The direct correlation between thorough and judicious Pre-Surveillance Intelligence Gathering and the successful outcome of a subsequent Surveillance Operation.

Thesis

Submitted to

The Institute of Professional Investigators

In Proposed Fulfilment of the Requirements for a Fellowship

By

Andrew Duffin MIPI CII ACFS

August 2017

Table of Contents

Acknowledgements

To former-Police Surveillance Instructors Michael Beere and Nigel Strongitharm, thank you for your patience and your professionalism in teaching me the skills which enabled me to secure a long career in operations.

To my valued and respected intelligence gathering colleague, Victoria Hawrylak, thank you for keeping me contemporary in an ever-changing research world.

To my investigative mentor for over twenty years, David Beardsworth, thank you for your generosity, your invaluable guidance and your support.

Terminology referred to within this thesis

Intelligence Gathering terminology:

OSINT: Open Source Intelligence – any information that sits within the public domain and is readily accessible by the general public, such as Google, Facebook, Twitter.

SUBSCRIBER DATABASE: Any 'pay to use' proprietary database that allows the user to access information not available to most members of the public, such as GB Insights, Equifax, X-1 Social Discovery.

PROFILE: The user name of anyone with an online presence

HANDLE: Another term for PROFILE, the name the user chooses to be known by online

USER: The person using a PROFILE or HANDLE

SUBJECT: The person being investigated; the subject of the enquiry

CLAIMANT: The subject individual that has submitted an insurance claim

TIMELINE: A chronological list of events, messages and images posted to a social networking profile

DOB: Date of birth

Surveillance Terminology:

SUBJECT: The individual that is being followed; the subject of surveillance

CONTACT: Sighting of the Subject

TOTAL LOSS OF CONTACT: Follows a 'Temporary Loss of contact'. When the surveillance team has lost control of the subject.

AREA SEARCH: A systematic search procedure used by the surveillance team immediately after a TOTAL LOSS, in an attempt to re-establish contact with the Subject.

TRIGGER: The surveillance team member that will alert the team to a sighting of the subject.

FOXTROT: A foot follow

MAKE GROUND: A command to a backup operative to close up the space during surveillance

VRN/VRM: Vehicle Registration Number/Vehicle Registration Mark

Introduction.

This thesis will explore the combined subject matter of pre-surveillance intelligence gathering and the direct bearing that this investigative function has upon the successful outcome of a subsequent surveillance operation. It will examine the problems and challenges that a surveillance team faces and will identify how intelligence can overcome these challenges and improve the quality of the final surveillance findings.

It is recognised from the onset that intelligence gathering is a specialist form of investigation in its own right, as is the professional and proficient undertaking of a surveillance operation using the correct methodology and techniques. Indeed, extensive publications exist on both of these specialist areas and it is not the intention of this thesis to provide comprehensive instruction on either subject. The intention is to illustrate how the correct application of pre-surveillance intelligence has a correlation on the positive outcome of surveillance.

The thesis will draw upon the training, personal experiences and 'lessons learnt' over a 35 year career, specialising in surveillance and intelligence gathering.

The main type of surveillance work that an operator in the private investigation sector will undertake is Personal Injury observations to assess if a Claimant in a litigated insurance claim is genuine, exaggerating or fraudulent. The content of this thesis will be predominantly aimed at this sector, but, the techniques and methods detailed herein will still have applications for all other forms of surveillance such as matrimonial, due diligence operations and intelligence gathering surveillance.

The reader should note that all of the techniques described herein are adopted on a daily basis and they do work. The thesis does not, by design, take into account the use of GPS vehicle trackers. The writer personally does not condone the use of vehicle trackers on the type of work undertaken within his sector, and has spoken out against the use of trackers on a Radio 4 documentary, The Report. The use of trackers could, in certain circumstances, be deemed to be disproportionate and potentially committing the offence of criminal damage or the civil offence of trespass. The disclosure of the use of trackers is always used by the legal teams for the opposing side in a disparaging way and can seriously undermine the weight of the evidence obtained. Long discussions in Court around the legality of the use of trackers often takes a Judges focus away from the evidence and more onto the welfare of the subject of the investigation and the adverse effect upon them and their family. Furthermore, there is some very poor policy advice that certain organisations have issued to their members regarding the

use of trackers that could leave their members exposed at the evidential disclosure stage and upon examination under oath. It is recognised that certain organisations may use trackers and that they may have their place in intelligence gathering, but, GPS vehicle trackers will not be referred to at any stage within this thesis and it is hoped that the demonstration of the good use and correct application of pre-surveillance intelligence, combined with physical surveillance undertaken by highly trained and skilled operators, will show that these devices are not required.

Finally, although it is acknowledged from the onset that both intelligence gathering and surveillance techniques are two very specific and distinct specialist investigative areas, it would be remiss not to direct the reader to excellent source material that may assist the inquisitive or the inexperienced.

In terms of surveillance, there can be no replacement for professional training by Police or Military instructors, but, a recommended publication for the instruction of the private investigator is Peter Jenkins excellent book titled 'Surveillance Tradecraft: *The Professionals Guide to Covert Surveillance Training*' published by Intel Publications ISBN-10: 095353782X and ISBN-13: 978-0953537822.

Another informative and interesting publication is 'Secrets of Surveillance: *A Professionals Guide to Tailing Subjects by Vehicle, Foot, Airplane and Public Transportation*" published by Paladin Press ASIN: B004Q5C4XG

In terms of intelligence gathering one of the most definitive sources is the publication 'Open Source Intelligence Techniques: *Resources for Searching and Analysing Online Information*' written by Michael Bazzell published by CreateSpace ISBN:-10 1530508908 and ISBN-13 978-1530508907.

An additional source is the Institute of Professional Investigators 'Tracing – *An Investigators Guide to Finding Wanted and Missing Persons*' written by David Palmer FIPI F.Inst.L.Ex, specifically Chapter 5: *Computer Enquiries*.

