, just before his court date in 2011, the prosecution admitted that it had vastly exaggerated the classification of the documents Drake had been holding. Drake pleaded guilty to a misdemeanor charge that carried a year of probation and community service.

In the sentencing hearing, the judge in the case called the prosecution's behavior in exaggerating the charges against Drake "inappropriate" and "unconscionable."

By that point, Drake had spent eighty-two thousand dollars in legal fees, taken a second mortgage on his house, and been dismissed from his job both at the NSA and as an instructor at the National Defense University. Factoring in his lost pension after decades of military service, he estimates his financial damages in the millions. His Pentagon colleagues cut ties with him. He was separated from his wife for a year. Even his father, a World War II veteran, struggled to understand his actions. Today, he works at a Washington, D.C., Apple store for an hourly wage.

Thomas Drake

"I worked with the system, and I got fried," he says.

Thomas Drake's story is hardly unique. The Obama administration has pursued more leakers under espionage charges than all other presidential administrations combined. They include Jeffrey Sterling, an ex-CIA analyst who gave information to author James Risen about how the agency had botched an attempt to sabotage Iran's nuclear development plans. Lawyer and FBI translator Shamai Leibowitz pleaded guilty to leaking classified transcripts of bugged conversations in the Israeli embassy to the blog Tikun Olam, in the hopes of stemming Israeli aggression toward Iran. Stephen Kim, an arms expert for the State Department, the military, and Lawrence Livermore National Lab, was prosecuted for leaking a report to Fox News on North Korea's plans to develop a nuclear weapon. Ex-CIA officer John Kiriakou, who had at times defended and criticized the Bush administration's use of waterboarding, was indicted for revealing the name of two of the agency's interrogators to media including *The New York Times*. As of this writing [2012], prosecutions of Kiriakou, Kim, and Sterling continue — as does that of Bradley Manning.

All totaled, that makes six leakers prosecuted under the Espionage Act, compared with three such cases in all previous history — the Obama administration may yet pursue a seventh case with the prosecution of Julian Assange. All of which adds up to an unlikely track record for a president who came to office spouting promises of unprecedented government transparency and proclaiming on his official website in 2009 that whistleblowing is an act "of courage and patriotism, which can sometimes save lives and often save taxpayer dollars" and "should be encouraged rather than stifled."

Where did that evident hypocrisy come from? Obama has been "co-opted" by Washington's culture of secrecy, argues Jesselyn Radack, a lawyer at the Government Accountability Project who has advised Drake, and who once served as a whistleblower herself, leaking evidence of Justice Department ethics violations to *Newsweek* in 2002. "He wants to curry favor with the national intelligence community, where he's perceived as weak," she says.

But Drake, who has tasted secret information many times over in his career, offers an explanation of Obama's behavior that comes closer to the speech about Circe's potion that Daniel Ellsberg once gave to Henry Kissinger.

"He had never had that kind of access to secrets before," says Drake. "It was a lot of power. He was enamored with it. And it changed him."

Don't shoot the messenger!

Whistleblowing appears to be on the increase. But so is the war against those who do it. Where will it end, asks VANESSA BAIRD.

New Internationalist, April 2014, pp. 10–14

(The theme of this issue of the monthly magazine *New Internationalist* is "The war on whistleblowers." This is the lead article, slightly edited and omitting footnotes.)

Is this the age of the whistleblower? It would seem so, from the column inches, air time and cyberspace given to Edward Snowden.

According to campaigners, the 29-year-old former systems analyst at the US National Security Agency (NSA) is close to being the perfect whistleblower.

A quick look at the video clip interview with Laura Poitras shows why. Measured, thoughtful, Snowden comes across as your average guy, intelligent but with no political axe to grind. He just thinks we should know that the secret services are capturing and storing every phone call we make or internet message we send and that our privacy is being violated wholesale. And he thinks we should at least debate whether we are happy with that or not.

His modest demeanour, his very ordinariness, is in sharp contrast to the scale and impact of his revelations. The sheer amount of data he was able to pass on to select media — some 1.7 million files — beats Chelsea Manning's impressive 251,287 diplomatic cables into a hat.

