Issues in Information Systems
Volume 23, Issue 1, pp. 204-213, 2022

DOI: https://doi.org/10.48009/1_iis_2022_116

The impact of social media geolocation on national security and law enforcement

Frank X. Hartle, *Robert Morris University, hartle@rmu.edu*
Megan Garfinkel, *Robert Morris University*, *garfinkel@rmu.edu*
David O'Neil, *Robert Morris University, deost163@mail.rmu.edu*
Gaetano Scalise, *Robert Morris University, gxsst229@mail.rmu.edu*
Nicholas Sauer, *Robert Morris University, nasst285@mail.rmu.edu*
Christopher Willard, *Robert Morris University, cmwst3@mail.rmu.edu*

Abstract

Evaluating the simple dating applications Hinge and messaging app Telegram, we demonstrate that information gleaned from either the person posting or via the application, it is possible to geolocate individuals in near real time. When this is applied by either adversaries or law enforcement, it is possible to track down individuals or learn of strategic and tactical activity and do so in near real time.

Keywords: social media applications, national security, military, law enforcement

Introduction

Today, social media is a key component of many people's daily lives. Whether it is to keep up with old college or military friends, to stay in touch with extended family who live great distances, or to communicate with friends and family daily, social media has become a means of communication in the 21st century. In fact, one could argue it has all but replaced traditional letters and, in some demographics, even email. Social Media's rise as a day-to-day facet started in the late 1990's and most commonplace social media sites were well established by 2010, with Facebook and Twitter trading as a public IPO in 2012 and 2013 respectively (Jones, M. et al., 2021).

Studies have been conducted to demonstrate that social media can be used to counter national security threats. Mugari and Chisuvi (2021) noted how in Zimbabwe, a study of 274 respondents from both public and security arms of the state indicated that the overwhelming majority of respondents felt social media enabled better communications between the government and its citizens. In addition, they showed that government monitoring of social media played a key role in countering threats as well (Mugari & Chisuvi, 2021). In this example, social media could be construed as a positive, however, the over usage and almost addictive dependence upon social media has created an entire generation wherein all aspects of life are beginning to center on social media applications. Furthermore, it has been argued that while there exists benefits to social media, the risks of adolescent development can include "profound social and psychological consequences such as depression, anxiety, isolation, and tragic suicide" (Elsayed, 2021, p. 3). Even more concerning is the risk daily usage from an early age can cause with respect to indifference towards privacy. As such, this phenomenon has not escaped even those in sensitive positions. While one

could argue the merits from a law enforcement perspective, if users are not careful, they run the risk of not only compromising themselves but national security.

The Law Enforcement Community (LE) in the United States and abroad have been using open source intelligence techniques as an investigative resource for decades (Delavallade, T., Bertrand, P., & Thouvenot, V., 2017). Investigators have used information gleaned from public Facebook pages all the way to utilizing legal services to actively track a person's Facebook page in an effort to solve crime and convict criminals and dismantle the organizations they work within. Most of the techniques utilized by law enforcement are simple, open to the public, and effective in the location of and gleaning the activity of targeted individuals (Delavallade et al., 2017). Similarly, those same techniques can be employed by adversaries with malicious intent.

The following illustrates how social media, more specifically dating and messaging applications, can be exploited. This concept is measured through the implementation of geolocation in law enforcement as well as how easy the authors were able to identify military personnel through the use of a common dating and messaging applications. Under the same circumstances, we were able to identify everyday users of various dating applications. By learning information about the individual through normal social media presence, one can now effectively pinpoint physical locations and thus, depending on their role, identify military activity. For example, if an individual is stationed in San Diego but begins advertising, they will be in Japan in four weeks, and one can easily deduce that the ship will be departing and heading towards Japan. Likewise, depending on the dates, it may be possible to ascertain course and speed. From a national security perspective, this could be problematic, especially should there exist the possibility of hostilities. Depending on an adversary's intent, this type of information could be detrimental to national security.

Likewise, through the use of said technology, the intent could be nobler such as law enforcement attempting to identify the location of individuals wanted for crimes. As such, this same principle of leveraging applications for geolocation will be shown through the discussion of several real case studies. Finally, because the study was able to identify real individuals, the names and some locations have been changed to protect their privacy.