It should be noted that the published word is only as current as the date it was printed and, given the rapid changes that occur in online research functionality, it is highly recommended that current research information techniques are continually monitored, refined and collated.

One of the best online resources for training and remaining current, which also provides regular updates and advice, is IntelTechniques OSINT Training available via https://inteltechniques.com

A further useful UK source of OSINT training, advice and guidance can be found on the *Qwarie* website available at http://www.uk-osint.net/

Chapter 1: The Evolution of the Investigator

Over the last four decades the day to day operating procedures of investigators engaging in surveillance has changed dramatically and the 21st Century investigator is now equipped with a vast array of technical equipment and online resources to assist them in their enquiries.

Video cameras have evolved from cumbersome shoulder mounted VHS cameras, to Super 8 and Mini DV camcorders and further reducing in size over time to miniature digital cameras with micro SD cards. The advent of pinhole covert cameras now allows for excellent footage of a subject to be obtained discreetly and without fear of detection. Covert recording devices disguised within mobile telephones and other everyday objects have increased the effectiveness of a surveillance operator. Hand-held or covert body-worn radios have reduced in size and increased in range.

Unfortunately, all of these advances in surveillance technology count for nothing if the surveillance team do not actually observe the subject of enquiry or if the team is unable to re-establish contact in the event of a total loss, and with no intelligence to indicate where the subject was heading or their intended final destination.

The need for as much intelligence as possible in relation to the subject of the enquiry prior to undertaking the surveillance is as paramount now as it was four decades ago. The difference is that the requisite intelligence is now readily available; can be accessed securely and remotely without leaving a digital footprint and the sheer quantity and richness of the available intelligence can at times be a revelation to the intelligence researcher.

Historically, accessing even the simplest of information, such as identifying the occupants of the subject address, involved a physical journey to the Local History library and reading through endless columns of the huge, dusty and unwieldly books that contained the Electoral Roll information. This information source was also restricted to just the names of the occupants.

Now, it is possible to access that same information simply by using a subscriber database and entering the house number and postcode. These subscriber databases hold an additional value to digital investigators in that they also contain ‘consented data’, which is consumer data that is sold on to the database provider. For example, if an occupant of the address completes any form of online survey or application and does not tick the box to withdraw permission for their

details to be shared, then key elements of their personal information becomes available to investigators via the same research methods used to establish occupancy. Examples of this consented data are email addresses and telephone numbers attributable to each occupant shown on the Electoral Register. As detailed later, this information is of immense value at the pre-surveillance intelligence gathering stage.

Likewise, historically, when trying to find any relevant or adverse media articles in relation to a subject of enquiry, the same physical attendance at the Local History library source would provide hard copy back issues of the original local publications, which then required a manual trawl. Even the advent of microfiche still resulted in a time-consuming research process as it was impossible to search by the subject name or the subject matter. The modern investigator now has a wealth of media information available at their fingertips. Searches of Google and deep web sites such as *Dogpile* and *Ixquick* will reveal any attributable online information and the seasoned researcher can further refine such searches until there is a degree of certainty that the individual identified in online media is indeed the subject of their enquiry.

The basics of surveillance will always be applicable, such as a close target reconnaissance of the subject address prior to deployment, which can provide valuable information such as attributable vehicles, egress routes, the location of the nearest public transport, the local environment, whether it is a 'hard target' area, and the possible areas that the surveillance units can deploy in order to maintain direct observations with minimal collateral intrusion.

It is possible to access much of the information traditionally obtained by a physical reconnaissance of a subject address simply by an online search of databases such as Google Streetview. As detailed later, there are alternatives to Streetview that can also provide additional information.

Whilst all of the above are illustrations of how modern day investigators are enjoying the best of times in terms of the richness, quantity and availability of intelligence, without question the most defining moment in the explosion of instantly available intelligence information was the advent of Social Media.

Social Media actively encourages and rewards people to communicate publicly with friends, family, business colleagues and strangers. Users will openly discuss their daily lives; their routines; upcoming events; their wants and needs; their interests and pastimes; their relationships and a plethora of additional information such as photographs of themselves and

family, which allows the intelligence gatherer to harvest a huge quantity of information that is of use to a surveillance team.

Second only to Social Media as a source of rich intelligence is the ongoing rise in 'Apps'. Most users of i-pads, tablets and mobile telephones will subscribe to applications that are of interest to them or assist them in their daily lives. If a researcher identifies and accesses any online traffic from the subject profile on these applications, this in turn generates useful intelligence. A prime example of this is '*Strava*', which is an application that uses the Location Services GPS tracker on a user's mobile telephone device to digitally map either a bicycle ride or a run; data which the user will then access and upload onto a public site. Accessing these public sites will show a researcher how often the subject of an enquiry cycles or runs; how far; the routes they take and the speed that they travel.

The modern-day investigator has a wealth of intelligence available to them that their predecessors could only dream. It is, therefore, incumbent on them to make the best use of this resource. Indeed, they could be considered remiss in their duty of care to their end user client if they did not fully embrace it.

Chapter 2: The Legality and Admissibility of the use of Online Intelligence Resources

OSINT means Open Source Intelligence. By definition, this is information that can be obtained using open source links and constitutes publicly available information, either in the form of a free service to subscribers such as social networking sites, or as a paid subscriber service, which is restricted to customers that sign a service agreement, such as Equifax.

Companies that sell their data to paying subscribers hold their own strict data policies that a customer must sign. These are legally binding agreements confirming that the customer agrees to the terms and conditions of the use of the database and the data set.

Any intelligence or evidence obtained via these two sources is admissible in Court. The evidence is secured and collated in such a way that there can be no suggestion that this information was obtained by illegal or unethical means such as the online 'hacking' of personal information.