Since the advent of Wikileaks, whistleblowing has gone from being a "cottage' to an "industrialized' activity, to use the analogy suggested by Icelandic information activist Smári McCarthy.

Yet for most who do it, making disclosures about wrongdoing is a lonely, limiting and isolating affair. It's not like being on a production line with your mates.

Paradoxically, this also applies to the most celebrated. Edward Snowden and Wikileaks founder Julian Assange may have achieved rock-star status but they are fugitives, effectively exiled.

Chelsea (formerly Bradley) Manning is serving 35 years in a military jail.

The Obama administration, for all its rhetoric of free speech, has started more prosecutions against whistleblowers than all presidents combined since 1917.

"War against whistleblowers is a toxic trend," says Jesslyn Radack, Snowden's lawyer and a former US Justice Department whistleblower herself.

Jesslyn Radack

And not just in the US. Japan recently approved sweeping government powers to punish those who would expose awkward truths about the country's nuclear industry, following the Fukushima disaster.

A dangerous vocation

At the source of most exposures of wrongdoing is not a government regulator or police investigator or even an investigative journalist, but a whistleblower. A moral insider who breaks ranks to tell the truth about the malpractice she or he sees.

Once the scandal has broken, such people will be hailed as heroes, admired for their integrity by a public grateful that such courageous and outspoken people exist.

But gratitude offers no protection.

In 2010, millions of Chinese parents were horrified to find that their children were drinking milk that had become mixed with toxic chemicals at fresh milk collection points. Two years later, one of the two men who exposed the practice, farmer Jiang Weisuo, was murdered in circumstances that have never been explained.

Jiang Weisuo

More recent is the case of Lawrence Moepi, a fearless and principled South African auditor, dubbed the "fraudsters' worst nightmare." Last October, as he arrived at his Johannesburg office, he was shot and killed by, it is believed, hired assassins. He had been investigating several suspected corruption cases, including a notorious arms deal.

Lawrence Moepi

Silencing or exacting retribution can take many forms, violent and direct — or more devious.

Craig Murray, a former British ambassador who exposed how the British and US secret services were supporting torture in Uzbekistan, was subsequently accused of asking for sex in exchange for visas. It took him 18 months to clear his name.

Janice Karpinsky, the most senior woman in the US army, was arrested and accused of shoplifting the day after revealing that Donald Rumsfeld ordered the torture of prisoners at Abu Ghraib.

Murray comments: "Whistleblowers are rare because it is a near suicidal vocation and everyone else is too scared to help. And if your whistleblowing involves the world of war and spying, they will try to set you up on false charges … and not just sack you but destroy you."

While public opinion is generally on the side of whistleblowers, governments, institutions and employers are not. When it comes to the really embarrassing and damaging disclosures, those in power will do all they can to turn the revealer into the enemy.

This has worked on a significant minority of the US public, furious with Manning and Snowden for allegedly putting at risk the security of all Americans. When pressed to say exactly how, the political and secret service players have failed to come up with one concrete example, resorting to vague comments about "agents in the field" and the fact that "terrorists will now change their tactics."

These are high-profile, international cases. But most whistleblowing happens at a far more modest, local level. Sometimes the revelations will reach the local press or emerge during an employment tribunal after the discloser has been dismissed or demoted. Often media outlets are afraid to investigate the information whistleblowers bring them, because they cannot take the risk of a costly libel suit, or because the story is too complicated or time-consuming to corroborate.

Legal protection

"Effective whistleblowing arrangements are a key part of good governance," says the British organization Public Concern At Work (PCaW). "A healthy and open culture is one where people are encouraged to speak out, confident that they can do so without adverse repercussions, confident that they will be listened to, and confident that appropriate action will be taken."

If only. In the topsy-turvy world of whistleblowing it tends to be the person revealing wrongdoing, rather than the wrong doer, who is punished and who ends up losing most — typically their job and career, but often

also their relationship, their home, even their liberty.

Far from being rebels and outsiders, most disclosers are diligent, conscientious, somewhat obsessive insiders, who think their employers will be grateful for the information given and will naturally want to do the right thing.

An increasing number of countries have laws on their statute books — with more in the pipeline — specifically to protect whistleblowers from retaliation, harassment or victimization. But most laws are severely limited in their scope and effectiveness. For example, in Canada and Australia, the law does not apply to people working in the private sector, while New Zealand's law is limited to government agencies.

