Chapter 13
Use Cases and Best Practices for LEAs

Steve Ramwell, Tony Day and Helen Gibson

Abstract The dramatic increase in the use and proliferation of the internet over the last 15–20 years has seen increasingly large amounts of personal information made, not necessarily intentionally, available online. Consequently, law enforcement agencies have recognised they must open their eyes to this information and begin to use it to their advantage, especially since one of the key benefits of utilising open source information is that it is significantly less expensive to collect than other intelligence. This chapter illustrates how OSINT has become increasingly important to LEAs. It discusses how those carrying out open source intelligence investigation work online might best go about such a practice through the use of specific techniques and how an officer may protect themselves while carrying out such an investigation. It further presents exemplar case studies in how these best practices may, or already have been, exploited in order to bring about tangible results in real investigations.

13.1 Introduction

Open Source Intelligence is not a new phenomenon. Since the 1940s those working in intelligence have leveraged open sources to their advantage (Bradbury 2011). More than law enforcement agencies (LEAs), the military have led the field in realising the value of open source intelligence, the methods and techniques for obtaining it and exacting the benefits from it. BBC Monitoring (a worldwide news aggregator with translated content),[1] in one form or another, has existed since the start of the Second World War translating and examining foreign broadcasts, whilst during the Cold War both sides created vast repositories of open source information from print magazines, books and newspapers (Schaurer and Storger 2013).

[1] http://www.bbc.co.uk/monitoring.

S. Ramwell (✉) · T. Day · H. Gibson
CENTRIC/Sheffield Hallam University, Sheffield, UK
e-mail: S.Ramwell@shu.ac.uk

B. Akhgar et al. (eds.), *Open Source Intelligence Investigation*,
Advanced Sciences and Technologies for Security Applications,
DOI 10.1007/978-3-319-47671-1_13

The dramatic increase in the use and proliferation of the internet over the last 15–20 years has seen increasingly large amounts of personal information made, not necessarily intentionally, available online. Consequently, law enforcement agencies have recognised they must open their eyes to this information and begin to use it to their advantage, especially since one of the key benefits of utilising open source information is that it is significantly less expensive to collect than other intelligence.

The Metropolitan Police have been a proponent of OSINT for a number of years. In 1999, Steve Edwards and colleagues (Edwards et al. 1999) presented an overview of their open source unit and its role within the police. They noted how officers openly and quickly accepted the idea of gathering data from open sources and its advantages of speed, efficiency, availability and cost. Furthermore, they also acknowledged that open source information does not just have one use case within the police: It can support both strategic and tactical responses.

The use of open source information within law enforcement is now becoming more widespread, and subsequently there is a real need for those carrying out such work to be exposed to some initial best-practice principles that they can exploit within their own work. This chapter firstly sets out how OSINT has become increasingly important to LEAs, it then follows with a further discussion on some of these best practice principles for OSINT investigators and then goes on to illustrate their worth within the context of some real-world use cases.

13.2 OSINT in an Increasingly Digital World

Are you a tourist or native? For those of you who were born before the internet was a readily available resource then you are a tourist. Your digital footprint was conceived at a time when the internet was invented and you personally placed it there or someone else did with or without your knowledge. The rest of you are native, born and entering a world where this means of technology is without surprise and possibly any significance; you have never known any other way of life. To compound this, a quick search of open source social media sites reveals proud parents to be, displaying images of a foetus still in the womb, a human with a digital presence prior to birth!

Basic OSINT investigation, within the context of the internet, seeks to identify the online and social footprint of these users and extract data. This is an inevitable by-product of any online visit made, including but not restricted to social media use, chat rooms, etc. Information can also be obtained from resources that seek payment for their services and whilst of value, caution should be exercised as this may cause the investigator to expose their action and or intent. The investigator should also consider that a person has no awareness of their online presence. This can be demonstrated by a photograph of them appearing on a social media site and their name being allocated to the image, all done without their knowledge.

Once an individual has participated online, consensually or otherwise, the ability to remove or erase their digital footprint becomes an extremely difficult task and

given the correct training, continued practice and up to date tools an investigator can usually find a user's online footprint.