In addition to these existing sources, the online investigation sector is seeing a rapid increase in the number of suppliers that offer real time monitoring of social networking channels. These service providers offer the investigator the ability to lock onto an individual's social networking profile and receive an instant notification every time the subject 'posts' a new online message. Examples of monitoring platforms are *X1 Social Discovery, Geofeedia* and *Media Sonar*, although there are many more. These organisations rely on ingesting the live stream of social media data feeds from organisations such as *Twitter, Instagram* and others and then commercialise this data as a product to the intelligence community.

To put this monitoring functionality into perspective for a surveillance use-case, a team could be following an individual and lose contact with them. The subject may subsequently 'post' a message to their online social networking sites to inform friends and family that they have just arrived at a location, or that they are undertaking a particular activity at a certain premises, and the monitoring platform will capture this message or image. The intelligence contained within the message or image may enable the surveillance team to quickly re-establish contact.

The use of these monitoring platforms is on the increase, particularly for law enforcement agencies, and some organisations lock multiple subject profiles into their system and monitor the daily activity of a subject of investigation over a prolonged period. The extracted data can then be used to analyse a pattern of life and apply some predictive analysis to identify a subject's anticipated movements on certain days.

The ethical investigator should exercise caution and restraint over the duration of the use of monitoring platforms, as the prolonged digital surveillance of an individual may not be considered to be proportionate to the level of investigation required. There are well publicised issues raised by civil rights groups that became aware that monitoring provided by these platforms was being used by law enforcement agencies.

On 11th October 2016 Twitter announced that it was severing ties with the social media monitoring company *Geofeedia*, a company that ingests data and resells it to investigation and law enforcement agencies. A week later, on 20th October 2016 Twitter further announced that it was severing ties with another social media monitoring company, *Snaptrends*. (Source: Mashable UK. Article: *'Twitter cuts off Snaptrends, which mines tweets for law enforcement')* http://mashable.com/2016/10/20/twitter-social-media-surveillance-snaptrends/#af9auokBS5qF

Twitter withdrew their live feed to a third social media monitoring company, *Media Sonar*, on 12th October 2016. (Source: The Daily Dot. Article: '*Twitter cuts of third surveillance firm for encouraging police to spy on activists')* - https://www.dailydot.com/layer8/media-sonar-twitter-social-media-monitoring/

Twitter's decision to withdraw the live *Twitter* feed to these monitoring companies was as a direct result of individuals and journalists claiming that citizens' civil rights were affected by the excessive and intrusive online monitoring of their social networking activities. Subsequently, *Geofeedia, Media Sonar* and *Snaptrends* have had to work closely with *Twitter* to re-establish trust and restore their access to the *Twitter* 'firehose' of online messages.

Given the adverse media that exists around this form of intelligence gathering, serious consideration should be given to the correct use of online monitoring tools and the proportionate duration of the monitoring function when locked onto an individual's social networking profile.

The submission of a 12-month social networking monitoring report on an individual may not be deemed proportionate when dealing with, for example, a Personal Injury insurance claim. A far more considered and compliant approach would be to research the individual for a limited period, extract any relevant intelligence data, and then discontinue the monitoring.

Any investigator or online intelligence researcher will handle data at some point throughout the lifecycle of a case and, therefore, they or their business must be registered with the

Information Commissioners Office. Furthermore, they must adhere to the regulations set out within the Data Protection Act 1998 (DPA).

It is vital that all researchers are aware of the Data Protection Act regulations. The Act is complex, it should be studied by all investigators, and can be summarised by the following eight data protection principles, which govern the use of personal information.

- **First principle** - Personal data shall be processed fairly and lawfully
- **Second principle** - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- **Third principle** - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Fourth principle** - Personal data shall be accurate and, where necessary, kept up to date.
- **Fifth principle** - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- **Sixth principle** - Personal data shall be processed in accordance with the rights of data subjects under this Act.
- **Seventh principle** - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- **Eighth principle** - Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In summary, there has to be a legitimate reason for obtaining the personal information, such as a client instructing an investigator to undertake research. It is important that the investigator undertakes due diligence checks, or 'Know Your Customer' checks, on the instructing client to ensure that the information they have requested is legitimate.

Personal digital monitoring of the subject of the enquiry should not be 'excessive', in accordance with the Third Principle.

Any person that handles data should ensure that an appropriate Retention Policy exists and that data is destroyed at the time of the expiration date. Adequate online security measures must be in place to protect the data from theft or misuse.

Investigators should also be mindful of the impending new GDPR regulations which will come into effect in 2018. The General Data Protection Regulation (GDPR) will require some cultural changes in the way that we handle data and the regulation will have an effect on companies and their future considerations relating to budget, IT, personnel, governance and communications implications.

Investigators that handle data would be wise to begin the transition process relating to GDPR at an early stage to ensure full compliance in 2018.

Chapter 3: The value of pre-surveillance intelligence to the end user client

The value of accurate and evidential intelligence to an end user client cannot be underestimated. Most clients, particularly within the insurance and legal sector, are bound by strict protocols around the use of surveillance. At times, they appear almost fearful of surveillance and seem to consider it a necessary evil rather than an effective method of proving the accuracy and veracity of the alleged situation.

Whilst many surveillance instructions do not fall under the remit of the Regulation of Investigatory Powers Act, as the originator of the instructions is not a Public Body, it is still good business practice to adopt the RIPA framework as a solid basis for guidance around surveillance.

RIPA details two types of surveillance, which are Directed Surveillance and Intrusive Surveillance. Pre-surveillance intelligence gathering assists regarding justifying the need for Directed Surveillance. RIPA defines Directed Surveillance as covert, but not intrusive, and undertaken "for the purposes of a specific investigation or operation". The richer the pre-surveillance intelligence is, the easier it is to justify progression to the surveillance stage.

RIPA also states that the surveillance must be justifiable and details that "A person shall not grant an authorisation for the carrying out of directed surveillance unless he believes that the authorised surveillance is proportionate to what is being sought to be achieved by carrying it out".