Social media applications dominate the social landscape of human interaction. It has been argued that while there exists benefits to social media interaction, there also exists significant threats to human development and possibly national security. As humans become more dependent upon social media for interaction, one could argue that it creates an almost indifference or insensitivity to what one is communicating via their social media presence. Therefore, with a generation having been raised on social media now assuming roles of national security, does this indifference create a national security threat? Likewise, does it create a complacency among criminals? Evaluating the simple dating applications Hinge and messaging app Telegram, we demonstrate that information gleaned from either the person posting or via the application, it is possible to geolocate individuals in near real time. As such, if this is applied by either adversaries or law enforcement, it is possible to track down individuals or learn of strategic and tactical activity and do so in near real time.

Law Enforcement Utilization

As social media maintains a presence today (2022), it has become a necessary tool for Law Enforcement (LE) agencies to utilize for historical information or real time information for investigations ranging from narcotics trafficking to fugitive apprehension (Trottier, 2015). Social media sites contain a large amount of open-source intelligence (OSINT) which is information that appears public and unrestricted in print or electronic form and is easily obtained by law enforcement without a search warrant or court order (Trottier,

2015). Social Media OSINT is used in all aspects of police operations, community engagement, crime prevention, and criminal investigation (Rice & Parkin, 2016).

LE also utilizes social media information in the prevention of crime, searching for preparatory actions that can indicate that a crime or protest is being planned or taking place can help LE get the necessary resources in place for quick response or mobilization or specialized units (Rice & Parkin, 2016). LE can monitor social media in real-time in attempts to track communications and location information, this is especially helpful in civil unrest and violent offender standoff situations, monitoring real time allows LE to provide a safe environment for all affected (Rice & Parkin, 2016). Furthermore, historical information gleaned from social media can be a power tool utilized to collaborate or contradict testimony during trial proceedings (Rice & Parkin, 2016).

OSINT collected from social media sources can be used as evidence to support probable cause for a search warrant, arrest warrant, identifying or locating actors, or understanding how a criminal organization is structured (Rice & Parkin, 2016). Social media applications with the ability for two-way communication and location based services (LBS), can be an excellent starting point for investigative leads (J. Novakowski personal communication January 7, 2022). Location-based services (LBS) are services that utilize the location data of smartphones to control features like maps, navigation services, and nearby information searches (Jang & Lee, 2018). LBS utilizes global positioning system (GPS) technologies which enable location services on smartphones when users have the LBS turned on, 74% of users have LBS enabled on their smartphones (Jang & Lee, 2018). Geosocial services can tell you where your friends are meeting, where you can hook up with a date, or LE can utilize it to track your movements all because of LBS (Jang & Lee, 2018). Detective Joseph Novalowski who is a 29 year veteran of Pittsburgh Bureau of Police (Pennsylvania) and currently assigned to West Pennsylvania United States Marshal Service Fugitive Task Force stated, “Real time LBS information coupled with historical social media information such as residences, next of kin, street names (nicknames), and friends, can be an effective way to track down suspects wanted for felony crimes” (J. Novakowski personal communication January 7, 2022).

While LE has the ability to gain information which is private or restricted from public view through the utilization of legal services and nonpublic databases such as the National Crime information Center (NCIC), websites such as Lexisnexis, a subscribable public record database, can give users such information as job history, address history, and even identify neighbors and relatives of suspects (About Us | LexisNexis, 2022). Lexisnexis and other such websites are available for subscription for the use by the public, which means that criminals and nation state adversaries alike can utilize these sources (About Us | LexisNexis, 2022). Conversely social media has become a way to hold police accountable in questionable use of force incidents, justified or otherwise (Fallik et al., 2020). In the case of Michael Brown, communication flourished on social media sites in demands for justice (Fallik et al., 2020). Sites like Facebook, Twitter, and Instagram helped to organize and call for civil protests across the United and in some cases internationally in response to perceived police brutality and state sanctioned murder (Fallik et al., 2020).

