Leakers: Truth-teller, Threat, or Fake News?

By Margaret S. Marangione

Snowden, Manning, Winner, and Comey. These names have captured the headlines of news media and, ironically, they have used news and social media to amp their fame through releasing, leaking, espionage, whistleblowing, or, depending who you ask, being wrongly accused. Additionally, President Donald Trump has conflated the issue with his war on reporters and news media. He either incorrectly accuses people of leaking or uses the term to underscore accurate reporting. For example, he stated, “leaks are a massive over exaggeration put out by the Fake News Media in order to make us look as bad as possible” (@realDonaldTrump, May 14, 2018). He also inaccurately called James Comey a leaker of classified information (Washington Post May 1, 2018). The word choice of “leaker” and its meaning has been used haphazardly. What it connotes and denotes has contributed to the muddling of leaking in understanding and managing both insider threats and Millennials in the workplace.

The sharing or leaking of government information is a multifaceted subject. Certainly, there is a history of leaking to media outlets and many can remember the Pentagon Papers blasting a new road to leaking in the early 1970s. Besides historic precedent, there are numerous variables that affect leaking in the twenty-first century, which include Millennials’ and the general public’s attitudes toward information sharing and validity, punishment of leakers, intent, and over-classification of information. Many feel that the increased amount of information being classified in the post-9/11 era has contributed to the prevalence of leaking. Additional factors include that information is purposefully leaked. There is politics in leaking, and people can be accused of leaking to fit an agenda of a politician or political party. Also, there seems to be a disparity in how leakers are punished and the use of the Espionage Act to punish them. For example, author John Kiriakou argues that the antiquated Espionage Act should be written to deal with issues of intent, motive, as well as applicability (Kiriakou 2014). He feels it should also be enforced without disparity citing Leon Panetta’s leaking information about waterboarding to screenwriter Mark Boal. “Besides,” he states, “it has never been applied uniformly and is woefully antiquated.” For example, the Espionage Act is so outdated that it refers to national defense information rather than classified information because the classification system had not yet been invented.

For Millennials, intent and motive of leakers is paramount. In the 2016 Rand Report, The Millennial Generation, 22 percent of Millennials polled felt Snowden
was a patriot and 15 percent said they would have released the information if they had been in his position (Weinbaum, Girven, and Oberholtzer 2016, 14). Clearly, with Millennials making up 59.7 percent of all military branches, and 30 percent of the Federal workforce, their attitudes, especially about information and transparency, are crucial for classified information management (U.S. Office of personnel Management 2017).

Another issue in examining these cases is the short-sighted examination with the lens of the psychology of espionage and insider threat model. In doing so, there may be a risk in utilizing an outdated psychological model of espionage pathologies and psychological traits and applying it to individuals in the digital age. Even the term “insider threat” seems old school when viewed through the lens of the millennial generation and the recent cases. For example, 58 percent of college students scored higher on a narcissism scale in 2009 than in 1982 (Roller 2013, para. 1). This is a major red flag for insider threat management, as narcissism is a characteristic of people susceptible as insider threats (Wilder 2017). Therefore, understanding what drives Millennials and how they feel about transparency, loyalty, information sharing, as well as their opinions of these prominent leaking cases can be a way forward for the government and its contractors in mitigating any possible Snowden effect.

While looking at Millennials with a microscope might provide clarity, some of the challenges are more large scale, which include the current whistleblowing reporting structure and lack of support for a whistleblower. The decision to prosecute whistleblowers under the Espionage Act is viewed by some, to include the perpetrators, as a gross war on “truth tellers” by ignoring the legal definition of whistleblower—any person who brings to light evidence of waste, fraud, abuse, or illegality. This brings us to another issue in this complicated problem, that whistleblowing, which many see as quality assurance, should be supported by the federal government and its agencies; new legislation must be written that would protect whistleblowers while allowing the government to prosecute traitors and spies.

