Cyber Whistleblowers: The Black Sheep of Whistleblowing?

Andrew Wisniewski Jr.
Christopher Newport University

Cyber Whistleblowers: The Black Sheep of Whistleblowing?

Andrew Wisniewski, Junior, Christopher Newport University

Research Mentor:
Dr. Iria Giuffrida, Professor of the Practice of Law, William & Mary Law School, and Visiting Faculty for Business Law, Raymond A. Mason School of Business

Contents

Table of Contents

Introduction

Twitter has been grabbing the headlines for weeks, and we are likely to read much more about it over the next few months. While the current news concerns Elon Musk's purchase of Twitter and his attempts to turn around the fortunes of this popular social media site, Twitter was recently on the news for a different reason: whistleblowing. In July 2022, Peiter "Mudge" Zatko, Twitter's former head of security, blew the whistle on Twitter's allegedly shockingly poor cybersecurity and privacy practices (Duffy, O'Sullivan, and Fung, 2022). Mr. Zatko made disclosures about these issues to Congress and Federal Agencies. He also made disclosures to the media and agreed to be identified.

Merriam-Webster defines a whistleblower as "one who reveals something covert or who informs against another". A definition that brings in more context would be "the disclosure of organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (Near & Miceli, 1985). Essentially, whistleblowing is the act of exposing wrongdoing in an organization.

This paper calls "cyber whistleblowers" those whistleblowers who expose an organization's wrongdoings or negligence with its digital security, which puts at risk not only their commercial information but also their customers' data and, potentially, the security of other public and private organizations. Companies that have misused data, such as Facebook in the context of the Cambridge Analytica scandal, are becoming more prevalent in our ever-advancing digital age, so there is an increasing demand for cybersecurity professionals to speak out. There has been a trend for businesses to treat cybersecurity as an afterthought and the users are paying for it (Makrygiannis, 2020). For example, the Anthem medical data breach where 78.8 million users were affected (Mathews, 2015). These users might face potential identity theft issues in the future due to negligent digital security.

Whistleblowers have legal protection under the Whistleblower Protection Act (WPA) and the Civil Service Reform Act of 1978 (CSRA). However, despite these protections, there is a disconnect between these protections and the treatment of cyber whistleblowers. Currently, there are no federal laws that specifically protect cyber whistleblowers (Alam, 2020). Due to

the lack of specific federal protection cyber whistleblowers are at risk of retaliation for their whistleblowing actions.

While in the context of other domains, such as financial integrity, whistleblowing is considered a necessity for combating corruption, cyber whistleblowers are seen as threats to organizations. Without an internal actor that reveals wrongdoings behind the curtain, the public would remain ignorant of these misdeeds. For example, in the case of Facebook and Cambridge Analytica, users were being targeted with political ads based on data collected without their consent. If it were not for Christopher Wylie that blew the whistle on this "psychological warfare tool," the public would have been left ignorant about these nefarious uses of data (The Guardian, 2018).

Whistleblowers lack a safe setting for their complaints to be heard. There are two ways in which whistleblowers' complaints could be heard. One is internally through the company or entity for which they work. However, there is a risk that these complaints are ignored and may even trigger some form of retaliation. On the other hand, a whistleblower could report externally. In the absence of a central agency responsible for receiving whistleblowing complaints in the context of cybersecurity, whistleblowers have leaked sensitive data to the public at large, causing unintended harmful consequences.

Contrary to popular belief, this paper argues that cyber whistleblowing can contribute to a greater cyber security posture. However, this requires the development of clearer legal obligations and protections for cyber whistleblowers. This paper will explore the psychology behind whistleblowing, the effectiveness of whistleblowing in a cybersecurity context, how to create a safer and more transparent environment for whistleblowers and companies, and how current laws contribute to cyber whistleblowing.

Whistleblowing explored through the psychology and legal lenses

Identity Fusion Theory and whistleblowers

The first step in the proposed analysis is to explore how the literature assesses the role of cyber whistleblowers. This paper will focus on two specific domains: psychology and law.

