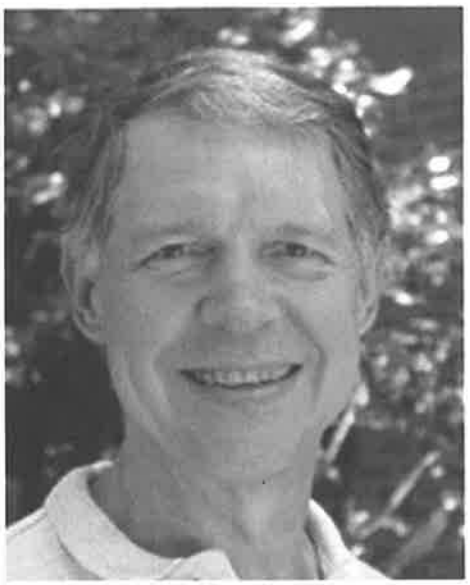
Learning from Snowden: lessons for whistleblowers

This is a review and commentary on Luke Harding's book *The Snowden Files: The Inside Story of the World's Most Wanted Man*, with special attention to implications for leaking and whistle blowing, by **Brian Martin**, Professor of Social Sciences at the University of Wollongong. He was president of Whistleblowers Australia from 1996 to 1999 and remains the International Director.



Professor Brian Martin. Photograph by Christine Anderson

In June 2013, spectacular revelations were reported in the news. A secretive US organisation, the National Security Agency, was carrying out extensive spying on people's electronic communications. This spying was massive. The NSA, according to reports, was collecting just about everything imaginable: emails, phone calls, texts, you name it – from everyone around the world.

The revelations continued for weeks and months. The NSA was spying on US citizens in the US, apparently in violation of the law. It was also spying on foreign leaders. For example, there were reports that the NSA had monitored the personal mobile phone of Germany's chancellor Angela Merkel, and the phones of many other political leaders.

The stories were broken by *The Guardian*, a well-known British newspaper and media group. *The Guardian*'s information came from an NSA insider who had leaked vast amounts of NSA top-secret material. This was unheard of. The NSA did not have leaks.

Several days later, the leaker went public. He was Edward Snowden, a 29-year old NSA contractor who looked even younger than his age, and he was in Hong Kong.

Snowden said he had released the material because it showed the US government was carrying out massive surveillance, and that this needed to be exposed. He seemed to be sincere.

US government officials were furious. Snowden became a wanted man, and the full power of the US government was deployed in an attempt to arrest him.

If you've read Robert Ludlum's novels about Jason Bourne, or seen the films based on them, starting with *The Bourne Identity*, you'll have an idea of how surveillance capacities might be used to track down a rogue agent. Something similar happened in Snowden's case, but this time in reality rather than fiction. The US government pulled out all stops, not to assassinate Snowden, but to arrest him.

If you followed the Snowden revelations via news reports, like me, some of the basic points will be clear but how it all hangs together may not be so obvious. For a broader perspective, I recommend Luke Harding's book *The Snowden Files: The Inside Story of the World's Most Wanted Man* (London: Guardian Books, 2014). Harding is a journalist for *The Guardian* and has obtained first-hand information on key events.

The Snowden Files covers Snowden's early online presence, his patriotism, his work for the NSA, his gradual disillusionment due to observing dubious activities carried out in secret, his collection of NSA files and leaking of them to *The Guardian*, and his experiences as a fugitive. In between the Snowden narrative, Harding tells about the massive spying operations carried out by the NSA and its partners, especially its British equivalent GCHQ. He also tells how the media – especially *The Guardian* – handled the biggest leak in history in the face of implacable hostility from intelligence agencies and top politicians. Snowden was incredibly brave and shrewd, but so were quite a few others in the story.

Lessons for whistleblowers

Here I offer a few lessons for whistleblowers based on Snowden's experiences. Although few whistleblowers reveal information warranting international headlines, every effort at speaking out in the public interest is important and hence worth doing as well as possible.

Leaking is revealing inside information, typically to media or sometimes to interested groups. A lot of leaks are from top politicians and bureaucrats. These leaks are everyday operations intended to manipulate public opinion for political or personal purposes.

However, when someone leaks information in the public interest, for example exposing corruption or dangers to the public, top managers typically treat this as a serious breach of trust. Leakers are often called traitors. The double standard is stark: it's okay for bosses to leak but not for employees.

Whistleblowers are people, typically employees, who speak out in the public interest, and most of the time they reveal their identity immediately, such as when they report a problem to the boss or some internal body. Unfortunately, this is disastrous much of the time: the whistleblowers are attacked – for example ostracised, denigrated, reprimanded, sometimes dismissed – and furthermore their access to information is blocked. As soon as their identity becomes known, they have limited opportunities to collect more information about wrongdoing.