So, whilst most private investigative surveillance activity will not be regulated by RIPA, it should be accepted by the industry as the best framework to adopt. Instructing clients, not bound by RIPA, are still reassured when they are informed that the surveillance operators adopt the RIPA guidelines.

Insurer clients, and specifically solicitors acting on their behalf, will be very careful in their letter of instructions to instruct the investigators to act in a legal and compliant manner. Undertaking a thorough pre-surveillance intelligence report reassures both the client and the surveillance team that there is sufficient intelligence to indicate that surveillance is a viable and proportionate option.

Many insurers and solicitors instruct an investigation agency to only undertake a pre-surveillance intelligence report, also known as a Claimant Profile, and to report the findings back to them before undertaking surveillance. This allows the client to review the findings and

reach an informed decision as to whether surveillance is a cost effective and viable option and, more importantly, if there are sufficient grounds to justify surveillance.

Historically, surveillance was a very attractive option to insurers, who tended to adopt a 'scatter gun' approach to claims investigation and would automatically instruct surveillance on nearly every claim over a certain value. Surveillance was often speculative at best and was seen as a fishing expedition to establish if the claim could be repudiated.

But, with the advent of Lord Woolf's reforms to the civil justice system in his 1995 report and the subsequent changes to the Civil Procedure Act 1997 and the CPR 1998, the whole landscape of claims investigation changed. Lord Woolf sought to eradicate what he perceived to be numerous problems within the civil evidence system, including the length and cost of litigation and the adversarial aspect of litigation. His reforms were intended to encourage openness and co-operation between both parties and, wherever possible, to reach an agreement out of Court.

As a result of this, it was no longer possible for the defence teams to 'ambush' a Claimant in Court during their testimony under oath, by introducing surveillance evidence that the Claimant was unaware of at that point. Pre-Woolf, the usual preferred tactic of an insurers lawyer was to place the Claimant in the witness box, under oath, and ask him questions about his level of physical activity before the accident subject of claim, and then to attest to his current level of disability since the accident. Once a fraudulent Claimant had given false testimony about their alleged disability, the cross-examination would be postponed whilst the Claimant was still under oath, and he would be shown video evidence of him undertaking a level of physical activity which contradicted his testimony, and then he was asked to comment. The case would fall apart soon after and the claim was invariably withdrawn.

Rightly or wrongly, the Woolf Reforms took away the power and impact of a defence team, leaving them in a weakened position, and the balance of litigating power shifted in favour of the Claimant. Now, every piece of evidence relating to the case, including all of the intelligence and surveillance findings, must be disclosed to the opposing sides legal team long before a Court date is ever agreed.

This means that every aspect of a disclosed surveillance report is analysed by the opposing team and, if the evidence is detrimental to their clients claim, they will seek to challenge and discredit the evidence and render it inadmissible out of fear that it will destroy their client's credibility and reduce the claim. Whole teams of experts are tasked with undermining

surveillance evidence; indeed, one investigation firm plays both sides of the fence and seeks to undermine other investigators evidence in return for a fee from the opposing side.

Full disclosure pre-trial also allows the Claimant's legal team to have a ready explanation for the surveillance evidence. For example, if the evidence shows the Claimant is working on a building site and the surveillance budget only allows for three days from Monday to Wednesday, then the Claimant's legal team will state that the Claimant was at home in bed on the Thursday and Friday as he had tried to return to work but the work activity had exacerbated his injury. Or they will say that he experienced a 'good day' in surveillance terms, but quickly deteriorated.

But if we take a similar example of a Claimant being observed out cycling for three days, the opposing legal team can argue the same 'good day – bad day' defence, but, the impact of this defence is completely diminished if there is supporting online intelligence evidence, such as *Strava*, or *Map My Ride,* that provides a full online breakdown of all of the recorded days and mapped rides that the Claimant has undertaken over a period of weeks and months either side of the surveillance dates.

The problems facing the end user client are numerous. Can the surveillance be justified? Is it a cost-effective solution? Is it proportionate? Is it worth the risk of potential adverse media or a complaint? Will the surveillance evidence hold up to any challenges? Whilst there are few definitive answers to these questions, a professional and intelligent approach will reduce the risks of any issues.

This is the rationale that drives instructing clients to seek reassurance from the information provided with the intelligence reports. It allows them to make an informed decision. Beyond that, they also see the true value of the online evidence that is obtained and, in many cases, there is such a vast array of evidence that is so detrimental to the Claimant, it transpires that there is in no need to undertake expensive physical surveillance and huge savings are made on surveillance fees.

To put this into perspective, pre-Woolf Reforms the writer spent all of his Court attendance time as a witness providing evidence on surveillance cases. Post-Woolf he now attends Court to provide witness evidence only on intelligence findings, as the surveillance evidence is usually agreed beforehand. The evidence found during intelligence gathering is often so damning to a Claimant that this is the preferred evidence of use in a defence and, providing the

evidence is secured correctly at source, is impossible to refute. This will be covered later within Chapter 7.

The areas that pre-surveillance intelligence gathering is of value to the end user client can be summarised as follows.

Regulatory

Clients are reassured that all of the intelligence evidence is obtained and secured in an evidential and compliant manner, with all of the underlying metadata intact. The clients expect the evidence to be produced in such a way that it demonstrates it was obtained in accordance with the provisions of the Data Protection Act.

The intelligence assists the client in the decision-making process and allows them to issue surveillance instructions on the grounds that the intelligence evidence clearly shows that surveillance is justified and the instructing person believes that the authorised surveillance is proportionate to what is being sought to be achieved by carrying it out.

Evidence that creates cost savings

In many cases, the extent of the evidence obtained from an online investigation is sufficient for a skilled litigator to repudiate the claim long before it progresses to Court. Digital evidence, secured via online investigation, that shows the subject of the enquiry of a Personal Injury claim engaging in any form of employment, physical activity or sporting activity undertaken post-accident date is collated and stored. This online evidence can then be viewed by insurers in conjunction with the claim, as presented, to highlight any areas of exaggeration or fraud.