There is a psychology theory that establishes a trend with whistleblowers called the Identity Fusion Theory (Swann, 2009; Gomez, 2011; Whitehouse & Bastian, 2012). This theory evaluates a 'fusion level' between an individual and their 'fused' organization. If a person is strongly fused, that means their individual identity and group identity mesh together. This leads the individual to take pro-group actions despite detrimental individual consequences, to achieve a positive group outcome. This includes a greater willingness to physically fight and sacrifice their lives to defend their country from threats (Swann, 2009; Gomez, 2011).

Strongly fused individuals also tend to form close identity relations with other group members (Buhrmester, 2013). Highly fused individuals are more likely to endorse committing suicide to save fellow country members' lives (Swann, 2009; Morales & Hixon, 2010; Gomez, 2011). Most notably strongly fused individuals are willing to endure severe in-group ostracism to retain the ability to promote their group (Gomez, 2011).

These trends of extreme responses are also apparent when applied to the context of whistleblowing. Experimental studies have concluded that Identity Fusion Theory is the best predictor of whether an individual is likely to be a whistleblower (Buhrmester, 2013). Identity Fusion Theory was tested in a more real-world context in Buhrmester's dissertation. Buhrmester tested the fusion levels of university students in a real-world situation. Students were placed in a room under the impression they would be taking a test. The test was designed with the presence in the room of a "planted" cheater: a student who—under the direction of the experiment organizer—outwardly took the answer key from a drawer and copied the answers, in full sight of the other students. During the debriefing session, about 70% of the strongly fused individuals mentioned the cheating to the confidant, a member of the research team, while only 40% of the moderately fused mentioned it, and only 30% of the weakly fused did so (Buhrmester, 2013). Having gathered the fusion levels of the students and having a confidant speak to the tested student after they took the test, it was concluded that fusion theory was the best predictor of whether a person would whistleblow (Buhrmester, 2013). This demonstrates that whistleblowers are not outsiders or malicious actors, but individuals working for their group's best interest. When examining whistleblowers, they should be treated as a personality trait instead of people who engaged in a one-time act. This will help break down the stigma that

speaking up is wrong. Whistleblowers speak up because of their loyalty to a group instead of a traitorous adversary.

Whistleblowers and the law

From a legal standpoint, the United States grants whistleblowers protection against retaliation. Some examples include the Civil Service Reform Act of 1978 (CSRA) and the Whistleblower Protection Act (WPA). There are even certain laws, such as the False Claims Act, that offer whistleblowers financial rewards for reporting fraud and other serious regulatory violations (Callahan, 2000). However, the type of protection that whistleblowers can receive depends on the type of information that they share and the kind of employee that they are (federal employees receive different protections than employees of private businesses).

Although cyber whistleblowers are technically under this umbrella, they exist in a gray area. Due to the nature of security and the risks of triggering national security concerns, cyber whistleblowers are often faced with retaliation. Some have been charged with criminal offenses due to their actions not being covered by the whistleblowing legal frameworks. An example that dominated the discussions about cyber whistleblowers is Edward Snowden. In 2013, he leaked data exposing mass surveillance operations conducted by U.S. and British intelligence agencies (Dance, Gellman, Macaskill, and Poitras, 2013). Because Snowden released classified information, his actions fell outside the scope of WPA. Therefore, despite being a whistleblower, Snowden was charged under the Espionage Act.

Many businesses have historically ignored internal whistleblowing complaints, as evident with Cheryl Eckard and Mary Willingham. Eckard blew the whistle on GSK, the multinational pharmaceutical company where she was working, about GSK's poor health standards in a plant in Puerto Rico. Eckard repeatedly reported internally her concerns only to be ignored and, eventually, terminated (Lipman, 2012; Pope, 2018). Willingham was the professor at the University of North Carolina who discovered that, for over 20 years, some colleagues had been giving fake classes to student-athletes–this came to be known as the paper class scandal. Willingham reported her concerns internally as well, only to be ignored until she eventually blew the whistle on a blog (Pope, 2018). What followed were years of accusations on the part of the university until an independent review found widespread and systematic

academic fraud (Ganim, 2015). She eventually sued the university and agreed on a settlement. The cases of Eckard and Willingham demonstrate the imbalance between whistleblowing complainants and the internal enforcement of these complainants.