General Methodology

This illustrative case study describes specific approaches, using one primary dating application and one messaging application, wherein current locations of military personnel were able to be discerned with a high degree of confidence. To begin, researchers used Hinge, which is an online dating application, to find multiple individuals in multiple different settings. Specifically, research was conducted on the Hinge dating application for the purpose of assessing the security risk dating apps pose to military personnel. This application was chosen out of other dating apps because of its ability to allow the user to switch dating

locations without requiring the user to physically move the actual location of the device. Later, we illustrate how Telegram is being utilized to identify and target military personnel in Ukraine.

Starting with a military focus, researchers were able to find a few individuals on Hinge with basic filters that did not indicate anything specific about the individuals. For example, they used interests being set to prefer women, no religious preference, no smoking, no alcohol, etc. Found in Figure 1 below, a wide variety of filters not only allowed for reconnaissance outside of the dating app, but also allowed for continually finding a target individual amongst 100s of possible users.

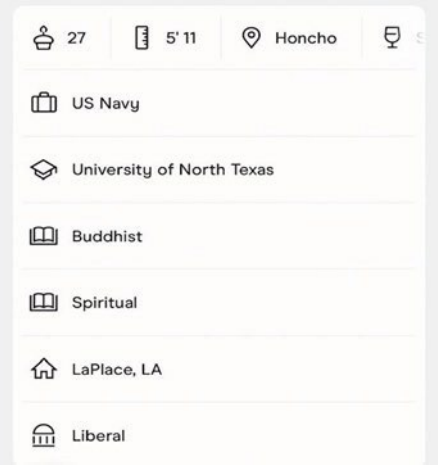

Figure 1: High utility filters on Hinge

Using these filters researchers then placed themselves, via the Hinge application settings, on the island of Okinawa, Japan. Seeing as there is a large United States military presence there, it would be a prime place to set up an online persona in order to identify a few people who might have put too much information on their profile through pictures or simply via their preferences. With this in consideration, filters were used to search out military age individuals within a 30-mile radius of Higashi, Okinawa. The military installations within the target radius were Camp Gonsalves, Camp Schwab, Camp Hansen, Camp McTureous, and Camp Kinser. With all of this information, researchers started reviewing profiles and looking through potentially at-risk accounts that give away too much information.

Potential Security Concerns with Application Usage

The following identifies three initial potential concerns of the dating application Hinge, which were reviewed, and their significance to the studies involving military personnel. The first, location tracking, was reviewed by itself and determined by the research team to pose a moderate risk to a service member. The location listed on the profile changed based on manually updating the location. While testing the research profile that was set up, it was observed that automatic updates based on a phone's location takes roughly 24 hours and is not instantaneous. Adversaries or malicious actors would need to use additional information to precisely geolocate a service member's recent location and would most likely resort to alternative tracking methods.

The second potential concern is that highly detailed information can be gathered on a service member through hidden details in profile pictures. Stephanie (name changed for privacy purposes) posted a picture with a hat indicating which specific vessel she is deployed on (Figure 2). With this information however, the research team was still unable to find additional personal details about her. On an additional profile,

Julia (name changed for privacy purposes) had uploaded a photo where her social media username was tagged. Through this tag, profile information and personal information about Stephanie including last name, Facebook Profile, Instagram profile, and LinkedIn Profile was discovered. With knowledge of her full name, the team was able to discover nearly all of her active social media profiles. Upon reviewing these profiles, her hometown, hometown high school, university, ships stationed in both past and present, and current and past jobs in the U.S Navy were all discovered.

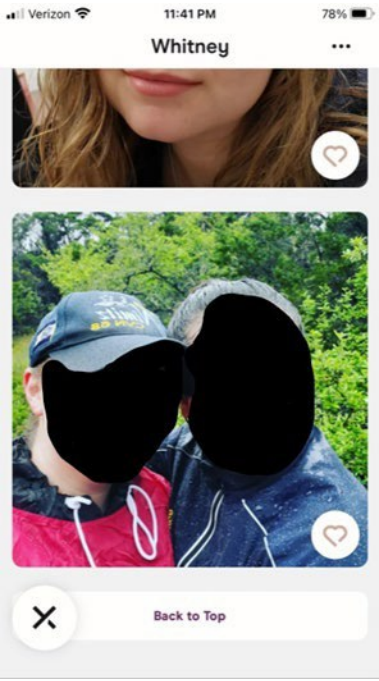

Figure 2: Identification of Navy personnel

With this in consideration, the researchers assessed that profile pictures and the potential details hidden within them may pose a severe risk to military personnel. Enemy psychological operations could potentially utilize this during and/or leading up to conflict in an attempt to demoralize service members. In a similar vein, this kind of information is routinely used for creating customized phishing emails targeting individuals. With this data about military personnel, possible tactics could include targeted messages to family members and friends found via the service member's Facebook page and/or targeted messages to the service member's social media itself.

