Leszakal (details modified for privacy)

Professor Name

Course: Computers & Society

4 April 2022

Little Birds with Big Mouths: The Power of Open Source Intelligence

Many of us compartmentalize our online lives. We have different personas for different places. An “alpha male” on Facebook posing with his favorite Glock secretly posts pictures of his crocheted animals to Reddit. Meanwhile, the straitlaced accountant down the street runs a risqué adult account on Twitter. Using different usernames across social media and hiding our faces gives a feeling of true privacy — true freedom to be who we want to be. Unfortunately, you are not safe, and it’s all because of some pesky crumbs and some very loud, little birds. Soon the crocheted cat is out of the bag and your neighborhood gossips are going on about how Bob down the street is into some very interesting things. You might wonder how all this could have happened. How the anonymity, which so many of us assume we have, was shattered. Enter the stage, Open Source Intelligence (OSINT).

OSINT has been around longer than one might initially think. The practice saw use during World War II, in which readily available information would be collected, links would be drawn, and the results would be transcribed into transparent reports (Glassman and Min). While the digital landscape that surrounds us today was not a reality back then, OSINT still retains the same core ideas. Michael Bazzell, a former federal officer and expert in computer crimes, describes OSINT as “any intelligence produced from publicly available information that is

collected, exploited, and disseminated" ("Introduction", para. 3). With the prevalence of social media and readily available cameras in the pockets of the masses, there is certainly a lot of publicly available information these days.

From the President of the United States to your neighbor's grandmother, nearly everyone is constantly online — and that's a problem. The internet can indeed be an outlet of freedom for many people. However, it is also one of the easiest ways to conduct surveillance. It's cheap, readily accessible, and minimizes the risk of being caught in the act. People often expose tidbits of personally identifiable information in their online posts, the crumbs, if you will. By their lonesome, these small pieces don't cause much harm. When pieced together, however, they can form a surprisingly cohesive image. Unfortunately, those who are concerned about privacy also have the crumbs of the crumbs to worry about. Metadata, or data about data, can be revealing as well (Hagnady, 54). For instance, research has suggested that Snapchat's Snap Map, which displays user activity on a publicly accessible map using posts' geolocation metadata, has the potential to be used in law enforcement surveillance (Matthews, et al.). There are also concerns about the culture such monitoring would bring, with some privacy advocates warning of an internet rife with self-censorship (Trottier).

The privacy-erasing power of OSINT is one of the most powerful things about it. It has the potential to put a lot of eyes on an individual. Everyone has something they want to keep to themselves, even the most shameless of people. The wonderful thing about social media is that we can express ourselves in a way that in-person communication might not allow. However, losing all privacy would limit this self-expression. As Glenn Greenwald asserts during a TED Talk on privacy, "when we're in a state where we can be monitored, where we can be watched,

our behavior changes dramatically." Shame is a powerful motivator that encourages conformity and compliance (Greenwald). To continue enjoying the freedom that the internet gives, privacy and anonymity must be protected. Of course, OSINT isn't an inherently evil thing that is only used to strip away your privacy.

The other edge of the OSINT sword is one used to promote safety and knowledge. Law enforcement can use OSINT techniques to identify possible terrorists, stopping them from carrying out devastating attacks (Trottier). Then there are the many instances of criminals being caught after posting to social media. Meanwhile, internet denizens have used OSINT to help clear the fog of war surrounding the Ukraine-Russia situation (Perrigo). This collaborative OSINT effort has been helpful in debunking fake media, finding holes in Kremlin rhetoric, and verifying the authenticity of videos coming out of the conflict (Perrigo). In these cases, OSINT is not being used maliciously. Those involved with the Ukraine efforts are even reported to have developed a kind of informal ethical framework, avoiding the posting of possibly distasteful material (Perrigo). Penetration testers and other cybersecurity professionals routinely make use of OSINT to locate issues and harden systems against attacks (Bazzell). The impact of OSINT truly depends on the one who wields it. Unfortunately, not everyone has such noble aspirations.

Cybersecurity Ventures estimated that cybercrime would cause $6,000,000 (six-million) in damages by 2021 ("Cybercrime"). The damages from OSINT specifically would be understandably difficult to quantify. However, there are ample, qualitative examples of the potential harm it can cause. Step away from military, or law enforcement incidents for a moment, as those are often muddled with other techniques. Instead, focus your gaze on the numerous debacles caused by people simply digging up publicly available information. Debacles that have

ended up with people being publicly embarrassed, shamed, or even losing their jobs. In many of these incidents, the person in question has been doxed. For those unfamiliar with the term, doxing occurs when details about someone's personal life are used to attack or humiliate them (Hadnagy, 35). The attack often includes the victim's name and address, as well. Controversial figures tend to be at particularly high risk of falling victim to a dox. Kiwi Farms is a web forum infamous for doxing people who they find amusingly disagreeable. Its members use OSINT to gather this information, scanning the target or the target's social circle for usernames, posts, and photos to find any embarrassing information, alternate accounts, or addresses.

To demonstrate how easy it can be to find embarrassing information using OSINT techniques, I'll recount an experience I had with a Twitter account I follow. For privacy reasons, the user will be referred to as User X. Looking through the Twitter biography and posts of User X, one can see that he is an artist and animator. He mentions his university, his love for birds, his current location, and provides a link to his personal site. There are videos of him rock-climbing and reacting to certain events. Seeing his face, User X is almost certainly East Asian. The current username looks like a Chinese name using Taiwanese style romanization. A look at his professional page confirms it as his name but makes no mention of nationality. This account is clearly used to help showcase his artistic skills, which is important in that industry. Overall, User X has certainly given away a lot of information on this public profile, but there isn't anything that might raise eyebrows. That is until you happen to glance through the list of users he follows.