The bedrock of any investigation is the initial information provided to conduct such a search. This should be as comprehensive as possible. It is recommended that a document be designed by the investigator and provided to those seeking to use their skills. This ensures that all information is obtained where possible to the satisfaction of the investigator. It cannot be stressed enough how comprehensive this first information should be. Often nicknames, street names, schools, clubs, historic mobile numbers, associates and old email addresses are the key to locating a social profile or online presence as opposed to a simple name and date of birth. Indirect links by association can often prove to be the best method of finding persons.

Other factors to consider are the ethnicity and if known the geography that can be associated to any person being sought. Ethnicity can direct investigation towards social sites used by particular nations. The site VK[2] is used by Russian nationals. To compound this 50–80 % of global OSINT is not English. Furthermore we should have awareness of what the different social media sites are being used for and what can be accessed.

From experience it should be noted that as LEAs in the UK are now extensively working in partnership roles with local authorities, and therefore LEAs ask that the author of the request seeks any additional information from these partners. One final comment is to ensure that the request has a clear and defined objective. What is it that those who conduct the search and the investigation want to achieve?

The information being sought can best be described by use of the analogy "drilling for oil". The oil field being the raw data on the internet being drilled for and extracted, then going through a series of refining processes until a pure clean product is produced. The vast majority of open source online research follows this process (see Chaps. 6 and 7).

An exception to this rule would be to create a plausible social profile and embed it within a geographic or specific crime group to monitor and extract information. This should not be entered into lightly as a considerable amount of backstop or history needs to be created. Often bank accounts are needed and mobile numbers that are active but untraceable are required, as is an address. This persona would not engage beyond making "friends". It would only post generic comments or thoughts designed and constructed to be open questions or thoughts and not directed or focused on any person or group. The longer this account remains functional the better it will become at finding the product, as it becomes immersed into the social platform(s) with age. This style of profile requires significant dedication to maintain and remain plausible with constant checks on security and data leakage. Often the pitfalls surrounding these accounts are not the other users of the social platforms, but the software vendors themselves that monitor for unusual activity. Also legal and ethical considerations need to be taken into account (see Chaps. 17 and 18).

[2]https://vk.com.

Fig. 13.1 Investigative best practices

13.3 OSINT Best Practices for LEAs

On commencing an investigation there are four points of research to be examined. At least one of these MUST exist to have an enquiry. These are *person*, *object*, *location* and *event* (abbreviated to POLE) and can be referred to as the *absolutes*. From years of experience two other areas have been established to investigate: These are *laziness* and *ego* or LEgo, referred to as the *exploitables* (Fig. 13.1).

13.3.1 Absolutes

Intelligence obtained through any technique may be attributed in terms of the people, object, location and event (POLE) data model. This is of particular importance for law enforcement agencies to remain in-line with the guide for authorised professional practice from the UK College of Policing (College of Policing 2013). Furthermore, the usage of POLE has already started a discussion (TechUK 2014) around best practices and common standards for LEAs in the sharing of information between themselves and their partners identifying that it would be instructive if the UK Home Office mandated more best practices around data within LEAs. The emergence of the use of POLE has exemplified how this approach could be beneficial.

13.3.2 Exploitables

Individuals, especially if they know they are doing something wrong, will often make an effort to cover their tracks, which can be achieved in a number of ways which includes measures such as tightening their privacy settings or using an alternative name. That being said, human beings are fallible, even when trying to be

careful they make mistakes, and they often leave a trail of their activity that they may have not considered as particularly important or even be aware of at all. These weaknesses result in a number of areas that can be exploited for the purposes of open source intelligence.

The most important of these are laziness and ego (or 'LEgo' for short), which have particular relevance to microblogging and social media. *Laziness* is not just attributable to any weakness in the security of the user's online profile, but can often be more associated to insecurities in associates, friends or family of the party being sought. This openness or insecurity allows a 'backdoor' to information on the main person of enquiry, hence the need for all available information in the initial request.

Ego is the common pitfall of social media: People consciously or subconsciously use social platforms to share their emotions, thoughts and significantly images of themselves. They often display this by posing in images suggesting their mood with a comment to match. The very purpose of social media sites is to be social. Therefore ample opportunity can be found to develop this (see Chap. 6).