Online social networking connections between parties that allege that they do not know each other can be very damning evidence. For example, the occupants of *Vehicle 1* allege that they were struck from the rear by the driver of *Vehicle 2*, and all of the passengers of both vehicles submit personal injury claims and deny any knowledge of the other parties. Any subsequent online evidence that shows that the occupants of *Vehicle 1* do in fact know and communicate with the occupants of *Vehicle 2* will provide a strong indication of claims fraud. A seasoned investigator can conclude that the alleged collision was either staged or fabricated for the sole purpose of deceiving the insurance company.

Evidence that indicates targeted surveillance will maximise the opportunity for activity by the subject

Surveillance is expensive. Any available online intelligence that indicates the best time to undertake observations, combined with a known or suspected level of activity, is of value to the end user client. The client is not only reassured that surveillance is needed, they also have confidence that the surveillance team will not subsequently submit a 'non-mover', inactive observations log.

For example, if online intelligence indicates that the subject plays for a local football team on a weekend, then the end user client will instruct for a period of surveillance to coincide with this date in an attempt to maximise the opportunity for a successful outcome, combined with strong evidential video footage of the subject undertaking activities that are not commensurate with his alleged level of disability, as presented within his claim.

Window of opportunity

This is an extension of the above, and relates to date and time specific pre-surveillance intelligence that greatly increase the possibility of a successful outcome and of observing the subject undertaking activity. This intelligence is far more precise and often results in an urgent instruction for surveillance, to ensure that the limited time window of opportunity is covered by the surveillance team.

An example of this would be any online social networking information volunteered by the subject that identifies a time and date specific surveillance opportunity, such as an online comment that the subject of the enquiry will be attending the Glastonbury music festival the following day.

A client would be very quick to instruct surveillance in light of this level of rich intelligence.

Collateral Intrusion

Pre-surveillance intelligence can provide information that may indicate to a client that surveillance is not a viable option.

For example, if the subject address is identified to be located near a sensitive area, such as a military base, then the risk of a detection of the surveillance team's presence will be of concern and will inform the clients decision making process.

Financial status of the subject

Pre-surveillance intelligence enquiries into the financial status of a Claimant are of immense value to the insurer client.

If the Claimant is identified as potentially experiencing financial problems, such as County Court Judgements (CCJ's); an Individual Voluntary Agreement (IVA) or a Bankruptcy, then insurers would consider that the Claimant may more readily accept a lower claims settlement offer.

Conversely, if the Claimant is a person of financial means and is represented by a good legal representative, then insurers are aware that a low offer of settlement will be rejected and will therefore plan their alternate strategy accordingly.

Genuine Claimant

In many cases, pre-surveillance intelligence will actually identify evidence that fully supports an insurance claim by the subject of an enquiry. Extensive online comments and photographs that clearly demonstrate the day to day challenges that the person is experiencing and the ongoing adverse and detrimental effects on their life, can make for compelling and distressing reading.

In these cases, insurers recognise the claim is genuine and follow the correct legal procedures to provide full compensation to support the injured person.

These intelligence findings will negate the need for surveillance, but, they are still of immense value to a client as they will reduce the unnecessary costs of speculative surveillance, and allow the client to manage the claim effectively.

Accuracy of the Reserve figure

Upon receipt of an insurance claim, insurers have a legal obligation to set aside a financial amount in anticipation of eventually paying the claim, which is known in insurance terms as a reserve figure.

Accurate reserving is crucial to insurers as this fund is effectively locked during the life cycle of the claim and cannot be used to re-invest back into the business, although adjustments can be made. Therefore, if a reserve is too high, then this means that finances are committed that could have greatly benefitted the ongoing development of the insurance company and shareholders. If the reserve figure is too low, then this places a burden on the insurer if they

unexpectedly have to look to other parts of the company to introduce more funds to cover the claims.

If we consider a Personal Injury claim for a Catastrophic and Life Changing injury that has a potential claim value of millions of pounds, then the inaccurate reserving of one million too high or too low can have a serious effect on insurers.

Therefore, the richer the level of pre-surveillance intelligence provided by the investigator to the insurer, the more accurate the reserve process of the claim becomes.

Chapter 4: The Value of Pre-Surveillance Intelligence to the Surveillance Team

Surveillance is one of the most challenging and rewarding aspects of an investigation. When executed professionally, using highly trained operatives, skilled in all aspects of static observations and mobile, vehicular and foot surveillance, the results can be extremely effective.

The challenges facing any surveillance team are vast. Where to position surveillance units; what time to deploy; how many options are there to consider in terms of entry and egress from the location; will the subject use public transport, walk or drive; how will positive identification be achieved; how will the team remain undetected whilst still operating effectively? The list goes on and the circumstances and challenges differ hourly and daily, dependant on the location of the subject address and the subject.

Wherever possible, the surveillance team needs to take advantage of any intelligence that is afforded to them. This may be as simple as a DOB, gender, or family circumstances. In many cases the team can seek further intelligence from the instructing source. Insurance companies may be able to provide details from medical reports that show height, weight and disability, but, if the matter is in early litigation this is not always possible.

Therefore, the information obtained from Pre-Surveillance intelligence gathering is of paramount importance to a Team leader and will affect their decision-making process before, during and after the surveillance operation.

A surveillance Team Leader supplied with only the most basic of details such as name, address and date of birth would be limited in the approach they could take to undertaking the surveillance and they would rely on traditional methodology. But, the Team Leaders decision making process would be greatly enhanced and supported if they were made aware of the following case information that intelligence gathering can, and very often, does provide:

Risk Assessment:

Media searches and online enquiries will reveal if the location is in an affluent area or a deprived and challenged area. It will reveal any adverse online comments from media or residents that would serve to indicate that the location may be a ‘hard target’ area. Even information in relation to statistics such as gun crime, knife crime and car crime may direct the Team Leaders thoughts around the personal safety of his team and the security of surveillance vehicles and equipment.