In Canada, a fierce libel regime contributes to creating possibly the most hostile environment in the English-speaking world. Britain is one of the few European countries with a law that applies across both private and public sectors, but in practice British whistleblowers do not fare too well either and libel laws that favour the rich have a chilling effect. US law is patchy and contradictory, extremely hostile to those who speak out in some areas, but enabling large financial rewards for those who disclose fraud against the government.

While whistleblowers may need to be compensated for loss of earnings, the awarding of massive cash settlements is controversial. Cathy James of the British PCaW sees "moral hazard" in a US-style system. In her view: "Whistleblowing should be seen as a very positive issue, everyone should be encouraged to protect the public interest. I don't want to live in a society where people do the right things because they think they are going to benefit."

Going public on confidential information may put disclosers on the wrong side of the law, especially if they have smuggled out documents or broken official secrecy arrangements. This has led to absurd examples, like that of the banker Bradley Birkenfeld who exposed $780 million tax fraud at UBS, receiving a Swiss prison sentence for breaking confidentiality.

Under British law, disclosers who break the law to reveal wrongdoing can claim, in their defence, that they were acting in the "public interest." This is not widely available elsewhere.

"I now recommend leaking"

Considerable energy goes into lobbying for laws and practices to protect properly those who speak out and many whistleblower organizations believe this is the way forward.

Brian Martin is a veteran campaigner with Whistleblowers Australia who has talked with hundreds of disclosers and written a highly regarded practical guide on the topic.

And he has come to the conclusion that the intense focus on legal protection is misguided.

"It seldom works and can even make whistleblowers more vulnerable; they think they are protected but aren't."

Instead, he now encourages potential disclosers to develop their skills and understanding so that they can be more effective in bringing about change. The most effective strategies, he says, involve taking messages to a wider audience, through mass media, social media or direct communication.

"I now recommend leaking — anonymous whistleblowing — whenever possible."

This may not come naturally to most disclosers, who are conscientious employees who believe the system works. They will try official channels first and are reluctant to contact the media or action groups.

But, Martin points out, whistleblowers are "hardly ever effective in challenging the problems they attempt to expose. This sounds pessimistic. Whistleblowers are courageous but they need a lot of help to be more effective. Probably the best scenario is a link-up between a network of leakers and well-connected action groups."

Smári McCarthy is another activist who is moving away from the legal protection route. For three years he, and others in his native Iceland, worked to create a model legal environment for leakers, whistleblowers and journalists. They were making good headway until April 2013 when a rightwing coalition government came to power and stalled reform.

Smári McCarthy

Now he is focusing more on technology. There are two laws, he says, that governments have to obey: "physics and economics." He plans to use the former to make mass surveillance — whereby intelligence services gather everybody's private internet and phone communication — too expensive to do.

He has calculated that the total budget of the "Five Eyes" — that is the communications snooping services of the US, Britain, Australia, Canada and New Zealand combined — is $120 billion a year. With that they can scoop up the data of 2.5 billion internet users, making the cost per person per day a mere 13 cents.

"My five-year plan is to increase that cost to $10,000 per person per day. The services would have to be a lot more selective and do their job properly."

How to do it? Encryption — the types that hackers have developed and which the NSA has still, as far as we know, not managed to crack. "I use encryption a lot," says McCarthy. "But we need to make it easier to use and available to everyone."

This will help disclosers too, he says, because if everybody's privacy is improved then so is that of whistleblowers. Naturally, their leaks need to be accurate, need to pass the "public interest" test and not gratuitously violate personal privacy.

Snowden and others have revealed the extent to which free speech and civil liberties are being violated by the state, and not just in countries like Russia or China.

More and more information is being classified as top secret and we have no way of debating whether or not it should be. The recent Stasi-style destruction of laptops at *The Guardian* newspaper, under the supervision of Britain's GCHQ, should serve as a warning. As they say, democracy dies behind closed doors — and now too in smashed hard-drives in newspaper offices.