There needs to be a safe procedure for cyber whistleblowers to report their concerns. Cyber whistleblowers are seen as insider threats to an organization. Evident with the SolarWinds breach some organizations only bolster digital security post-breach. In 2021, SolarWinds, a software company known for its networks and information system management tools, revealed that it had fallen victim to a supply-chain attack that caused the company's data breach (GAO, 2021). Three years before this attack took place, Ian Thornton-Trump had suggested to the SolarWinds executives to hire a senior director of cybersecurity (Bloomberg, 2020). Because the management was unresponsive to the suggestions, Thorton-Trump felt compelled to resign (Bloomberg, 2020).

Proposed Solution for Cyber Whistleblowing Dilemma

Understanding Identity Fusion theory as a personality trait that many whistleblowers possess, would help expunge the stigma of whistleblowers as traitors. Whistleblowers blow the whistle, not for a petty chance at fame or as retribution against their employers, but because they feel that their identity has been attacked by wrongdoings toward their fused group. Since fused individuals take pride in their group, they are more likely to feel the need to speak up to remedy wrongful acts. To help combat this flawed understanding there needs to be a larger public discourse on the psychology of whistleblowing. Applying the Identity Fusion theory in the context of whistleblowing demonstrates that whistleblowers are trying to do "good" and are reacting against the ethical misconduct at the core of the whistleblowers' complaint (such as academic dishonesty).

An important extension that needs to be made is an application of Identity Fusion theory to cyber whistleblowers: they do not see themselves as insider threats–far from it. To help differentiate cyber whistleblowers from insider threats, an analysis of the trends of fusion level within malicious insider threats is necessary. This will solidify the difference between good faith whistleblowers and insider threats.

There is a disconnect between the treatment of cyber whistleblowers, especially those that identify potential national security hazards, and legal whistleblower protection. The general whistleblowing protection the United States currently has in place can only be vaguely attributed to cyber whistleblowers due to the scope being outside what is 'allowed'. Whistleblowing is at the forefront of exposing organizational wrongdoing. The current legal regime provides very limited opportunities for whistleblowers of classified information to report their concerns (currently, they can only do so to the Department of Justice). Cyber whistleblowers should not face different treatment due to their complaints involving classified materials. Whistleblowing should be accepted and encouraged at all levels, especially in our government.

The difference between whistleblowing in the private sector and the federal government is that a private company is not the same entity that pursues charges for whistleblowers, while the federal government does. Edward Snowden fled the country and then blew the whistle because he knew of this reality. Chelsea Manning blew the whistle with numerous classified documents and videos of United States military personnel unlawfully engaging civilians. Manning was sentenced to thirty-five years by the United States court martial.

Having a neutral third party in place would help remedy this issue by allowing an investigation that is not plagued by ulterior motives. This independent entity would also act as a safeguard against sensitive information being released to the public that can cause harm and national security threats. If names of spies or covert operations currently undergoing were to be leaked that would put the personnel involved in physical danger. Historically, abortion doctors that have had their names leaked have faced harassment and have even been murdered (Cairney, 1999). A leak could spark the same extreme physical danger or put the United States at risk of a cyber attack by a foreign threat actor. This is another case where an independent entity would step in. Instead of whistleblowers mishandling sensitive data, they would report it to an independent entity, which, in turn, would address the issue at hand while not releasing information that can lead to harm.

The increasing number of data and cybersecurity breaches requires a different approach to whistleblowers. Like in other domains, they should be considered a resource to prevent harm,

rather than a source of harm. It is valuable to identify companies using data for nefarious purposes or who have negligent security policies. The public deserves to know what is happening with their data. Businesses with poor cyber practices are getting away with massive data breaches putting many of their users at risk. The average user is unaware of how their data is being used and how protected if at all, their data is behind the scenes. Without cyber whistleblowers, the public would never know about the nefarious use of their data.