The third potential concern reviewed was the filter information provided for each profile. For the purpose of this study, free accounts were utilized, and as such filter results were limited. The filter results available consisted of age range, maximum distance, ethnicity, religion, gender, education, and occupation. Among these filters, maximum distance, occupation, and education can give a perpetrator a way to search for a profile's user outside of the platform. As an example, obtaining a profile's personal information allows an adversary or malicious actor to search for that person via Facebook and LinkedIn. With regard to the other four filters, age range, ethnicity, religion, and gender, the research team only found them to be useful when attempting to relocate a profile after it has already been passed in the reject and accept function of the application. After reviewing roughly ten profiles with personal information listed, no connections were found on Facebook or LinkedIn. Considering this, the researchers had determined that the filter information

may pose a low to moderate risk to military personnel security. However, these bits of demographic data can be utilized to confirm information gleaned from other social media platforms.

National Security Related Findings

The following section provides several examples of how, employing the above methodology, researchers were able to locate various individuals with what may be construed as those holding sensitive positions. In order to preserve the privacy of individuals, the names have been altered and pictures have been edited.

Illustrative Case Study: Okinawa

Through the Hinge online dating application, 36 dating profiles of both men and women, who had listed being a member of the United States military, were located within a 44-mile radius of Kusugauracho, Japan. This specific location was picked because of its proximity to Yokosuka Harbor, the home port of the U.S Navy's Seventh Fleet. Out of the 36 profiles found, 21 had the individual's university listed and, of the same profiles, 17 had their specific military roles listed. It is important to note that all profiles are required to have their height and age listed. For example, one was "Johanna". She stated she was with the United States military and had a picture of her and presumably friends at a bar (Figure 3).

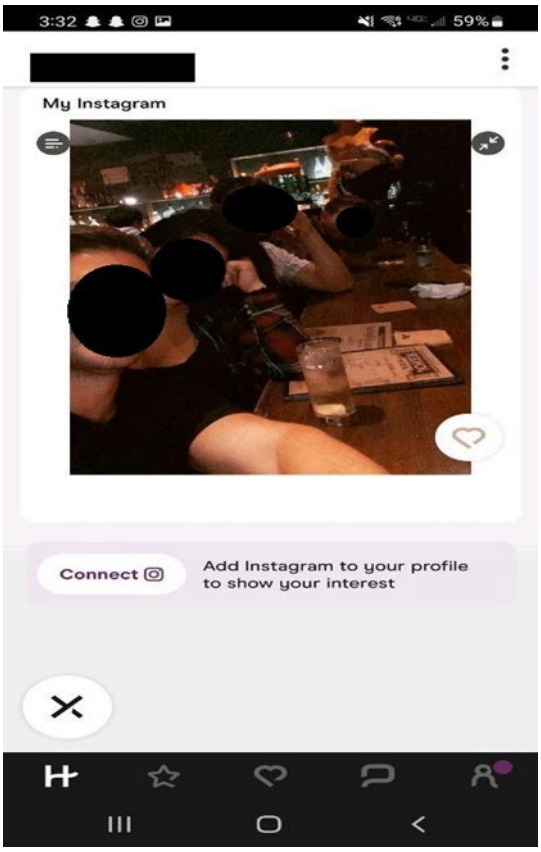

Figure 3: Identification of military personnel in Japan

At the top of the menu was the name "JOKER.". Research was conducted to identify where this bar was located and as such, it was determined to be in the middle of the island of Okinawa, Japan. This indicates that they have been there, recently, and would likely be a prime area to find this individual in person. Again,

from a security perspective, the information gleaned provides an adversary both talking points to engage the individual and better insight into their social behavior. Furthermore, if that is not their home station, one can assume either they were deployed for military activity or there on vacation. From an adversarial perspective, the next step would be to go to the bar, take similar pictures, and immediately try to 'connect' with the individual.

