Te Matataua

The Scouting Party of Air Power

RNZAF Air Power Development Centre Bulletin

Issue 9, June 2017

THE HIDDEN DANGERS OF THE SMART PHONE:

INTEGRATING LOCATION INFORMATION WITH SOCIAL MEDIA

(Originally published as RAAF Pathfinder 282. Reproduced with permission of RAAF APDC).

"Mobile phones are one of the most insecure devices that were ever available, so they're very easy to trace; they're very easy to tap"

Evgeny Morozov, 9 February 2011

It wasn't long ago when the process of locating someone based on data from their mobile phone meant using triangulation algorithms combined with accurate aerial imagery. This process was not only complicated and time consuming but was well beyond the skill of the everyday user. Today, we live in a vastly different world. Rapidly evolving technology, combined with a general ignorance of that technology is a 'perfect storm' for privacy and personal security. Users need to be aware of the information that is stored on their mobile device, and how it can be exploited.

High fidelity geospatial information has increasingly become easy to use and freely accessible to the everyday user. However, since the introduction of personal global positioning system (GPS) devices by companies such as Tom-Tom in 2001, this individual data has become readily available to the wider community. Around the same time that personal GPS devices were becoming household items in the mid 2000's, social media platforms such as Facebook (in 2004) were also being introduced. At the time of their introduction, GPS devices and social media platforms were two separate technology markets and the degree to which their interdependence would develop was not widely understood.

The introduction of the smart phone from 2007 provided a platform with the ability to integrate both geospatial and personal information of the user into one easy-to-use device. Over the last decade, the smart phone has become a common household item and its usefulness has been enhanced through the introduction of various applications, or 'apps'. These apps are designed to improve the quality of day-to-day life and efficiency of the user. In most cases the app does this by collecting and storing both personal and geospatial information and presenting it on demand in a way that is easy to use. However, the full implications for privacy and security were not transparent.

Today, the majority of smart phone users depend on their phones for storing all manner of personal information for their day-to-day usage. Such information can include anything from their date of birth to personal photos, banking details and contacts. Although this type of personal information is usually stored knowingly by the user, the modern smart phone is also capable of sharing data unbeknown to its user. Such information includes the location information embedded into photographs and the ability for apps to track the user's location even when the app has not been opened. It is this direct integration of the user's personal details combined with the near real-time geospatial data that makes the application so useful, while at the same time making it a potential privacy concern, especially if the capability is not fully understood.

Readily available commercial software can locate mobile phones

The simplest example is in the traffic display on Google Maps as you sit on a congested freeway. You, along with your fellow motorists are contributing to a geospatial 'crowd sourcing' by Google, showing congestion and velocity of traffic, via the harvesting of data from your mobile device. Similarly, insurance companies are increasingly asking for imagery (perhaps with geospatial information) of insured items. After damage or loss, their websites seek post-damage or loss imagery and geospatial and temporal data.

To the reader with a background in air operations, or for that matter any military endeavour, the correlation between this data fusion and the aspiration of intelligence preparation of the battlespace, intelligence, surveillance and reconnaissance and indeed battle damage assessment, must be self-evident. When the opportunities for network analysis are added, such as information regarding who has been called and responded to (and indeed the priorities of the response or dismissal), what is presented as convenience and efficiency also becomes fertile ground for those with a darker purpose.

Smart phones carried on operations are a particular risk

It is now clear that a lack of knowledge and understanding of what information can be stored automatically by mobile devices can cause significant privacy and security risks to the user. Not only is the device collecting data, and connecting to overt geospatial tools such as Google Maps, but it is also interacting with social media sites that are automatically collecting the embedded location information stored within a digital photograph.

As an experiment, a photograph was saved from a firearms forum in the USA directly onto an iPad. This photograph clearly showed the make of firearm and type of cabinet used to store the firearm. The iPad user was then able to see exactly where the photograph was taken using the 'Places' function within the iPad software. Using the satellite image background layer, the address and the approximate location on the property where the photograph was taken could be obtained. This experiment demonstrated the ease with which this type of information could be obtained and misused. Fortunately, major social media sites such as Facebook and Twitter now automatically remove the embedded location information as a photograph is uploaded on their sites.

The above example highlights the importance of understanding the risks and implications associated with using the automatic link between personal and geospatial information. However, this is only the tip of the iceberg.

The ability of applications and social media to link personal information with near real-time geospatial information of a user should not be taken lightly. This capability opens the possibility to build up a profile outlining the user's daily routine. What was once the purview of sophisticated intelligence collection is now available to criminal and/or terrorist activities and could be used to compromise missions conducted by Defence and Security staff.

Throughout history, military forces have taken great pains to manage operational security. However, to remain functional in modern society, individuals have become dependent on technology that has the potential to make individual information available on a daily and hourly basis. The last century has seen the 'front line' morph into 'manoeuvre warfare', into 'hybrid warfare'; just how aware and prepared are military forces to deal with the emerging future challenge when 5th-generation military platforms co-exist with a 5th-generation civil society?

More information regarding protecting individual privacy while using smart phones (for both iOS and Android smart phones) can be found at the following site: https://www.staysmartonline.gov.au/mobile-devices

Key Points

- The combination of a smart phone and a lack of knowledge by the unsuspecting user makes it possible to locate an individual easily
- At the time of their introduction, GPS devices and social media platforms were two completely separate forms of technology
- The modern smart phone is capable of storing data that has the potential to compromise the security of individuals and organisations.

APDC Update

The Journal of the RNZAF, Pt B, 2017 has been released. Hardcopies have been sent to bases and camps and an e-copy can be accessed on the APDC website.

E-mail: ohapdc@nzdf.mil.nz