Organizations have to be more responsive internally to matters of digital security to avoid large data breaches. However, since organizations are beholden to their shareholders, digital security often risks being left underfunded until drastic change occurs. Cyber whistleblowers need to have the option to report their complaints and be heard not by the same entity that is committing the wrongdoing.

Currently, once whistleblowers blow the whistle on information pertaining to national security, their whistleblowing protection goes by the wayside. The entities that are at risk of whistleblowing complaints are the same entities that persecute these whistleblowers.

There is no safe avenue for whistleblowers to voice their complaints. Some whistleblowers attempt to file a concern internally only to be ignored or face retaliation such as the case with Cheryl Eckard and Mary Willingham. Some whistleblowers file concerns externally with an agency, the media, or on their own, which can cause the wrong information to be leaked. One of the hurdles in cyber whistleblowing is that whistleblowers are seen as insider threats to an organization. Instead of correcting the issue that the whistleblower is complaining about, entities take the approach of treating whistleblowers as inside attackers and this obfuscates the truth. Without clear protection from retaliation, cyber whistleblowers cannot safely and reliably report cyber breaches and weaknesses. Government agencies are a historic example of organizations that retaliate against whistleblowers in terms of whistleblowers facing criminal charges. While private whistleblowers can be shielded from certain retaliation, government agency whistleblowers have faced retaliation in the form of felony criminal charges under the Espionage Act. A safe outlet would assist in making the whistleblower seem less like a spy and more like a concerned employee. An independent third-party outlet that focuses on

correcting wrongs instead of prosecuting whistleblowers would help remedy this rift in cyber whistleblowing.

Furthermore, having an independent third party receive cyber whistleblower complaints will assist in classifying whistleblowers from just being insider threats. Instead of focusing on vilifying the whistleblowers, this independent third party would seek to establish the objective truth. The lack of external accessibility in cybersecurity complaints is contributing to businesses taking advantage of the current lax data protection laws. Without more cyber whistleblowers exposing improper data security, companies will continue to treat security as an afterthought.

Taking a step back from the whistleblower's point of view, it is important to examine the reasons why other employees did not blow the whistle. Fear of retaliation and fusion levels help paint the picture of why many individuals do not blow the whistle. As evident from past ethical research on the Trolley Problem, most people act in an ethical manner (Bruers & Braeckman, 2014). With current research, there is no correlation between low-fused individuals and a lack of an ethical code. Therefore, it would not be fair to draw a conclusion that low-fused individuals agree with the wrongdoings due to their complacency.

Two important traits that will hinder whistleblowers are how the wrongdoing affects them personally or the consequences associated with speaking out. In highly fused individuals, the threshold for what they consider to affect them personally is lower due to their personal and group identities being merged. Low-fused individuals, on the contrary, may not feel it is their place to step up and do something. This inevitably leads to the bigger reason why whistleblowers do not speak out and is a result of the lack of legal or physical protection as a whistleblower. In the case of Edward Snowden, he is not the only former NSA contractor that is against mass privacy intrusion. However, he was the only contractor that took the risk of disclosing the mass surveillance at the cost of having to go into hiding from the United States government. When more options are available to voice employees' concerns, employees feel more empowered to blow the whistle on these negligence standards.

An additional line must be drawn on the legal persecution of these cybersecurity complaints. If a data breach occurs in a company, should it be standard to terminate the executive officer in charge of cybersecurity? The focus should be on applying better

cybersecurity procedures in organizations to *prevent* these issues instead of attempting to vilify an individual if a data breach occurs. Focusing too much on an individual will create a scapegoat situation instead of finding solutions to mitigate these attacks in the future. Companies should take more responsibility for upholding digital security through effective cybersecurity measures.