Deployment:

Research of the location via Streetview and other sources will provide top down aerial maps of the location combined with 3-dimensional street maps of the actual road and the address. This assists in determining the best locations to position surveillance units in order to maximise the possibility of observing the subject and minimising the exposure of the team.

Research will assist the team in identifying exit routes from the subject location. It will also identify the nearest forms of public transport such as buses, trains and underground stations. This can be useful if a team goes 'foxtrot' to follow a subject as, if they know the subject is approaching a previously identified underground or bus station they can be ready to purchase a fare by swiping a payment card and they can relay to the rest of the team to 'make ground' if needed.

Start times:

Intelligence gained from research may provide an indication of the pattern of life of the subject. If they are known to work at a certain location then the opening hours of the work premises can be established and a travel time plan can be calculated from the home address to the work premises, which informs the team of the best probable start time. A surveillance team ideally wishes to spend as least time as possible around the subject's home location, to avoid exposure and detection.

Occupation:

The occupation of the subject may be established during research. Therefore, although the actual employers are unknown, if the subject is followed to a location that is commensurate with their occupation it serves to support positive identification.

Also, in the event of a temporary or total loss it allows for an informed decision making process around suitable search patterns. For example, if the subject is known to be a joiner and he is followed to a large building site and thereafter identification becomes problematic as all workers are wearing hard hats and safety clothing, then a focus on any workers undertaking carpentry work will yield better results and other workers can be eliminated from the process.

Employment:

Social Networking users will often post details of their past and future employment online. Any information relating to a new employer or indications that the subject is venturing into a period of self-employment, is of value to the surveillance team.

A new employers address can be identified, likely start times can be assessed, predicted routes can be established and, in the event of a total loss of contact, the team can re-establish contact at the identified employers address.

Known Family Members:

The identification of known family members is important for several reasons.

Firstly, it allows for 'identification by association'. To clarify, if an unidentified subject is seen in company with identified and known close family member, this assists in the positive identification of the subject.

Secondly, the presence and sighting of known family members would serve as an indication that the subject continues to reside at the property, that they are likely to be within the premises, and reassures the team that they are not watching a 'dead address'.

Thirdly, if the surveillance team recognise the family members they can make efforts to ensure the team members are not exposed or observed, by either remaining covert or moving their position, which minimises the possibility of the subject being made aware of surveillance that has been detected by family members.

Fourthly, if the team are following a subject and they see a known family member at a location, they will know that a meeting may take place and the team will also be aware of the need to exercise a higher level of caution to ensure they are not detected by a family member whilst the teams focus is solely on the subject of their enquiry.

Attributable Vehicles.

The subject may have posted images of his car on Social Networking sites. This information is of obvious use to the surveillance team.

Additionally, a known family member identified during intelligence gathering may also have posted images of their vehicles online. The surveillance team members would be made aware

of this vehicle and monitor the occupants if the vehicle is seen arriving or leaving the area, as the subject of enquiry may be a passenger.

Lifestyle:

Many social networking users regularly publicise information relating to their daily routines, hobbies and past times. This is of value to the surveillance team. Often, intelligence can inform them of specific days when a subject will be undertaking a known activity identified via research, such as attending a sporting event, a music festival or a family event.

This information can unlock many opportunities and considerations for the surveillance team. The team may decide to already have an operative at a known location in anticipation of the arrival of the subject, which takes the pressure off the following team in the event of a total loss and reduces the possibility of a detection if a subject becomes surveillance aware.

Collateral Intrusion.

Intelligence gathering will identify any sensitive area in the anticipated area of operation that the team will need to be mindful of such as nurseries, schools, churches, Police stations and hospitals.

An awareness of these locations allows for a sensible and considered approach that will reduce the possibility of a detection of the teams presence.

Applying the intelligence to surveillance:

If we consider the challenges that a Surveillance Team in the following scenario are facing, which will be familiar to any experienced operative, and then compare the traditional approach to the pre-surveillance intelligence approach, it will illustrate the effectiveness of intelligence gathering.

In this scenario, the surveillance team are faced with a challenging address location, or 'plot'. The subject of their enquiry resides in a tower block containing forty (40) flats. There is a communal lobby exit to the front which leads to various public transport options, and a rear communal exit that leads to a 'residents only' car park with parking for forty (40) vehicles. Both doors are controlled by security intercom access. There is a manned security concierge desk in the lobby and CCTV cameras protect the interior and exterior of the location.

The Team only knows the name and address of their subject, his DOB, which indicates he is aged in his late twenties, and the fact that he is a married man with a 7-year-old child. When

viewing the layout of the block it is established that the flat number of the subject address is located on the 6th floor.

So, the Team is faced with a number of immediate challenges. Where to plot up to be able to watch the front and rear exit? How to positively identify the subject amongst the other multiple occupants of the location that will exit from the same communal doors? How to identify any attributable vehicles? How to minimise the team's exposure to any third party or to the subject whilst continuing to maintain direct observations in the location?

Whilst challenging, these problems are not insurmountable using traditional methods. The Team Leader can ensure that they deploy operatives that can maintain observations on the front and rear exit and trigger out anyone that matches the age range of the subject. Perhaps they will be fortunate enough to be able to see into the lobby and the lift and stairs exit, which would eliminate the four ground floor flats but still pose a challenge for identifying the remaining occupants. Using this method, the best the team can hope for is identification by process of elimination by age, but, if there are multiple males of the same age range at the location, this can be a lengthy and challenging process.

Perhaps the Team Leader may consider deploying an operative into the lobby to see if the lift comes down from the 6th floor? Or to try and obtain a position on the landing of the 6th floor with a direct view on the subject flat door? These tactics can be effective, but, they run a very high risk of a compromise and a detection of the operatives' presence, especially in a premises that has manned security and CCTV. No matter how good the operatives cover story is, his 'cover for action' or his 'reason for being there', it is not an option that can be sustained over time.

