Social Media and Intelligence Gathering

Joshua I James[1]

Online social media has changed the way many people, businesses and even governments interact with each other. Because of Twitter's popularity and its ability to broadcast small pieces of information to a large number of people, it is an effective form of mass communication. However, ease in communication that allows the public to freely communicate anything they wish can be used for both benefit and harm in a number of ways.

For example, in 2011 panic ensued as parents in Veracruz, Mexico rushed to pick up their children from school amongst reports of gang-related kidnapping and shootings [1]. During this time, it was reported that panic led to an increased number of car accidents and denial of service on emergency response numbers [2]. The panic, however, was based on (plausible) claims from two people who posted about the false gang-related activity on Twitter, which later went 'viral'.

In 2012 a teen gained worldwide notoriety by asking her followers on Twitter to call the police, claiming someone broke into her home [3]. Her case was later determined to be a runaway attempt, but was not discovered before reaching the number 2 most popular worldwide topic on Twitter for that time-period [4].

And in the 2008 terrorist attacks in Mumbai, India, claims emerged that the terrorists were monitoring social media outlets to extract operational intelligence to avoid police and potentially locate more victims [5][6].

These, and other similar cases, are not necessarily new. Abuse of emergency response numbers for non-emergencies are relatively common [7][8], and are even sometimes used as a way to attempt to distract police [9][10]. But just like emergency response numbers, social media can also be used to help in many situations.

For example, many law enforcement agencies, and even some communities themselves, have been creating and advocating the use of social networks to create a 'virtual neighborhood watch' that can consist of crime alerts from law enforcement and the public alike [11][12][13].

Even though social media was potentially used by the 2008 Mumbai terrorists, it was also used during the attacks by the public to report the news before traditional media outlets, warn of dangerous locations, communicate to loved ones, and even help organize support services such as blood donation [14][15]. This type of public emergency coordination was again demonstrated during the 2011 Mumbai bombings, where social media was used to track the bombings as well as organize support services for victims [16].

---

1 James JI. (2012) "Social Media and Intelligence Gathering". Virtual Forum Against Cybercrime. Issue 16. Korean Institute of Criminology.

The negative aspects of online social media have prompted some countries to consider shutting down communication infrastructure services when they can be used against the public or state [17][18], with one extreme example being the 2011 Egyptian Internet outage during riots against the government in an attempt by the government to suppress information and disrupt public coordination [19]. However, some experts believe that the benefits of social media far outweigh any potential abuse. For example, Schneier [20] claims that "[t]errorist attacks are very rare, and it is almost always a bad trade-off to deny society the benefits of a communications technology just because the bad guys might use it too".

How social media will continue to shape the public, governments and even crime remains to be seen. However, from a law enforcement perspective, the ability to communicate with and inform a large number of citizens at a time can be invaluable during a crisis. Further, intelligence about crime and criminals can often be gained via online social media sites such as Twitter. Again, gained intelligence can be used for positive or negative purposes depending on the perspective, but nevertheless, many users and criminals are constantly producing a stream of publically accessible data that may help investigations.

While the content of postings should normally be considered hearsay and treated with caution, analysis of the produced meta-data may provide some potentially relevant information for investigations. Several related online social networking security awareness campaigns have been created to raise awareness for the amount of personal information people are – normally unwittingly – posting.

One such site, "ICanStalkU.com" (I can stalk you), pulled Geo-Tagging information from the meta-data of pictures posted on TwitPic.com. This Geo-Tagging information was then used to plot the user's current location in real-time, and could potentially be used to track the current location and movements of a suspect, or help to place them at or near a location at the time of an incident. A more advanced, stand-alone program called "Creepy" [21] also uses the same Geo-Tagging information from many more social media outlets.

Another similar site that claims to raise awareness about over-sharing, is "PleaseRobMe.com", which uses Twitter, Foursuare or Gowalla check-ins with associated times to attempt to report if the user is home or not. Similar location-tagging features now exist on many social media sites, and could potentially be used to gain intelligence about a particular user.

While location information may be relevant, perhaps an investigator needs to plan when an operation should take place. For this, the site "SleepingTime.org" may provide an analyst with the best time to find the user at home or away. SleepingTime.org uses a user's Twitter account activity and time zone to estimate when the user is most likely to be asleep based on the time they normally do not have any twitter activity.

And finally, online social media is about social networks. Paterva's Maltego [22] is a more advanced web mining application that can work with social network data, among others, to generate communication networks and conduct entity link analysis.

These are just some of the tools and potential intelligence that can be extracted from public sources for many users. Even without specific tools, publically available information about a particular user can oftentimes be mined with very little skill or time investment.