Illustrative Case Study: Local Area Matching

In a similar manner, the researchers moved into the realm of public accounts, but not specifically military. As such, the researchers then switched a few of the preferences on the account indicating that this persona now has a preference for men in a local area in Coraopolis, Pennsylvania. While doing this, the researchers were able to get the same preferences and match with one another, further demonstrating the power of switching preferences. Provided one knows what a particular person likes, roughly where they live, and/or if they have a Hinge profile, it is very likely that an individual can track and find someone else and configure their preferences to ensure a match. This is shown by how the researchers were able to find each other solely based on location and preferences. Another key point, while some do not post specifically where they work for safety reasons, it is still possible to glean information based solely on photos and locations. In the case of one of the following individuals, they posted that they work at a Starbucks somewhere in the Sewickley area in Pennsylvania. There are only two Starbucks within this area, and they are both within a ten-minute drive of each other. Again, the significance is that now adversaries can utilize this information to either visit the location or attempt to alter preferences to ensure a match.

Illustrative Case Study: Military Application Telegram

The final illustrative case study focused solely on military application as researchers used Telegram to find and locate military associated accounts within Ukraine. Russian military units appear to have brought their phones into the conflict zones in Ukraine even though the Russian military strongly suggested phones not be brought into combat. With a heavy reliance on teenage conscripts however, it is clear mobile devices are still embedded within units. A myriad of TikTok and Telegram videos continually surfaced showing Russian military personnel utilizing social media.

This fact provided an opportunity to test theories related to the targeting of military personnel via personal technology. Specifically, Telegram was used for this test because it is a mobile app that is currently a popular medium for Ukrainian citizens and soldiers to share videos, pictures, and overall conflict updates. The app also has a built-in feature that uses the users location search nearby for other Telegram users. This function provided an exceptional opportunity for researchers to find military personnel accounts. Telegram does not permit the user to actively change location to search for nearby users. However, an application called Wondershare can be used to change a phone's virtual location to the GPS coordinate of choice. For the purposes of this research, the GPS coordinate of the researcher's iPhone was changed to 47.105726386614656, 37.540690898895264 in the city of Mariupol, Ukraine. This was conducted on 03/22/2022. Eight military profiles total were found utilizing this technique, with one profile confirmed to be Russian and two profiles confirmed to be Ukrainian. The other five found could not be identified (Figure 4).

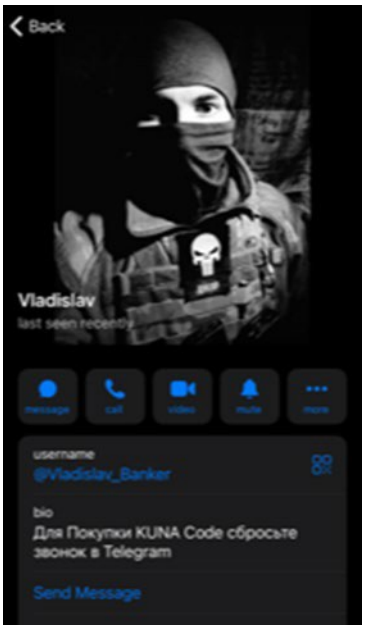

Figure 4: A soldier who goes by the name Vladislav is listed on Telegram. Found near Mariupol

These findings have military applications in the theater of war as profiles who are identified as belonging to a particular side can become victims of psychological warfare campaigns. More specifically, fake Telegram accounts can be utilized to repeatedly send anti-Ukrainian messaging with the purpose of demoralizing the individual and his/her unit. Another potential opportunity with Telegram is to utilize the 'find a group' feature to mobilize the defending communities against Russian invading forces. In an operation, the Telegram accounts of known Russian military operatives can be shared with local Telegram community groups, where instructions can then be given to repeatedly send demoralizing messages or videos to the account. Having dozens, or even a hundred of individuals send these messages provides a low probability that all accounts will be blocked by the target account.