Near the top of that list, there is an adult art profile that stands out, both because it is clearly for explicit drawings and because User X is linked as the non-explicit account. In the Twitter biography for this adult art account, there is a Taiwanese flag, a partial name that

matches that of User X, an age, the user's relationship status, and a link to yet another account. While there is a variety of pornographic drawings, one character is reoccurring. This character happens to look a lot like an anthropomorphic bird that is displayed on the personal site of User X and looks extremely similar in art style. Either these are the greatest coincidences in the world, or this adult art account also belongs to User X. Considering these explicit drawings are associated with an oft-ridiculed subculture, this account certainly has the potential to be very embarrassing.

Following the other link on this profile redirects to another adult account, this time depicting solo pornographic acts by the user. The Twitter biography describes itself as the "after dark" account of the explicit drawing account. I silently wonder if he wants this to be tied to his public identity, but the videos show an effort to hide his face. I also search the internet for the usernames he has used on Twitter. This reveals a profile on an art site that explicitly confirms that he is from Taiwan and lists his sexuality. From just a few minutes of scanning his public profiles, I was able to learn his name, his appearance, his hobbies, the university he attended, his profession, his nationality, his age, the languages he speaks, what he sounds like, the city he lives in, his sexual orientation, his relationship status, his sexual fetishes, and even what he looks like nude. Had I the patience, I may have even been able to identify his approximate location based on the rock-climbing gym shown in his videos. If I was a malicious actor, I could easily move to dox him.

It is unsurprising that the ordinary person might get lost in the constant stream of notifications and mindless Tweets, but not even high-level officials are immune to leaving a trail of crumbs. In 2017, one internet researcher set out to identify the social media accounts

belonging to former Director of the Federal Bureau of Investigations (FBI) James Comey (Hadnagy, 18). The researcher began by listening to press statements and appearances given by Comey, in which he mentioned having Twitter and Instagram accounts (Hadnagy, 18). Having trouble finding Comey directly on these sites, she sent a request to follow Comey's son on Instagram, who was much easier to find (Hadnagy, 20). Upon requesting a follow, Instagram suggests others who are in the same social circle as the person you desire to follow, thus pointing the researcher to possible accounts (Hadnagy, 20). From there, she noticed an account named "reinholdniebuhr," which a Google search showed to be a deceased theologian who had died long before Instagram was born (Hadnagy, 20). Further investigation revealed that Comey wrote about Reinhold Niebuhr in a college thesis (Hadnagy, 20). Finally, searching Twitter for this username showed one @ProjectExile7, which had a similar name to Project Exile, which was a program Comey was involved in (Hadnagy, 20). Like the more ordinary Twitter user covered before, this is either an extreme coincidence, or it is Comey's Twitter account. Obviously, there are huge security implications with a compromised social media account for someone like Comey. A Tweet about a vacation or something similar could give potential attackers sensitive information to act on. For some, leaving a trail of crumbs can be dangerous.

If you value your anonymity, your privacy, then you should keep in mind the power of OSINT. Chances are nobody will ever come looking for you. If they should, however, every single post you've made, every picture you've shared, and every account you have will be under the scrutiny of some very tenacious individuals. Social media allows us to share ourselves with the world, but that comes with risks. Remember that the internet is forever. Once a piece of information is there, it's fully possible that it shall never truly be erased. Remember that those

Tweets you made will never truly go silent. Remember that it is easier to bring a plate, rather than to try picking up every tiny crumb you had let fall.

Bibliography

Bazzell, Michael. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.* 9th edition, Self-published. 2022

Bradbury, Danny. "In Plain View: Open Source Intelligence." *Computer Fraud & Security*, vol. 2011, no. 4, Elsevier B.V, 2011, pp. 5–9. *ScienceDirect*, https://doi.org/10.1016/S1361-3723(11)70039-2.

"Cybercrime Damages $6 Trillion by 2021." Cybercrime Magazine, Cybersecurity Ventures, 9 Nov. 2020, www.cybersecurityventures.com/annual-cybercrime-report-2017/.

Feinburg, Ashley. "This is Almost Certainly James Comey's Twitter Account." *Gizmodo*, Gizmodo, 30 Mar. 2017. www.gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641.

Glassman, Michael, and Min Ju Kang. "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)." *Computers in Human Behavior*, vol. 28, no. 2, Elsevier Ltd, 2012, pp. 673–82. *ScienceDirect*, https://doi.org/10.1016/j.chb.2011.11.014.

Greenwald, Glenn. "Glenn Greenwald: Why Privacy Matters". *YouTube*, uploaded by TED, 10 Oct. 2014, www.youtube.com/watch?v=pcSlowAhvUk.

Hadnagy, Christopher. *Social Engineering: The Science of Human Hacking*. John Wiley & Sons, Inc., 2018.

Matthews, Richard, et al. "Ghost Protocol – Snapchat as a Method of Surveillance." *Forensic Science International: Digital Investigation*, vol. 36, Elsevier Ltd, 2021, p. 301112–. *ScienceDirect*, https://doi.org/10.1016/j.fsidi.2021.301112.

Perrigo, Billy. “How Open Source Intelligence Verified Ukraine Attack Videos.” *Time*, Time, 24 Feb. 2022, www.time.com/6150884/ukraine-russia-attack-open-source-intelligence/.

Trottier, Daniel. “Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques.” *European Journal of Cultural Studies*, vol. 18, no. 4-5, SAGE Publications, 2015, pp. 530–47. *SAGE Journals*, https://doi.org/10.1177/1367549415577396.