For these reasons, it is often advantageous for whistleblowers to remain anonymous, and to leak information to outside groups, especially to journalists or action groups. The leaking option reduces the risk of reprisals and enables the leaker to remain in the job, gathering information and potentially leaking again. Furthermore, stories based on leaks are more likely to focus on the information, not the leaker.

Lesson 1: be incredibly careful

Snowden leaked the most top-secret information of anyone in history, but it wasn't easy. The lesson from his experiences is that to be a successful leaker, you must be both knowledgeable and incredibly careful. Snowden had developed exceptional computer skills. He was leaking information about state surveillance, and he knew the potential for monitoring conversations and communication. He took extraordinary care in gathering NSA documents and in releasing them. When he contacted journalists, he used secure email. When meeting them, he went to extreme lengths to screen their equipment for surveillance devices. For example, before speaking to journalists, he had them put their phones in a freezer, because the phones might contain monitoring devices.

Few whistleblowers need to take precautions to the level that Snowden did: his enemies were far more determined and technically sophisticated than a typical whistleblower's employer. Nevertheless, it is worth learning from Snowden's caution: be incredibly careful.

Lesson 2: choose recipients carefully

Snowden considered potential recipients for his leaks very carefully. He wanted journalists and editors who would treat his disclosures seriously and have the determination to publish them in the face of displeasure by the US government. He decided not to approach US media, which usually are too acquiescent to the government. US media have broken some big stories, but sometimes only after fear of losing a scoop. The story of the My Lai massacre, when US troops killed hundreds of Vietnamese civilians during the Indochina war, was offered to major newspapers and television networks, but they were not interested. In 2004, US television channel CBS initially held back the story about abuse and torture of Iraqi prisoners by US prison guards at Abu Ghraib prison, at the request of the Pentagon, finally going to air because the story was about to be broken in print.

Snowden didn't approach *The New York Times*. Snowden decided instead to approach *The Guardian*, a British media group with a history of publishing stories in the public interest, despite government displeasure. It was a wise choice.

Lesson 3: be persistent

Snowden decided to approach *The Guardian*, and not just anyone: in late 2012 he contacted *The Guardian*'s freelance columnist Glenn Greenwald, noted for his outspoken stands critical of US government abuses, especially surveillance. Snowden sent Greenwald an anonymous email, offering disclosures and asking Greenwald to install encryption software. However, Greenwald – resident in Brazil – was busy with other projects and didn't get around to it. So Snowden created a video primer for installing the software just to encourage Greenwald to use it. However, even this wasn't enough to prod the busy Greenwald to act.

Snowden didn't give up. In January 2013, he next contacted Greenwald's friend and collaborator Laura Poitras – a fierce critic of the US security state, and a victim of it – who he thought would be interested herself and who would get Greenwald involved. It worked.

The lesson is to be persistent in seeking the right outlet for leaks – and to be careful and patient along the way.

