BRIAN MARTIN

Snowden's Lessons for Whistleblowers

In June 2013, Edward Snowden burst onto the world media scene. He had worked as a contractor for the U.S. National Security Agency (NSA) and collected a vast quantity of top-secret documents. Snowden leaked the documents to the *Guardian,* a well-known British newspaper and media group, revealing that the NSA had been secretly carrying out extensive spying on electronic communications.

Snowden quickly became one of the world's best known whistleblowers. As well as extensive commentary in the mass and social media, several major books have been published about him and his revelations [1]–[3].

Lessons for Whistleblowers

I have been studying suppression of dissent since the late 1970s and have talked with hundreds of whistleblowers, seeking to provide practical advice [4]. So naturally I was impressed by Snowden's efforts and especially by his success in raising public awareness about surveillance.

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 ostracized, 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.

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. Snowden's experiences provide several valuable lessons for other whistleblowers.

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 extremely 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.

Digital Object Identifier 10.1109/MTS.2014.2367953
Date of publication: 1 December 2014

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 carefully considered potential recipients for his leaks. He wanted journalists and editors who would treat his disclosures seriously and have the determination to publish them in the face of opposition by the U.S. government. He decided not to approach U.S. media, which usually are too acquiescent to the government. U.S. media have broken some big stories, but sometimes only after fear of losing a scoop. The story of the My Lai massacre, when U.S. 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, U.S. television channel CBS initially held back the story about abuse and torture of Iraqi prisoners by U.S. 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 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 U.S. 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 U.S. 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.

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.

Snowden knew that it would be impossible for him to remain in hiding. The U.S. government would do everything possible, technically and politically, to find and arrest him. So Snowden decided to go public, namely to reveal his identity (though Greenwald convinced him to wait a few days after the initial media stories). Going public added 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 do 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 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 longtime 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

(continued on page 43)

All that these ideas really require is mutual respect and confidence in future business and cooperation.

Of course surveillance/data manipulation is one of the greatest potential human rights abuses. Those of us in the legal/tech community all recognize the dangers, but human society progresses with understanding and knowledge and harnessing data as a force for good (if ethically and carefully handled) can facilitate communication and understanding and enhance rights in developed and underdeveloped countries. Taking the opportunity to use data to combat human rights abuses is a positive that ought to be embraced.

Ideas and practices developed in cosmopolitan centers, such as at the United Nations, necessarily require translation into terms appropriate to the local context [6]. This is achieved by a combination of collective responsibility afforded to stakeholders networking together, and Government action plans which involve active collaboration with civil organizations and communities [7]. Human rights abuses occur in three contexts: past abuse, ongoing abuse, and abuse to come. Human history is understood through security, economy, health, education, and culture. These are terms that scientists can also understand. It is time for some big thinking to be done on big data – whether it is dropping pedometers from drones to monitor the movement of individuals, or whether it is harnessing social media to raise an issue or provide a vital and lifesaving service.

As I imagine Tess McGill might say if human rights lawyers turned up to a party for geeks… they might just be in the right place at the right time. Now all we have to do is find the guy with the money in the lift.

Author Information

Felicity Gerry, QC, is at 36 Bedford Row, London, U.K., and with Charles Darwin University, Australia. Email: Felicity.Gerry@cdu.edu.au.

References

[1] United Nations Entity for Gender Equality and the Empowerment of Women, "Conducting research, data collection and analysis," *endvawnow.org*, 2012; http://www.endvawnow.org/en/articles/322-conducting-research-data-collection-and-analysis-.html.

[2] S. Marsh, "How should councils use data? – Debate," *The Guardian* [online], Feb. 28, 2014; http://www.theguardian.com/local-government-network/2014/feb/27/how-should-councils-use-data-live-debate?CMP=twt_gu.

[3] J. Gabrys, "The Citizen Sense Project," *citizensense.net*, 2014; http://www.citizensense.net/about/.

[4] B. Fung, "How stores use your phone's wi-fi to track your shopping habits," *The Washington Post* [online], Oct. 19, 2013; http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits.

[5] University of Wollongong, *Map Jakarta (PETAJAKARTA) Project*, 2014; http://smart.uow.edu.au/projects/UOW164497.html.

[6] P. Levitt and S.E. Merry, "Unpacking the vernacularization process: The transnational circulation of women's human rights," 2012; http://citation.allacademic.com/meta/p_mla_apa_research_citation/3/1/0/9/2/pages310922/p310922-1.php

[7] J. Yogaratnum, "A review of the 2010 Domestic Violence Law in Timor-Leste," *Asian J. Comparative Law*, vol. 8, no. 1, pp. 1–26. 2013.

COMMENTARY *(continued from page 38)*

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.

Audience for Reprisals

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 showed that the NSA is not invincible: its crimes can be exposed. He showed that careful preparation and wise choices can maximize the impact of disclosures. He stood up in the face of the U.S. government, and continued unbowed. Although few whistleblowers will ever have an opportunity like Snowden, or take risks like he did, there is much to learn from his experiences.

Author Information

Brian Martin is professor in the School of Humanities and Social Inquiry, University of Wollongong, NSW 2522, Australia, and vice president of Whistleblowers Australia. Email: bmartin@uow.edu.au.

References

[1] G. Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London, U.K.: Hamish Hamilton, 2014.

[2] M. Gurnow, *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal*. Indianapolis, IN: Blue River Press, 2014.

[3] L. Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man*. London, U.K.: Guardian Books, 2014.

[4] B. Martin, *Whistleblowing: A Practical Guide*. Sparsnäs, Sweden: Irene Publishing, 2014.