Tracks are often left uncovered due to individual laziness, even when social media sites such as Facebook have security and privacy settings, which would close many of these gaps. Though laziness is only one facet, egotistical behaviour on the other side is exploitable as it often results in individuals bragging about their (illegal) activities. There are many entertaining examples such as the Michael Baker case in Kentucky, U.S. who decided to publish an image of himself siphoning fuel from a police car (Murray 2012) or the case of Maxi Sopo who, after committing bank fraud, evaded police by leaving for Mexico, only to brag about his idyllic whereabouts online and to find that one of his connections was in fact a justice department affiliation (Topping 2009). Another practice often observed is where individuals publish images of themselves brandishing illegal paraphernalia such as weapons, drugs, and copious amounts of cash.

On the other hand, some individuals simply do not understand how to cover their tracks online or choose not to further understand how to. This is often seen in traditional organised crime, where the lowest ranking members of the group are likely to be less educated and have greater potential to make mistakes or leak information.

Online social networks in particular provide rich information about offline social networks, which is often highly accessible in the open source arena. In the UK, population coverage of Twitter is around a fifth (Wang 2013) and around half for Facebook (Kiss 2013), and although many users may have more friends online than offline (often twice as many; Quinn 2011), this data can provide a deep insight into actual social connections. Exploiting these connections often makes it possible to discover individual user activity, even when that user has effectively locked down their account to prying eyes. Their public communications and posts between themselves and connections are often subject to the privacy settings of the other party, providing opportunities for the open source intelligence investigator. Other instances have been observed where online connections, being friends, family members or mere acquaintances, have published compromising content for the target individual—such as a photo.

13.3.3 Information Auditing

An important but often time-consuming and cumbersome process when performing open source intelligence, is the need to audit each step of an investigation. Reasons for doing so may include legal obligation to process, identification of research gaps, and maintaining oversight into the depth of research, among others. Common to all of these cases is the need to actively choose and justify following any path in the intelligence gathering process, as without justification of potential relevance, there may be privacy and ethical complications (see Chaps. 17 and 18).

Auditing can be carried out in a number of ways. The most basic and obvious, though time consuming approach is to manually audit every step in a document or spreadsheet. In other words, to manually record each URL and media item that is accessed whilst gathering intelligence for a particular case—an approach which is error prone. Capturing such data through an automated process is straightforward and common practice. Generally, computer systems capture all or most user, application and system events in event logs or log files, but in more highly scaled environments, databases can be commonplace for this role.

Automatic screen recording on the other hand is less common, and is often a manual process carried out by the individual user. However, it is possible to provide screen recording capabilities through an automated process outside the control of the investigator. An approach that could perhaps become a standard model in law enforcement agencies or anywhere needing accountability.

Finally, the automatic capturing of specific text and media whilst the investigator carries out their investigation is also an important possibility. Such an approach could be a powerful way to combine the processing and analytical capabilities of an automated system with the oversight and direction of an investigative mind-set.

13.3.4 Strategic Data Acquisition

It is feasible in open source intelligence to gather wider, more strategic data, but restraint should also be used to avoid gathering too much or—more importantly—to ensure due process in justification carried out for legal and ethical reasons. Commonly, when the topic of web crawling is discussed, it is often assumed that the optimal approach is that utilised by search engine providers—to access links on a web page recursively. In doing so, it takes little time to become over-burdened with data, and especially data that may be completely irrelevant to the needs of the investigation. Not only does this approach produce too much noise, but it may also be considered as mass surveillance.

Storage, bandwidth and processing can be very expensive when big data starts to become involved, but these are not the only costs. Accessing data in search engines or social media sites from automated systems can often be impossible without circumventing their policies or technologies, an act in itself which can introduce

legal complications. Where it is possible, there are often charges incurred for the privilege. For instance, using the Bing search engine API (application programming interface) for web searches only, a package of up to 500,000 requests currently costs around $2000 per month.[3] While other APIs such as Twitter's REST API are limited to a 15 requests per 15 min window for request pages of individual user posts[4] (see also Part 2 on methods and tools).

Where the investigation is interested in more general data, it makes sense to crawl specific start points related to the target information to a particular depth. Depth in crawling considers how many links the crawler will access recursively. Monitoring sources can be useful in a more strategic context. This consists of regularly revisiting particular web pages looking for changes or links to new unseen web pages.