Mr. Ellsberg, the leaker of the Pentagon Papers, who is 86, feels the Nixon administration’s attempt to halt the publication of those documents was a “mockery of democracy.” Mr. Ellsberg explains, “Can you have democracy in a real sense with the government having the final voice and the total voice as to what citizens shall know about what they’re doing and whether they are telling the truth and whether they are obeying the law? I should say no” (R.M. 2010, n.p.). Ellsberg echoes many of the current attitudes about leaking, information transparency, and news media. Justice Hugo Black, in his ruling on the Pentagon Papers, sounds eerily modern in light of Snowden, Winner, and Manning’s professed motives and intent. Justice Black stated, “The guarding of military and diplomatic secrets at the expense of informed representative government, provides no real security for our Republic...the Framers of the First Amendment, fully aware of both the need
to defend a new nation and the abuses of the English and Colonial governments, sought to give this new society strength and security by providing that freedom of speech, press, religion, and assembly should not be abridged” (Priest 2016, para. 7). Under the Trump administration, in addition to the blurred lines between leaker and traitor as well as the continued discrediting of journalism, whistleblower protection, and the First Amendment have also come into question.

Recent developments in the offices and cases handling whistleblowers are not encouraging for individuals with grievances and have increased the likelihood that leaking will continue when only 5 percent of reported cases are investigated (OSC 2016a, 2016b). The OSC report, published in September 2017, acknowledges that “whistleblowers play an important role in safeguarding the federal government against waste, abuse and fraud. However, [they] also risk reprisal such as demotion and firing” (OSC 2016a, n.p.).

Corresponding with these issues are the Department of Defense Office of the Inspector General (DODIG) investigations into employee whistleblower reprisal for 2013–2015, which did not meet statutory or timeliness goals for 83 percent of the cases (U.S. GAO 2017, para. 1). For example, DODIG’s timeliness goals were 240 days, but the average length of investigations was closer to 608 days (para. 1). This office also found that whistleblowers risk reprisal such as demotion, reassignment, and firing, as was found in the OSC report.

**Twenty-first Century Leaks**

The recent leaking cases underscore the disparity of feelings between leaker versus traitor and transparency versus treason. For example, in 2013, U.S. Army Intelligence Analyst Chelsea Manning delivered classified documents that she found troubling to WikiLeaks, after attempting to contact the *New York Times* and *Washington Post*, and was sentenced to 35 years in prison for espionage and theft (Tate 2013). The judge in Manning’s case stated that, “Providing classified information for mass distribution is a sort of treason if the government can prove the defendant knew he was giving information to the enemy by indirect means” (Liptak 2013, para. 4). Aiding the enemy is based on military law, and is not applicable to leakers in nonmilitary employment or media.

Intent seems to be a slippery slope of proof and is difficult to determine or prove a person’s or a publication’s intent. What applies to these cases is they expose the tension between government transparency, which is essential to a democratic society and weighed as paramount for Millennials, with the equally pressing factor of protecting national security from disclosure of information that could be used by people or groups to harm U.S.’ interests.

The American Civil Liberties Union referred to Manning’s ruling as a “... sad day for all Americans who depend on brave whistleblowers and a free press for a
fully informed public debate” (Tate 2013, para. 5). Manning states that the reasons for leaking classified information were her questioning of the morality and ethics of U.S. policy. Regarding serving time, she stated, “You have to pay a heavy price to live in a free country” (para. 11). Perhaps no one knows this better than Edward Snowden who was granted asylum in Russia after his information dump.

In 2013, Edward J. Snowden leaked classified details of a top-secret National Security Administration (NSA) electronic surveillance program to the Washington Post and the Guardian. The information revealed that the NSA and the FBI were collecting data, including email, chats, videos, photos, and social networking information from ordinary Internet users in the United States and abroad. Though some denounced Snowden as a traitor, many others, and especially Millennials, supported his actions, calling him a whistleblower.

Federal prosecutors charged Snowden under the Espionage Act; Snowden felt that mass surveillance by the government was going unchecked and that the classification rules were preventing public debate about this subject. Regarding the avalanche of issues that resulted from his information leak and exile, he stated, “... the mission’s already accomplished. I had already won. As soon as the journalists were able to work, everything that I had been trying to do was validated ... I wanted to give society a chance to determine if it should change itself ... All I wanted was for the public to be able to have a say in how they are governed” (Gellman 2013, para. 7).