Conclusion

Social Media has established itself as mainstream communication method. From its early use as a way to keep in touch with friends and family who are geographically separated (Facebook), it has now evolved into ways for people to find intimate relationships (Hinge, Tinder) and all the way to platforms for social influencing (Tik Tok, Instagram). Understanding how adversaries and criminals utilize social media in an adverse manner is the first step in securing personal social media accounts to mitigate the effects of those who would use it for nefarious purposes.

The authors discussed how an individual user of social media can be an effective tool for law enforcement to discover information about an individual's whereabouts. The authors also discussed how law enforcement used social media in real time data to make decisions concerning public safety and how historical information gleaned from social media can help to bolster evidence in court proceedings. The authors further discussed how location-based services are used in investigations to gain information concerning criminal suspects, victims or witness locations.

The authors demonstrated how seemingly harmless information or pictures posted on a dating application account coupled with other open-source information can lead to clues which could benefit an adversary in

an intelligence gathering role in an effort to destabilize national security. The information not only provides individual movement, but also specific unit movement and possibly unit activity, which equates to a breach in operational security for our national defense services.

Modern social media has a dualism that can affect the security of not only the individual users but could also harm organizations in which individuals are employed. The authors demonstrated using common social media applications, and with relative ease, that they were able to identify the locations of military individuals.

Future Research

While the authors were able to provide several illustrative case studies pertaining to various social media tools geolocation function, future research is warranted. Additional research will allow the concepts illustrated above to be expanded longitudinally. The research team can develop a better understanding of the long-term movements pertaining to unsecured military social media user accounts and the ability to glean useful tactical information from them.

Finally, the authors have shown how social media can be exploited using modern technology and open-source intelligence. The process outlined by the authors can be automated through the use of the application programming interface (API). Automating the process reduces the need for the authors to manually interact with social media applications, yet still returns the aforementioned results previously observed. These topics of future research serve as recommendations that will help to extend the authors' understanding of to what extent social media's geolocation functionality has an impact on public safety, national security, and law enforcement.

References

Delavallade, T., Bertrand, P., & Thouvenot, V. (2017). Extracting future crime indicators from social media. In using open data to detect organized crime threats (pp. 167-198). Springer, Cham.

Elsayed, W. (2021). The negative effects of social media on the social identity of adolescents from the perspective of social work. *Heliyon, 7*(2), e06327-e06327. https://doi.org/10.1016/j.heliyon.2021.e06327

Fallik, S. W., Deuchar, R., Crichlow, V. J., & Hodges, H. (2020). Policing through social media: A qualitative exploration. *International Journal of Police Science & Management, 22*(2), 208-218. https://doi.org/10.1177/1461355720911948

Jones, M., Contribution, G., & Hardy, J. (2021). The Complete History of Social media: A Timeline of the Invention of Online Networking. Retrieved 30 November 2021, from https://historycooperative.org/the-history-of-social-media/

Mugari, I., & Chisuvi, R. (2021). Social media and national security in Zimbabwe: Embracing social media for national security and addressing social media threats. *African Security Review, 30*(1), 86-101. https://doi.org/10.1080/10246029.2020.1857806

Trottier, D. (2015). Open-source intelligence, social media, and law enforcement: Visions, constraints, and critiques. *European Journal of Cultural Studies, 18*(4-5), 530-547. https://doi.org/10.1177/1367549415577396

Rowse, J., Bolt, C., & Gaya, S. (2020). Swipe right: The emergence of dating-app facilitated sexual assault. A descriptive retrospective audit of forensic examination caseload in an australian metropolitan service. *Forensic Science, Medicine, and Pathology, 16*(1), 71-77. https://doi.org/10.1007/s12024-019-00201-7

About Us | LexisNexis®. (2022). Retrieved 10 January 2022, from https://www.lexisnexis.com/en-us/about-us/about-us.page

Jang, S., & Lee, C. (2018). The impact of location-based service factors on usage intentions for technology acceptance: The moderating effect of innovativeness. *Sustainability (Basel, Switzerland), 10*(6), 1876. https://doi.org/10.3390/su10061876

Novakowski, J. (2022). Social Media and Police Investigations [In person]. City of Pittsburgh Bureau of Police Headquarters.