13.3.5 OSINT Pitfalls

13.3.5.1 Leakage

The use of online tools that aid the investigator with finding, decoding or enriching data could be potential sources of leakage or social engineering. It is not inconceivable that there are seemingly secure and useful online tools to aid the investigator that in turn could be assisting the investigated by way of alerting them. Also, it is possible that once data has been obtained by a third party service, it could then be exploited in a manner that could compromise any investigation. As a result of these possibilities, the investigator must consider information leakage by way of ensuring that, where possible, confidential or critical data is not unintentionally provided to an unverified third party.

A run of the mill example of this is the situation in which an investigator provides an image to a third party forum or web application in order to extract exchangeable image file format (EXIF) data such as geolocation, when there are many offline tools that will do a similar job. Once the image is uploaded, it is unclear to the investigator how this image may then be used.

13.3.5.2 Anonymization

Whilst it is a popular issue that criminals often exploit the availability of online anonymization technologies to cover their tracks, the same should be true for the open source intelligence investigator.

[3] https://datamarket.azure.com/dataset/bing/search.

[4] https://dev.twitter.com/rest/public/rate-limits.

The internet protocol (IP) address, which identifies the distinct identity of the source and target of an internet request, can be and almost always is tracked by web applications such as social networks. Combining this identity with multiple instances of unusual social network behaviour—where carrying out investigative activities is unusual when compared with the behaviour patterns of average users—may lead to the compromising of the investigation, or possible refused access to the server through account or IP address blacklisting.

Owing to this apparent vulnerability on the part of the investigator, it may be necessary to take extra steps in order to protect their online identity and to do so in a manner that is easily configurable. For instance, allowing them to switch IP addresses on a regular basis in order to keep the traces for individual investigations isolated from one another. Hiding the source IP address can be achieved through the use of web proxies which simply mask the address, VPNs which route and encrypt requests via an intermediary destination and anonymity or onion networks such as TOR, which not only encrypts the request but also scrambles its route from source to target through various randomly allocated intermediary locations.

13.3.5.3 Crowd-Sourcing and Vigilantism

The growing popularity of the crowd-sourcing movement also has roots in OSINT with multiple people coming together using open source data to attempt to investigate or solve a problem or crime (see Chap. 12). However, in the past crowd-sourcing has also spilled over into vigilantism with a number of catastrophic effects. The large crowd-sourcing effort surrounding the Boston Marathon exemplified a number of these problems. First, a number of completely innocent people were incorrectly identified as potential suspects causing emotional pain and suffering to themselves and their families (Lee 2013). Furthermore, the number of incorrectly identified suspects actually caused the FBI to go public with the names and images of the Tsarnaev brothers earlier than they would normally, simply to stem the flow of people being wrongly targeted (Montgomery et al. 2013). While this is less of an issue for an individual investigator, LEAs should be aware of the consequences of how these crowd-sourced campaigns can spring up and impact on their own investigations.

13.3.5.4 Corrupting the Chain of Evidence

All data collected and the means of its collection, even open source data, must not contravene the European Convention on Human Rights (ECHR)[5] and, in particular, Article 8 which protects a person's right to privacy. Moreover, in the UK, this is

[5] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005.

further emphasised in section 6 of the Human Rights Act[6] which states that a public authority cannot act in a way which is incompatible with this ECHR. Thus investigators have to apply significant care to understand what personal data they are allowed access within the context of that investigation to ensure that it can be used in future. In addition to this, investigators must also abide by data protection laws (such as the Data Protection Act[7] and the General Data Protection Regulation[8]). Investigators should also ensure that they use anonymous laptop when conducting such investigations and make sure that they take at least screen captures of any digital evidence they obtain that contain both a time and date.

13.3.5.5 Source Validation

An OSINT investigator must not get caught out by the fact that all open sources are not made equal and that some may be more reputable than others. It may be that the site itself is presenting a particularly subjective opinion or that only a small component of it is not reputable (e.g., a specific tweet or Facebook post). Some methods for exploring and validating the credibility of open sources are explored in Chap. 7.

13.4 LEA Usage of OSINT in Investigations: Case Examples

The use of open source information leading to open source intelligence is having a real impact on modern day policing. Information gleaned from open sources is leading to arrests for serious criminal activities. This section describes some examples of how the practice of open source intelligence has assisted in police investigations. The activities described in this section were all conducted using freely available software and social platforms. No interaction of any kind has taken place with any of the parties involved.