Snowden may have been right according to U.S. District Judge Leon who described NSA’s surveillance capabilities as “Orwellian” and “probably unconstitutional” (Gellman 2013, under “Going in Blind”). For the NSA, an agency accustomed to watching but not being watched, they had the eye of public scrutiny to suddenly endure as a result of Snowden’s actions. Snowden’s supporters argued that his actions opened up a much-needed debate on security, privacy, and transparency within the federal government. Cyber Security Professor and Baby Boomer Greg Austin stated, “When Edward Snowden went public with his leaks in 2013, in our organization in New York, we did a survey and found that [Millennials] thought he had done the right thing and people of my generation thought he had done the wrong thing” (Haynes 2017, under “Does he have a point?”). The former Director of the CIA Michael Hayden concurs: “I don’t mean to judge them all, but this group of Millennials ... simply have different understanding of the words loyalty and secrecy and transparency than certainly my generation did” (n.p.). Director of Australian Centre of Cyber Security, Jill Slay agrees: “My generation feel bound by [the] Official Secrets Act ... This generation values individuality” (under “New research shows Millennials have different views on cyber security”).

Snowden does not feel he broke an oath of secrecy though he signed standard form 312, the classified information nondisclosure agreement, because it is, according to Snowden, a civil contract. “The oath of allegiance is not an oath of
Leakers: Truth-teller, Threat, or Fake News?

Leakers: Truth-teller, Threat, or Fake News?

That is an oath to the constitution. That is the oath I kept that Keith Alexander and James Clapper did not" (Gellman 2013, under “They elected me”). Snowden also said that the law that Reality Winner was charged under when she exposed Russian hacking of elections “must be resisted” (Zaid 2017, para. 2). This sense of the importance of their own individuality and the power of their own ideas makes Millennials less tied to institutions and employers. According to the Pew Research Center study, Millennials have entered adulthood with low levels of trust and detachment to traditional institutions like employers, government, and even marriage (Pew Research Center 2014). Being less tied to employer ethics and values than the Baby Boomer generation should cause the Intelligence Community some concern, which has been fueled by another detrimental leak of classified information in the June 2017 case of Reality Winner.

On social media, people called Reality Winner a hero and a whistleblower and began raising money for her defense and family as soon as she was apprehended. Winner was accused under the 1917 Espionage Act of providing classified information about Russian hacking of U.S. elections to the news website the Intercept. “I felt really hopeless,” states Winner as to why she leaked the information. “... I was not trying ... to be a Snowden or anything” (Choi 2017, para. 5). The leak, published on the Intercept in June 2017, revealed an attempted hack by Russia’s military intelligence unit during the contentious 2016 U.S. presidential election (para. 6).

Whistleblower? Leaker? Spy?

The classified document that Reality Winner disseminated to the world through the Internet was obviously newsworthy, concerning, and ground-breaking in an election that was divisive, contentious, and murky. But, nothing in the document that she leaked exposed any type of fraud, waste, abuse, or unlawful conduct by the U.S. government. Legally, anyone who leaks classified information to the media instead of appropriate governmental channels is not a whistleblower entitled to legal protection. Because she signed, under her own volition, a secrecy agreement, she was bound by law, oath, ethic, and morals to her government to protect material she was handling and exposed to from unlawful disclosure, which included news outlets.

For an employee in the Intelligence Community, wanting to do the right thing in the face of a difficult and challenging ethical and moral issue can still be daunting despite all the whistleblowing avenues for reporting. For example, the clear-cut definition of whistleblower is Army SPC. Joseph Darby, who blew the whistle on prisoner abuse in Abu Ghraib and provided his superiors with a CD showing prisoner tortures; three months later, the abuse aired on “60 Minutes.” While not arrested, Darby has been ostracized by members of the military who labeled him a traitor (McLaughlin 2017a, 2017b).
There are other challenges besides being ostracized that face a whistleblower. Melvin Goodman, formerly with the CIA and State Department, feels intelligence employees have grounds to worry that their anonymity may not be protected, Congress may not follow up, and workplace culture will not support them. For example, with the Pentagon Papers, Daniel Ellsberg gave copies to Congress more than a year and a half before he released them to the New York Times. He released the Pentagon Papers to the New York Times because he received no input, action, or even concern (para. 11). So, going to the press may be the only successful avenue for government employees who want a problem to receive attention. “This is what whistleblowing is all about—going to the public arena to talk about wrongdoing,” said Goodman. “There aren’t a lot of avenues other than the media. The so-called guardrails of democracy are broken” (para. 13). Besides, echoes Attorney Edward McMahon, who represented a CIA officer who leaked information in 2015, “Not every government secret is national defense information,” and, therefore, not punishable under the Espionage Act (n.p.).