The Team Leader could consider deploying an operative to attend direct at the premises to undertake a pretext enquiry at the subject address in the hope of identifying the subject. This can be an effective technique but effectively 'burns' the operative for future use on the case; the subject may not answer the door; or they may be made suspicious after the pretext enquiry. Furthermore, in personal injury cases where the subject (Claimant) is legally represented by solicitors in an ongoing litigation matter, and the operative is acting on behalf of the insurers for the opposing side, then no-one should approach the subject directly. Most subjects that are filing an insurance claim are fully aware of the possibility of a surveillance operation being conducted against them during the lifecycle of the claims process. They are warned of the likelihood of surveillance by their own legal team and they see the numerous television and

newspaper articles that regularly show surveillance findings in civil claims and the prosecution of fraudsters.

If the team are in possession of a land line telephone number for the subject they may consider calling the number every time a male of the correct age range leaves the premises. Conversely, if the team knows the mobile telephone number they may consider calling the number when they observe a male of the correct age range, with the added bonus of visually seeing the person answer the mobile and thereby confirming identification. These are effective techniques, but, if this process of elimination system results in multiple calls to the subject before the subject can be identified then they will become suspicious. This technique must be used sparingly and, again, increases the likelihood of a detection.

The same technique could be deployed by calling the intercom every time a male of the age range leaves, but, this results in the same problems and risks as the telephone calls detailed above, with the added exposure of the physical presence of an operative using the intercom.

In this scenario, the problems for the Team Leader are increasing for every hour they remain on plot. If they have resorted to placing an operative in the building, or if they are having to park the team very close to the exit doors or they have an operative standing outside the communal exit of the premises, then the team's third party exposure time on the ground increases and therefore the risk of a detection increases exponentially.

If we view this exact scenario again, but with the added advantage of good pre-surveillance intelligence gathering, the challenges can be reduced and the chance of a successful outcome can be optimised. The following will refer to a number of assumptions and examples relating to the level of pre-surveillance intelligence that can be identified, but, all of these examples are accurate and have been used time and time again on surveillance cases.

The traditional approach the Team Leader has taken so far in this scenario may well result in a successful outcome, but equally it could result in following the wrong person, a detection of the team's presence, a wasted surveillance day and an increase in the teams' exposure in relation to time spent on the ground.

Good pre-surveillance intelligence equips the Team Leader with a level of knowledge that allows for a far more considered and discreet approach.

So, if a consumer search is undertaken on the subject this will identify his full name and any email addresses and mobiles or landline telephone numbers attributed to him. The search will

also identify his wife and the same level of detail. Using this consumer information for Social Media research can result in identifying several online user profiles for the subject such as *Facebook, Twitter* or *Instagram*.

When viewing the content of these social media profiles the researcher may identify photographs of the subject and his family. Research may also identify images of him standing next to his attributable vehicle which, at the very least, will provide a make, model and colour and in many cases the vehicle registration mark.

Equipped with this information, the Team Leader no longer needs to apply process of elimination. They can position the team further away from the exit doors to minimise exposure and the risk of detection. They can check the communal car park and nearby roads in the hope of locating the subject's attributable vehicle shown in the research images.

But what if the subject has no interest in social media and has no online presence? Again, thorough intelligence gathering can still be effective. Consider the wife's email address and mobile number that were identified during the consumer searches of the subject. These sources can also lead to the successful identification of her online social media profiles such as *Twitter* and *Facebook*. So, whilst the subject himself may have no interest in social media, his wife may have uploaded family photographs which include images of the subject, which again assists in his identification and alleviates the pressure on the surveillance team.

If we assume that the subject is a 'ghost' on the internet and has no presence whatsoever, and is not shown in any family photographs, there is still a huge operational value associated with pre-surveillance research into his family. Some discretion should be exercised here, as the family are not in litigation and are not the subject of surveillance, but, a discreet and proportionate review can be undertaken in the pursuit of a possible detection of an insurance fraud.

Still using the same scenario, and assuming that his wife has an online presence, the Team Leader now has sight of an identification photograph of her. Most mothers will also upload images of themselves with their children. In certain cases, children have been seen wearing school uniform clothing and a close inspection of the logo or school name can identify the location of the school premises. Whilst extreme care should be taken over the use of images of children it is important to note that information posted on *Facebook, Twitter* and similar sites lies within the public domain and is classed as OSINT. The user is fully aware that they are exposing their images to anyone in the world unless they adopt the appropriate privacy settings.

There can be no suggestion that any form of 'hacking' takes place to access this information. They are, in effect, inviting people to look at their lives. As long as the researcher exercises an appropriate level of proportionality and adheres to the DPA in relation to the use, storage, dissemination and retention of the information then there are no issues.

So, even if the Team Leader does not have an identification photograph of the subject of the enquiry, they now know what his wife looks like and his child. Any male of the correct age range leaving the location in company with the identified wife or child would be of interest. The Team Leader can have a reasonable expectation that any male accompanying them is likely to be the subject of enquiry. This is known as 'identification by association' with known parties.

If a male of the correct age range leaves with the child during the early morning hours at a time associated with a school journey, then not only is he likely to be the subject of the enquiry, as he would be unlikely to trust the care of his child to another person, but if the school uniform has been identified during pre-surveillance intelligence gathering, the surveillance team can anticipate the direction of travel and the destination that the subject is heading, which assists in the event of a total loss of contact. Indeed, a shrewd Team Leader may consider already having an operative at the school location to monitor the arrival of the subject..

The above scenario is an example of how the most basic of pre-surveillance intelligence gathering can affect the outcome of surveillance and supports the surveillance team in their ongoing operation. Further exploration of this scenario will follow in Chapter 6 to illustrate the benefits of ongoing intelligence gathering during the live surveillance operation.