13.4.1 Exploiting Friendships in an Armed Robbery Case

FL was wanted for an armed robbery. Owing to the gravity of this offence considerable resources and assets had been deployed to locate the suspect, however his current whereabouts were unknown. Specialist teams spent two days conducting

[6] http://www.legislation.gov.uk/ukpga/1998/42/section/6.

[7] http://www.legislation.gov.uk/ukpga/1998/29/contents.

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

observations on an associate's addresses at a significant cost, which did not result in the obtaining of the required information. In order to move the investigation forwards, help was then sought from an internet investigation unit known as the "Technology Intelligence Unit" (TIU).

Within two hours the TIU located FL on the Facebook social media site. Owing to the personal security setting used by FL his Facebook site revealed little public information. Furthermore, FL exposed little personal information meaning the team could have reached a dead end. However, postings made onto the account by another person disclosed a previously unknown girlfriend, RB who was an active member on social media at the time of viewing. The social media account of RB had little or no privacy settings enabled and displayed images of both her and FL on a beach. Through supplementary research on the account it was established that the location of the beach was in Cornwall, UK. It was further revealed that she had an infant. Additionally, images of her accommodation in the East Midlands were provided.

The consequence of these discoveries was the following positive outcomes. First, the fact that FL was not in the area for which the force was responsible allowed the specialist teams to be stood down saving significant costs. Secondly, research of RB on publicly available data sites offered several potential residential addresses where she may have been residing. These were all compared using Google Street View against an image posted on her social media site. From this image it was possible to identify the exact address of RB. All this information was provided in a readable chronological format to the investigating team. FL was subsequently arrested at RB's address in a safe and controlled manner.

This success illustrates the use of the absolute POLE points: both the person and the location were identified. Then further research using the exploitables LEgo showed the images of them posing for a selfie image on a beach in Cornwall and the image of her property.

The fact that the TIU information provided a known location also allowed the investigating team the opportunity for other tactics to be deployed in detaining FL.

13.4.2 Locating Wanted People Through Social Media

An individual, known as KS, was wanted on a Crown Court bench warrant, i.e., an order, within UK law, from the court directing that the person be arrested.

He had been sought for over three months by two different police forces, but the investigation had continued without much success. More than eight police officers had conducted research doing both house to house and council visits in order to try to locate the whereabouts of KS. These actions had amounted to a significant use of police time and costs that could be better used in matters of a greater priority. The TIU was tasked with seeing if they could help in identifying his location, and consequently he was arrested within one hour!

The TIU conducted their investigation as follows. A social media profile was located for KS. He had posted recent comments stating that he was working with chemicals for the Environment Agency. Additionally he put up a picture of a canal lock with a comment that this was his location when he wanted to take a cigarette break. Research on the internet identified the exact address of the Environment Agency and its proximity to the canal lock. Police officers were notified who travelled to the location and arrested him. The absolute used was the name of KS and the exploitables being the images and comments concerning where a place of work was and an image showing where the cigarette break was.

A second example of using OSINT in this manner was carried out by inspecting the Facebook account of a wanted person named ABC. He had breached his bail conditions and had been recalled to prison. Immediate inspection of his Facebook account provided little personal information. However, an image of him had been posted onto the account wearing a new looking, extremely bright red shiny puffa jacket. This had drawn several comments.

Owing to the uniqueness of the jacket he was wearing, a capture was made of the image and placed onto the electronic briefing system used by the police force. The following day a police officer on patrol in a local shopping centre spotted a male wearing the jacket and recognise it as being the same as the male was wearing from the briefing. Other officers were called in and a rapid and safe controlled arrest was made. Significantly the officer who spotted the male and made this arrest had never seen the person ABC before.

These examples again clearly illustrate how the LEgo effect can be easily exploited by OSINT.

13.4.3 Locating a Sex Offender

Police officers who were seeking to arrest AJ for a rape offence were unable to locate him in their home force area. Using the name and details of other family members, a Facebook account was located for AJ.

An image posted on the account showed a house surrounded by scaffolding, a metal storage container and a vehicle parked on the road. The vehicle clearly showed its registration number. The police initially attempted to check the details of the vehicle registration plate, but it failed to provide a current keeper for the vehicle. The image was inspected again, and it was noted that on the metal container was a fixed sign showing a phone number and the name of the company who had supplied it. By following up this line of enquiry with the company the police were able to establish the location of the container. This provided the investigating officers with an address that led to the arrest of AJ.