Conclusion

Cyber whistleblowing is not specifically protected by the law, which leaves a disconnect between cyber whistleblowers and legislation. Specific legislation pertaining to cyber whistleblowing would lead to more cybersecurity professionals speaking out and effective measures to ensure proper digital security standards. Once a whistleblower exposes classified material, they are subject to criminal charges, which creates obfuscation of wrongdoings from the public's eye. The Identity Fusion Theory helps showcase how whistleblowers are pro-group activists instead of malicious actors attempting to achieve fame. Whistleblowers of classified materials and negligence of digital security should be accepted without fear of scrutiny or reprisals. Furthermore, having an independent third party that has no invested interest receive these types of complaints will assist whistleblowers in protection and accessibility.

References

- Buhrmester, M. D. (2013, August 1). *Understanding the cognitive and affective underpinnings of whistleblowing*. TexasScholarWorks. Retrieved September 20, 2022, from http://hdl.handle.net/2152/21278
- Bruers, S., Braeckman, J. A Review and Systematization of the Trolley Problem. *Philosophia* 42, 251–269 (2014). https://doi.org/10.1007/s11406-013-9507-5
- Cairney R. Leak of abortion information creates turmoil at Foothills. CMAJ. 1999 Aug 24;161(4):424-5. PMID: 10478169; PMCID: PMC1230551
- Callahan, Elletta Sangrey, and Terry Morehead Dworkin. "The State of State Whistleblower Protection." American Business Law Journal, vol. 38, no. 1, Fall 2000, pp. 99-176. HeinOnline
- *Civil Service Protections for Federal Employees: Overview*. https://content.next.westlaw.com/practical-law/document/I7129290c862d11e498db8b09b4f043e0/Civil-Service-Protections-for-Federal-Employees-Overview?viewType=FullText&contextData=(sc.Default).
- Ganim, Sara. "UNC 'Fake Classes' Whistleblower to Get $335k in Settlement." *CNN*, Cable News Network, 17 Mar. 2015, https://www.cnn.com/2015/03/17/us/north-carolina-willingham-unc-settlement.
- Gellman, Barton, and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *The Washington Post*, WP Company, 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.
- Goldman, Barry M. "Toward an Understanding of Employment Discrimination Claiming: An Integration of Organizational Justice and Social Information Processing Theories." *Personnel Psychology*, vol. 54, no. 2, 2001, pp. 361–386., https://doi.org/10.1111/j.1744-6570.2001.tb00096.x.
- Gómez, Á, Brooks, M.L., Buhrmester, M., Vázquez, A., Jetten, J., & Swann, W.B. (2011). On the nature of identify fusion: Insights into the construct and a new measure. Journal of Personality and Social Psychology, 100, 918-933
- Hammer, Dallas, and Jason Zuckerman. "Solarwinds Breach Shows Why Cybersecurity Whistleblowers Need Protection." *Bloomberg Law*, 2 Feb. 2021, https://news.bloomberglaw.com/business-and-practice/solarwinds-breach-shows-why-cybersecurity-whistleblowers-need-protection.

- "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower." *The Guardian*, Guardian News and Media, 18 Mar. 2018, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

- Landert, Daniela, and Gianluca Miscione. "Narrating the Stories of Leaked Data: The Changing Role of Journalists after Wikileaks and Snowden." Discourse, Context & Media, vol. 19, 2017, pp. 13–21., https://doi.org/10.1016/j.dcm.2017.02.002.

- Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." Big Data & Society, vol. 1, no. 2, 2014, p. 205395171454186., https://doi.org/10.1177/2053951714541861.

- MacAskill, Ewen, et al. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained." *The Guardian*, Guardian News and Media, 1 Nov. 2013, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

- Makrygiannis, Konstantinos. "Businesses Consider Cybersecurity as an Afterthought despite Growth in Attacks, EY Survey Finds." *EY*, EY, 18 Feb. 2020, https://www.ey.com/en_gl/news/2020/02/businesses-consider-cybersecurity-as-an-afterthought-despite-growth-in-attacks-ey-survey-finds.