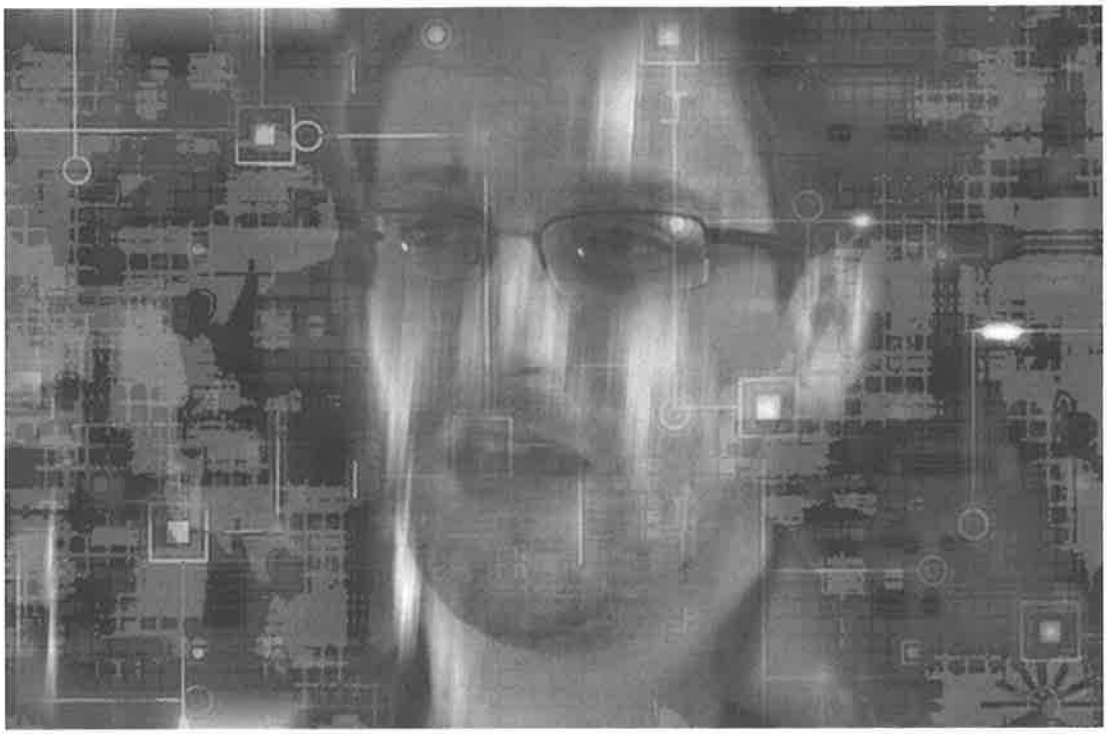
Lesson 4: improve communication skills

Snowden is a quiet, unassuming sort of person. He might be called a nerd. Contrary to some of his detractors, it was not his desire to become a public figure. Despite his retiring nature, Snowden knew what he wanted to say. He refined his key ideas so he could be quite clear when speaking and writing, and he stuck to his message.

Most whistleblowers need good communication skills to be able to get their message across. (In a few cases, leaking documents without commentary might be sufficient.) My usual advice is to write a short summary of the issues, but this isn't easy, especially when you are very close to the events. Being able to speak well can be just as important, if you have telephone or face-to-face contact with journalists or allies. Many people will judge your credibility by how convincing you sound in speech and writing. Practice is vital, as is feedback on how to improve.

›

› *Continued from Page 21*



Edward Snowden: through a lens darkly. Photograph by AK Rockefeller used under Creative Commons licence

Lesson 5: make contingency plans

Snowden thought carefully what he wanted to achieve and how he was going to go about it. Initially he leaked selected NSA files to journalists to pique their interest and demonstrate his bona fides. After all, who's going to believe someone sending an email saying they can show the NSA is carrying out massive covert surveillance of citizens and political leaders? After establishing credibility, Snowden then arranged a face-to-face meeting, to hand over the NSA files and help explain them: many of the files were highly technical and not easy for non-specialists to understand.

After the initial stories in and the ensuing media storm, Snowden knew that it would be impossible for him to remain in hiding. The US government would do everything possible, technically and politically, to find and arrest him. So Snowden decided to go public, namely to reveal his identity. This would help to add credibility to the revelations by attaching them to a human face.

He did not anticipate every subsequent development: it was not part of a plan to flee Hong Kong and end up in Russia. Even so, Snowden anticipated more of what happened than most whistleblowers, who are often caught unawares by reprisals and stunned by the failure of bosses to address their concerns and of watchdog agencies to be able to protect them.

The lesson from Snowden is to think through likely options, including worst case scenarios, and make plans accordingly.

Lesson 6: be prepared for the consequences

Snowden knew that leaking NSA documents would make him a wanted man. He was prepared for the worst scenario, arrest and lengthy imprisonment. He knew what he was sacrificing. Indeed, he had left his long-time girlfriend in Hawaii, knowing he might never see her again. He made his decision and followed it through.

So far, Snowden has avoided the worst outcomes, from his point of view. He might have ended up in prison, without access to computers (his greatest fear), perhaps even tortured like military whistleblower Chelsea Manning. Still, living in Russia – an authoritarian state, where free speech is precarious – is hardly paradise. Snowden is paying a huge price for his courageous actions. He knew he would, and he remains committed to his beliefs.

Whistleblowers seldom appreciate the venom with which their disclosures will be received. It is hard to grasp that your career might be destroyed, and perhaps also your finances, health and relationships. It is best to be prepared for the worst, just in case. Being prepared often makes the difference between collapsing under the strain and surviving or even thriving in new circumstances.

Reprisals are only partly directed at the whistleblower. The more important audience is other employees, who receive the message that speaking out leads to disastrous consequences.

Snowden has provided a different, somewhat more optimistic message. He has shown that the NSA is not invincible: its crimes can be exposed. He has shown that careful preparation and wise choices can maximise the impact of disclosures. He has stood up in the face of the US government, and continued unbowed. Although few whistleblowers will ever have an opportunity like Snowden, or take risks like he has, there is much to learn from his experiences.