Once again LEgo plays a key role in developing the enquiry. As mentioned in Sect. 13.4.1 on the arrest of FL, paying attention to images posted may result in additional information that the individual may have provided without awareness.

13.4.4 Proactive Investigation Following a Terrorist Attack

On the afternoon of 22nd May 2013 the British soldier fusilier Lee Rigby was run down and hacked to death by Michael Adebolajo and Michael Adebowale in broad daylight outside barracks in London. Both killers were identified as being British of Nigerian descent, raised as Christians and converts to Islam. The killers made no attempt to leave the scene of the attack, and it was rapidly broadcast on media platforms globally.

This crime was being monitored by the TIU in case of any reaction that required police intervention locally. During the course of this monitoring, online activity was noted on the social media platform Tweetdeck,[9] which is a dashboard application that facilitates the monitoring of Twitter in a more accessible way than through the Twitter web interface directly. This showed a posting by an online Australian news group who claimed to have had communication with a friend of one of the people responsible for the murder: Michael Adebolajo. The webpage was inspected and a full page article was online which named this friend as Abu Nusaybah. His real name is Ibrahim Hassan. Following this claim, Twitter was searched by a member of the TIU and an account was found for Abu Nusaybah. Details from the account and other information was captured.

The TIU also tried to search Facebook, but found no account. However, using the profile image posted to the Twitter account of Nusaybah, a Google image search was conducted. This revealed a cached web page of the Facebook account for Nusaybah. Through the further inspection of this page the TIU were able to uncover videos, images, postings and friends of Nusaybah, which were all captured and utilised in further investigations. In particular, the TIU identified that the videos contained material which contravened the terrorism laws of the United Kingdom. All this information was rapidly provided to partner agencies. Nusaybah was arrested two days after the Woolwich murder and moments after giving an interview to BBC Newsnight about his friend. He was subsequently jailed after admitting two terror charges for posting lectures by fanatical Islamists online and encouraging terrorism.

The data collected was all obtained using open source tactics and the case provides a good example of the LEgo exploitables as it was an individual's ego that allowed rapid identification and collection of intelligence. In addition, in contrast to the previous examples, it shows how OSINT can be employed not only when there is a specific initial target, as in the previous four cases, but also when there is a suspicion or an expectation that criminal activity may take place. In this case, the TIU began with a proactive investigation by monitoring information posted to social media in the aftermath of the attack rather than participating in an already ongoing investigation into a specific individual.

[9] https://tweetdeck.twitter.com/.

13.5 Going Undercover on Social Media

The information obtained in the above use cases was only gathered through the monitoring of profiles without actually interfering or interacting with them on social media. The usage and befriending of those suspected of criminal activity on social media sites by those in law enforcement can be seen to walk the line between ethical and unethical practice and, at least in the United Kingdom, is governed strictly with the use of non-attributable computers and logging of how and when the profile is in use (Association of Chief Police Officers 2013; HMIC 2014; Tickle 2012; see also Chaps. 17 and 18). However, there are numerous examples of police, especially in the U.S., going undercover on Facebook to get closer to the criminals they are trying to catch.

For example, Officer Michael Rodrigues (Yaniv 2012) made friends with numerous members of a gang associated with burglaries in Brooklyn. He was then able to know when they were planning their next 'job' as they talked of it openly on Facebook as well as seeing the images they posted afterwards of the items that had been stolen. Again, this highlights the LEgo principle: The members were too lazy and also perhaps too egotistical to vet those requesting to be their friend on Facebook, and they wanted show off about the items they had managed to steal.

Similar undercover work has existed previously with it being common for officers to enter chat rooms (Martellozzo 2015) pretending to be young children in order to get the attention of sex offenders (Tickle 2012) or by infiltrating forums that facilitate the exchange of images (CEOP 2008). This work has also now extended to social networks, which due to their popularity amongst young people, provide an opportunity for child sexual grooming (Hope 2013), but also for officers to go undercover on such sites and catch potential offenders themselves (Silk 2015). While these tactics are not unlawful per se, LEAs need to very careful that they do not overstep the line between legitimately creating an opportunity for others to commit crime and unlawful entrapment/incitement (see Chaps. 17 and 18).