Many Millennials, having grown up in an era of transparency, believe that information was meant to be shared. They feel that the government not supporting transparency and freedom of information violates the First Amendment. What is paramount for this generation is that the government must validate that the disclosure of truthful information is necessary and important to the public debate. This idea about truth, transparency, and information sharing is critical to understanding the Millennial generation, how it shapes their relationships and their worldview, and the larger scale issue of insider threat management.

**The Millennial Connection: Snowflakes or Truth Tellers?**

Every generation has looked at the generation preceding it as somewhat of an anomaly. Aristotle, in 320 BC, stated, “The young people of today think of nothing but themselves ... they have no reverence ... they are impatient of all restraint ...” Aristotle’s young people did not have smartphones or have most of their friends on Facebook (Pew Research Center 2014). This technology revolution has isolated the current generation in their global virtual village and made information immediate, shareable, and downloadable. This globalization and privilege is empowering and sometimes frightening, especially when the information that can be shared via social media and the Internet can run the gamut from a detrimental picture on Facebook to destroying national security.

Both the Pew Research Center and the Rand Corporation have produced similar findings about the Millennial generation’s value of sharing and transparency, with the common denominator being their exposure to and use of the Internet, and social media and its assisted technology from an early age. This sentiment is echoed by Shane Lambert, who has over 20 years of experience in Insider Threat Program Management. Lambert feels that Millennials do not comprehend why
we need state secrets because they share everything, and they have different ideas about privacy. “They are a generation of free information” (Marangione and Crosby 2017, n.p.).

Besides their views on information sharing, Millennials have a jaded and skeptical view of the federal government. According to one Millennial, “We don’t blindly trust these institutions; we understand their limitations and know their greed and corruption are inevitable ...” (Weinbaum et al. 2018, n.p.). Almost 80 percent of Millennials do not trust the federal government (“Survey of Young Americans’ Attitudes Toward Politics and Public Service” 2014, 17). Sixty percent of Millennials feel that the guiding morality in any situation is that they will just be able to feel what is right (Stein 2013). Many call these divided loyalties. According to Lambert, “They might be Americans but their allegiance is to their own beliefs and ideologies and definitely not their government” (Marangione and Lambert, pers. comm., 2017).

**Millennials and the Psychology of Espionage and Insider Threats**

Democratic, liberal views on political and social issues, maintaining a distance from what have been the core institutions of marriage, religious affiliation, and employers, the Millennial generation has taken the ideas of Emerson’s self-reliance to new levels. According to a Pew Research Center study, Millennials are considerably more liberal than other generations: about four-in-ten Millennials are mostly (28 percent) or consistently (13 percent) liberal in their views, compared with 15% who are mostly (12 percent) or consistently (3 percent) conservative (44 percent are ideologically mixed) (Pew Research Center 2014, n.p.).

While their independence can be exciting, their attitudes have been causing alarm within the Intelligence Community. For example, how do you mitigate an insider threat if they are all insider threats? One of the key variables in mitigating insider threats is being on the lookout for narcissistic personalities in the workplace, as narcissistic personality disorder is nearly three times as high with Millennials than people 65 or older. Importantly, narcissism can also be connected to feelings of entitlement (Stein 2013).