Those genuinely engaged in disclosing in the public interest need protection all along the communication line — from sources and whistleblowers, through campaigners and journalists, to print or web publishers and distributors. In 2011, under a social-democrat government, Iceland followed Council of Europe recommendations and made it illegal for journalists to expose their sources. In Britain a journalist can be jailed for not doing so. It is even worse in the US: Barrett Brown, a young freelancer, is facing 105 years in prison in connection with the posting of information that hackers obtained from Statfor, a private intelligence company with close ties to the federal government.

A better world

At its heart, whistleblowing is about the desire for truth to be known, for things to be done properly, and for the world to be made a better place.

A place where big business does not cheat or harm citizens for profit; where hospitals and care homes look after frail and elderly people and banks do not rob their customers. Where politicians see office as public service rather than self-service, priests respect the bodily integrity of children in their charge and military personnel do not go on shooting sprees for the hell of it.

Sometimes exposure yields tangible results and the information revealed improves or even saves lives. In 1994, US paralegal Merrell Williams leaked internal memos from Brown & Williamson Tobacco company that showed that the company knew it was lying when it claimed that cigarettes were not harmful, that nicotine was not addictive and that it did not market to children.

His action fuelled lawsuits that resulted in an industry pay-out of billions of dollars to pay smokers' medical bills.

Merrell Williams

Whistleblowers act as the guardians of morality, but too often they are solitary martyrs to democracy. As Wikileaks revealed towards the end of last year, the world is currently facing a major multilateral threat to democracy. It is coming not from religious fanatics in turbans but from fundamentalists in suits.

The acronyms TTP and TTIP are enough to lead even the most committed insomniac to the land of nod. But stay awake, please! This is important. These are US-led international trade deals being negotiated — in conditions of unprecedented secrecy — that will give corporations the power to trump national sovereignty and the interests of billions of people.

Two secret drafts of the TransPacific Partnership (TPP), obtained by Wikileaks, on intellectual property and the environment show the deals would trample over individual rights and free expression and give powerful companies the right to challenge domestic laws regulating, for example, resource extraction in Peru or Australia. The Transatlantic Trade and Investment Partnership (TTIP) — between the US and the EU — would have a similar impact, making existing national public services such as health and education even more vulnerable to aggressive action by big private corporations from outside. Those trying to save Britain's national health service from the clutches of private US medical companies know how bad this could be.

Such trade agreements are made at a high level, hatched between a nexus of powerful corporations, governments that do their bidding and secret services that we now know (again, thanks to Snowden) really do use public money to spy on behalf of big business.

The only thing that will counteract the undemocratic and self-serving power of this nexus is a growing network from below that involves whistleblowers, civil society activists and hactivists, journalists and citizens who care.

Only if we have access to information do we have democracy — and today the most relevant information often comes from whistleblowers.

Only if we can participate, is that democracy real — which is why we need to use the information to take action and stop sleepwalking into totalitarianism, be it that of a corrupt institution or a world order devised by and for a global, corporate élite.

Then the tremendous risks that whistleblowers take, and the sacrifices they make, will not be in vain.

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

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.

What's in *The Whistle*

Years ago, there was not all that much easily available information about whistleblowing. In the 1990s, one of the functions of *The Whistle*'s "media watch" section was collecting stories from various sources and making them available to readers. "Media watch" has continued to be a key part of each issue of *The Whistle.* Now, though, the challenge is to select items from the very large quantity of material being produced.

In editing *The Whistle,* I rely heavily on input from others. Associate editor Don Eldridge regularly sends me items from newspapers and magazines, and others do so from time to time. The challenge then is to pick out the stories most likely to be of interest to our readers. This includes members of Whistleblowers Australia, who receive printed copies, and many others, most of whom read the online version. Some readers go through back issues looking for items of interest, or are led to particular issues through web searches.

Some introductory articles are worthwhile, but it's also valuable to have in-depth stories for readers who know a lot about whistleblowing. However, some articles are too specialised. They might report the latest stage of an ongoing saga and not provide enough background information for someone new to the case.

I especially appreciate articles and letters written for *The Whistle,* often giving personal perspectives. These are what gives the newsletter its distinctive orientation, built around the experiences of those who have blown the whistle or are closely involved with whistleblowing. So if you have something to share, send it along!

Brian Martin

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