- Mesmer-Magnus, J.R., Viswesvaran, C. Whistleblowing in Organizations: An Examination of Correlates of Whistleblowing Intentions, Actions, and Retaliation. *J Bus Ethics* 62, 277–297 (2005). https://doi.org/10.1007/s10551-005-0849-1

- Near, J.P., & Miceli, M.P. (1985). Organizational dissidence: The case of whistleblowing. Journal of Business Ethics, 4, 1-16

- Office, U.S. Government Accountability. "Solarwinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)." *U.S. GAO*, 29 Sept. 2022, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

- O'Sullivan, Donie, et al. "Ex-Twitter Exec Blows the Whistle, Alleging Reckless and Negligent Cybersecurity Policies | CNN Business." *CNN*, Cable News Network, 23 Aug. 2022, https://www.cnn.com/2022/08/23/tech/twitter-whistleblower-peiter-zatko-security/index.html.

- Pacella, Jennifer M. "The Cybersecurity Threat: Compliance and the Role of Whistleblowers." Brooklyn Journal of Corporate, Financial & Commercial Law, vol. 11, no. 1, Fall 2016, pp. 39-70. HeinOnline.

- Press, Associated. “Anthem: Hacked Database Included 78.8 Million People.” *The Wall Street Journal*, Dow Jones & Company, 25 Feb. 2015, https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.
- Semnani-Azad, Z., Sycara, K.P., & Lewis, M. (2012). Dynamics of helping behavior and cooperation across culture. Proceedings of Collaboration Technologies and Systems 2012, 525-530
- Shaik Md Noor Alam, Hazlina. “Down the Cyber Rabbit Hole: Whistleblowing as a Means to Fulfilling Moral Obligations in Cyber Space.” *Jurnal Undang-Undang Dan Masyarakat*, vol. 2020, no. 27, 2020, pp. 20–24., https://doi.org/10.17576/juum-2020-27-02.
- Swann, W. B. Jr., Gómez, A., Dovidio, J. F., Hart, S. & Jetten, J. (2010b). Dying and killing for one’s group: Identity fusion moderates responses to intergroup versions of the trolley problem. Psychological Science, 21, 1176–1183
- Swann, W.B., Jr., Gómez, A., Huici, C., Morales, F., & Hixon, J. G. (2010a). Identity fusion and self-sacrifice: Arousal as catalyst of pro-group fighting, dying and helping behavior. Journal of Personality and Social Psychology, 99, 824–841.
- Swann, W. B. Jr., Gómez, A., Seyle, C. D., Morales, J. F. & Huici, C. (2009). Identity fusion: The interplay of personal and social identities in extreme group behavior. Journal of Personality and Social Psychology, 96, 995–1011
- Swann, W. B., Jr., Jetten, J., Gómez, Á. Whitehouse, H., & Bastian, B. (2012). When group membership gets personal: A theory of identity fusion. Psychological Review, 119, 441-456
- TEDtalksDirector. (2018, November 2). *How whistle-blowers shape history | kelly richmond pope*. YouTube. Retrieved September 20, 2022, from https://www.youtube.com/watch?v=51k3UASQE5E
- “The Remarkable Story of Cheryl Eckard and the $96 Million Bounty under the False Claims Act.” *Whistleblowers*, 2012, pp. 27–43., https://doi.org/10.1002/9781118386545.ch2.
- “Whistleblower Laws around the World.” National Whistleblower Center, 19 Apr. 2021, https://www.whistleblowers.org/whistleblower-laws-around-the-world/.
- “Whistleblower Rights and Protections.” *Front Page*, https://oig.justice.gov/hotline/whistleblower-protection#:~:text=Disclosing%20Classified%20Information,and%20transmission%20of%20classified%20information.

- "Whistleblowing and the Public Interest Disclosure Act 1998 (C.23) (Accessible Version)." *GOV.UK*, https://www.gov.uk/government/publications/whistleblowing-and-the-public-interest-disclosure-act-1998-c23/whistleblowing-and-the-public-interest-disclosure-act-1998-c23-accessible-version#document-details.