“I have done nothing wrong .... I no longer work for the government but the people,” tweeted Snowden, which can be interpreted as the benchmark of Millennial attitudes regardless of its tone of grandiosity and entitlement (The Guardian 2013, n.p.). This generational affectation, coupled with research that supports that constant interacting with a screen all day supplies a hit of dopamine when someone responds to a tweet or post, can reduce empathy (Stein 2013). Millennials may not see the far-reaching implications of their behaviors or how their ethical choices might implicate national security. According to Joel Stein, “Not only do Millennials lack the kind of empathy that allows them to feel concerned for oth-
ers, but they also have trouble intellectually understanding others’ point of view” (para. 9). This might explain how Snowden, Manning, and Winner disseminated classified information without awareness for the causal chain that might follow for themselves or the country. “They do not understand the long-term damage of leaks and how it compromises the United States” says Lambert (Marangione and Lambert, pers. comm., 2017). Fran Moore, former CIA Assistant Director, echoes, “Individuals like Snowden, Manning and Winner do not care about ramifications” (Marangione and Moore, pers. comm., September 19, 2017). Moore goes on to state, “One of the challenges of an organization that must be made clear is it is never O.K. to spill secrets. The real question is: how do you recognize if you have a Snowden [Winner or Manning] working for you?” This can be doubly troubling for the Intelligence Community if the Millennial generation has had such a profound shift in attitude that makes the insider threat as outlined by the National Cybersecurity and Communications Center’s (UCEERT) and psychology of espionage model outdated.

The model for espionage as outlined by CIA’s psychologist Ursula Wilder includes life crises, pathologies, and ease of opportunity, as well as financial gain. Wilder describes espionage as spying for the purpose of working against your own country. Leakers are defined as not involved with long-term dissemination and are not paid (Wilder 2017). Millennials do not fit into a clear diagnostic model of profiles for espionage. Wilder feels that the personality traits of narcissism, immaturity, and entitlement as well as the variable that long-term Internet usage “un-balances people,” are criteria that must be monitored for leakers. Well, welcome to the Millennial age.

Therefore, are these variables useful for mitigating insider threats? Perhaps the paradigms of working with Millennials, who have been molded and shaped by the information age and believe in transparency and their own ethical model, must be seen as normative. Perhaps it is the Intelligence Community’s approach to managing insider threats that has to change just like the Intelligence Community had to change, reactivity, after 9/11.

Recommendations

The partnership of Millennials and the Intelligence Community has to flourish. Millennials and the rising generation’s need for information sharing has to be acknowledged. The paramount necessity of a whistleblower program must be valued as serious by all parties involved. Without this, the Intelligence Community runs the risk of increased intelligence leaks, especially in this divisive political climate where Millennials feel that the government and leadership are at odds with their own morals and ethics. If the Intelligence Community does not channel dissent into constructivism, leaks may grow worse.
Leakers: Truth-teller, Threat, or Fake News?

The culture of all agencies and contractors handling classified information must strengthen ethical and law-abiding practices and this must be clearly embraced in a company’s mission and values and honored by the management. Employees must feel that management encourages and, more importantly, requires employees to discuss any issues and challenges they perceive as incongruous in the workplace; whistleblowers must be seen as improving the work environment, increasing accountability, and employers must honor transparency.

Often, the Intelligence Community has approached change from a reactionary position as exemplified by its overhaul post-9/11 despite a morphing international terror threat at the end of the twentieth century. Mitigating the Snowden Effect does not come from a 1950s insider threat model, a punitive approach to employee management, or a close scrutiny and monitoring of individuals. It comes from reshaping the workplace for inclusion and transparency, modifying the Espionage Act and providing a whistleblower protection framework so that an employee has no reason to leak information. Whistleblowers must not be ignored or punished. Otherwise, WikiLeaks and the Media will continue to be the whistleblower’s only course of action.

Efforts must be given to a basic shift in values that have direct implications on daily operations and employees must know from a tactical, strategic, and logistical perspective that they will be encouraged to bear witness honorably through appropriate channels. The culture of all intelligence agencies must highlight ethical, law-abiding behavior and employees must feel that management does not just encourage but expects employees to hold themselves, each other, and the organizations that they work for to standards of accountability.

Research supports that Millennials have a new attitude toward work and their faithfulness is to their own ethics; the government may be headed down a slippery slope for classified information management and leaking. This might be exasperated by the recent administration’s divisiveness, challenges to the legitimacy of information, and the dismantling rather than strengthening of current offices for reporting and protecting whistleblowers. Changing the paradigm must be paramount for every organization, otherwise Snowden, Manning, and Winner are just the canary in the coalmine.

References


Leakers: Truth-teller, Threat, or Fake News?