13.6 Conclusions

This chapter has explored how Open Source Intelligence is changing the way that law enforcement conduct their investigations. We discussed how those carrying out open source intelligence investigation work online might best go about such a practice through the use of specific techniques and how an officer may protect themselves while carrying out such an investigation. The second half of the chapter then went on to present some exemplar case studies in how these best practices may, or already have been, exploited in order to bring about tangible results in real investigations.

References

Association of Chief Police Officers (2013) Online research and investigation. Available online: http://library.college.police.uk/docs/appref/online-research-and-investigation-guidance.pdf

Bradbury D (2011) In plain view: open source intelligence. Comput Fraud Secur 4:5–9

CEOP (2008) UK police uncover global online paedophile network. Available online: https://www.ceop.police.uk/Media-Centre/Press-releases/2008/UK-police-uncover-global-online-paedophile-network/

College of Policing (2013) Information management: collection and recording. In: Authorised professional practice; Available online: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/#categorising-police-information

Edwards S, Constable D, Scotland, N (1999) SO11 open source unit presentation. In: EuroIntel' 99 PROCEEDINGS E1-European intelligence forum "creating a virtual previous next intelligence community in the European region", pp. 1–33

HMIC (Her Majesty's Inspectorate of Constabulary) (2014) An Inspection of undercover policing in England and Wales. Available online: https://www.justiceinspectorates.gov.uk/hmic/publications/an-inspection-of-undercover-policing-in-england-and-wales/

Hope C (2013) Facebook is a "major location for online child sexual grooming", head of child protection agency says. In: The telegraph. http://www.telegraph.co.uk/technology/facebook/10380631/Facebook-is-a-major-location-for-online-child-sexual-grooming-head-of-child-protection-agency-says.html

Kiss J (2013) Facebook UK loses 600,000 users in December. In: The guardian. https://www.theguardian.com/technology/2013/jan/14/facebook-loses-uk-users-december

Lee D (2013) Boston bombing: how internet detectives got it very wrong. In: BBC News. http://www.bbc.co.uk/news/technology-22214511

Martellozzo E (2015) Policing online child sexual abuse-the British experience. Eur J Policing Stud 3(1):32–52

Montgomery D, Horwitz S, Fisher M (2013) Police, citizens and technology factor into Boston bombing probe. In: The Washington post. https://www.washingtonpost.com/world/national-security/inside-the-investigation-of-the-boston-marathon-bombing/2013/04/20/19d8c322-a8ff-11e2-b029-8fb7e977ef71_print.html

Murray R (2012) Man steals gas from cop car, gets caught after he posts pic of theft on Facebook. In: NY Daily News. http://www.nydailynews.com/news/crime/man-steals-gas-car-caught-posts-pic-theft-facebook-article-1.1063916

Quinn B (2011) Social network users have twice as many friends online as in real life. In: The guardian. http://www.theguardian.com/media/2011/may/09/social-network-users-friends-online

Schaurer F, Storger J (2013) The evolution of Open Source Intelligence (OSINT). Comput Hum Behav 19:53–56

Silk H (2015). Paedophile snared after arranging to meet 12-year-old victim who was actually an undercover police officer. In: The mirror. http://www.mirror.co.uk/news/uk-news/paedophile-snared-after-arranging-meet-6414747

TechUK (2014) TechUK launches "Breaking down barriers" report. In: TechUK. https://www.techuk.org/insights/reports/item/2302-techuk-launches-breaking-down-barriers-report

Tickle L (2012) How police investigators are catching paedophiles online. In: The guardian. http://www.theguardian.com/social-care-network/2012/aug/22/police-investigators-catching-paedophiles-online

Topping A (2009) Fugitive caught after updating his status on Facebook. In: The guardian. https://www.theguardian.com/technology/2009/oct/14/mexico-fugitive-facebook-arrest

Wang T (2013) 2+ years, 15MM users in UK, teams in 6 EU countries, excited to return to HQ and home. Proud to hand off to incredible European leadership! In: Twitter. https://twitter.com/TonyW/status/375889809153462272

Yaniv O (2012) Cop helps take down Brooklyn crew accused of burglary spree by friending them on Facebook. In: NY Daily News. http://www.nydailynews.com/new-york/helps-brooklyn-crew-accused-burglary-spree-friending-facebook-article-1.1086892