Because of social networking sites such as Twitter, a large amount of potentially valuable information can be provided to – and found about – the public, businesses, Law Enforcement, governments, and even criminals. Communication technologies can benefit the world; however, the same communication channels could also be abused. With the large amount of data being generated at present, and ability to easily communicate with a large population in near real-time, Law Enforcement should embrace social media outlets to more effectively share information, and also to receive intelligence that can help in the protection and prevention of crime.

Bibliography

1. Miglierini, Julian. (2011) "Mexico Twitter terrorism chargers cause uproar." BBC News. http://www.bbc.co.uk/news/world-latin-america-14800200.
2. (2011) "2 Mexicans face 30 years in prison for tweets that caused panic in violence-wracked city." NY Daily News. http://articles.nydailynews.com/2011-09-04/news/30136979_1_tweet-panic-private-schools.
3. Murphy, Samantha. (2012) "Police: Teenage Girl's Viral Tweet Was Kidnapping Hoax." http://mashable.com/2012/10/01/teenage-girl-tweet-kidnapping/.
4. http://www.twee.co/topics/helpfindkara
5. (2008) "Terrorists turn technology into weapon of war in Mumbai." http://www.couriermail.com.au/news/world-old/terrorists-and-technology/story-e6freop6-1111118178210.
6. Oh, Onook, Manish Agrawal, H. Raghav Rao. (2011) "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter". Information Systems Frontiers. Vol. 13. Issue 1. P. 33-43. Springer.
7. Nichols, Mike. (2008) "False 911 calls are alarmingly common." Journal Sentinel Inc. http://www.jsonline.com/news/29432374.html.
8. Esposito, Richard, Christina Ng. (2012) "Police: Angry Ex-Girlfriend Triggered US Airways Bomb Hoax." ABC News. http://abcnews.go.com/US/police-angry-girlfriend-triggered-us-airways-bomb-hoax/story?id=17170280#.UHu9A2lrZ3J.
9. FitzPatrick, Lauren. (2011) "Man pleads guild to making fake 911 call to try to help buddy." Sun-Times Media, LLC. http://www.suntimes.com/news/6734423-418/man-pleads-guilty-to-making-fake-911-call-to-try-to-help-buddy.html.
10. (2012) "Smugglers Use Fake 911 Calls to Distract Police." http://www.krgv.com/news/smugglers-use-fake-911-calls-to-distract-police/.
11. Catone, Josh. (2009) "Virtual Neighborhood Watch: How Social Media is Making Cities Safer." http://mashable.com/2009/10/01/social-media-public-safety/.
12. Johnson, Kirk. (2012) "Hey, @SeattlePD: What's the Latest?." New York Times. http://www.nytimes.com/2012/10/02/us/seattle-police-department-uses-twitter-to-report-crime.html.

13. Barr, Meghan. (2009) “Neighbors Twitter, blog to keep criminals at bay.” NBC News. http://www.msnbc.msn.com/id/32372082/ns/technology_and_science-security/t/neighbors-twitter-blog-keep-criminals-bay/#.UHt5kGlrZ3J.
14. Beaumont, Claudine. (2008) “Mumbai attacks: Twitter and Flickr used to break news.” Telegraph Media Group Limited. http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.
15. Stelter, Brian, Noam Cohen. (2008) “Citizen Journalists Provided Glimpses of Mumbai Attacks.” New York Times. http://www.nytimes.com/2008/11/30/world/asia/30twitter.html.
16. Ribeiro, John. (2011) “Mumbai Uses Internet, Twitter to Cope with Terror Blasts.” IDG Consumer & SMB. http://www.pcworld.com/article/235672/article.html.
17. (2011) “British Government Considering Social Media Ban. Was China Right?” http://technode.com/2011/08/15/british-government-considering-social-media-ban-was-china-right/.
18. Phillip, Joji Thomas, Soma Banerjee. (2012) “Government for state-specific ban on social media, asks ISPs to build embedded technology.” Bennett, Coleman & Co. Ltd. http://articles.economictimes.indiatimes.com/2012-09-08/news/33696582_1_home-ministry-websites-social-media.
19. Bates, Theunis. (2011) “Protesters Left in the Dark as Egypt Blocks Internet.” http://www.aolnews.com/2011/01/28/protesters-left-in-the-dark-as-egypt-blocks-internet-cell-phone/
20. Schneier, Bruce. (2009) “Helping the Terrorists.” http://www.schneier.com/blog/archives/2009/01/helping_the_ter.html
21. http://ilektrojohn.github.com/creepy/
22. http://paterva.com/web6/