There are also hidden values to the surveillance team, and indeed the investigative firm as a whole, that go beyond just the professional surveillance output that is enhanced by intelligence gathering.

An understanding of the client's philosophy around the use of surveillance and their intended use of the evidence obtained is important in order to put this into perspective.

Insurance clients, who account for the bulk of surveillance work to the private investigation sector, are ultimately represented by a legal team that supports them during the claims process. The source of personal injury instructions to investigative firms will either be direct from the insurers or from their defence solicitors. Some knowledge and understanding of how the legal teams work will serve not only to illustrate the importance of intelligence gathering, but also how it can affect your own business in terms of client retention and repeat instructions.

Defence clients in the personal injury sector that instruct for surveillance are seeking evidence that will either serve to repudiate the claim in its entirety due to fraud; to reduce the amount of the final damages awarded by proving that the Claimant (subject) is exaggerating the extent of their disability; or to pay the claim in full if an investigation shows the person to be genuine.

The only way that insurers can make a commercial decision as to whether to choose the path of repudiation, negotiation or full settlement is by seeing the Claimant (subject) at a time when they are unaware that they are being observed, ergo covert surveillance.

The worst possible outcome for a legal team, after a surveillance instruction, is to be provided with a 'non-mover' or 'no show' report by the surveillance service provider. This does not allow them to progress the case in any way. Indeed, it is extremely detrimental for the surveillance provider in terms of future work for one crucial reason. The insurers legal team have to disclose every relevant piece of evidence to the opposing side prior to a Court hearing. This includes any days that the Claimant was not observed by the surveillance team. So, the legal team is very unlikely to instruct the same surveillance firm to undertake another period of surveillance because even if the team is successful on the second occasion, the previous non-mover days will still need to be evidenced and disclosed. For example, during a three-day surveillance the subject is not observed and the case is reported back. During a reinstruction to the same surveillance provider, the subject is observed to be active over another three days. At disclosure stage, all six days are submitted, which allows the opposing side to indicate that the Claimant was only active for 50% of the surveillance period, which diminishes the value of surveillance. Instead, shrewd legal teams and insurers may choose not to re-instruct an agency that submits a three-day non-mover surveillance report and may instead instruct a completely different investigation agency. The rationale they apply here is that if the second agency obtains a result, then the first agency's non-mover report will never be used or submitted. This means that if the second instructed investigators are asked under examination under oath if this is 'all of the surveillance' they have ever undertaken, they can truthfully reply in the affirmative and the Claimant is shown to be 100% active. This is one of the reasons why insurers have at least three surveillance suppliers on their panel appointments.

Legally, it must be remembered that the civil procedure for claims is, by nature, both litigious and confrontational and often the victor is the legal team that takes advantages of any shortfalls from the opposing side. So, in the above example, the Claimant's legal team would be well advised to ask the opposing solicitors if they have instructed any other periods of surveillance

on their client, rather than asking the investigator under cross examination, as the investigator may be unaware of the involvement of another investigative firm.

Ethically, it could be seen that the defence team are submitting all evidence relevant to the case which shows the Claimant to be active and, unless asked for additional information from the other side, they will rely on that evidence alone. Due to the confrontational nature of this form of litigation it is for the Claimant's legal team to ensure they have asked all relevant questions. This is done in the form of a Part 18 Further Information request under Rule 18.1 and 18.2 of the Civil Procedures Rules. A Part 18 request is a useful document that can be used prior to a court case to ensure that all of the requisite information is obtained and clarification of any points can be sought. If either side fails to ask all of the information relevant to the case prior to the court hearing, such as how many periods of surveillance have been undertaken on the Claimant, then the opportunity is missed and the defence team can use that to their advantage. It should be noted that this is purely a matter for the legal teams and the investigator will play no part in this process. Indeed, they will be unaware of any other surveillance beyond their own instructions, therefore, there is no ethical or legal dilemma for the investigator.

With the above described practice in mind, there are obvious dangers to a surveillance firm that provides a non-mover report and loses out to a client in this way, as it means that one of their competitors is given the opportunity to 'put the job right' and runs a high risk of a competitor becoming a preferred supplier.

Conversely, in light of the above, there is a real opportunity here for repeat business and client retention. If a surveillance provider is always able to submit an active subject surveillance report, then the legal teams are even more likely to reinstruct the same supplier as they desire continuity of evidence, save on witness fees at the upcoming court case by using the same investigator, and they have the confidence in the surveillance provider, given that they have already been issued a previous successful surveillance report from them.

It can be concluded, therefore, that a successful outcome to a surveillance operation instils confidence in a client and ensures repeat instructions and loyalty from the instructing client. Pre-surveillance intelligence optimises the opportunity for a positive surveillance outcome, which in turn keeps the repeat business flowing.

Chapter 5 - Operational methodology when utilising pre-surveillance intelligence sources

As discussed within the introduction, this is not an instruction manual on intelligence gathering and research techniques, but, it would be remiss of the writer to refer to various techniques without clarifying the sources and how those resources and techniques can be applied in a practical sense to increasing the likelihood of a successful surveillance outcome.

The primary function of online intelligence gathering is to identify any intelligence that relates directly to the subject of investigation. In order to do this, the researcher must first identify any online profiles, handles or user names of the subject that will provide access to social networking sites. This can be undertaking in numerous ways.

A consumer search of the subject address may reveal consented data in the form of emails and telephone numbers that can then be fed into various sites to establish if an attributable social networking profile is identified on the site. Once a user name, handle or profile has been identified this can be locked into a monitoring platform that provides real time updates every time the subject updates their public profile.

Pipl searches can be used to identify further social networking profiles of use to the intelligence gathering operation.

Geo-location searches can be undertaken by placing a geo-fence around the subject premises and identifying any social media posts sent online from the address. Systems such as *Echosec* or *Geofeedia* are ideal for identifying any posts or messages from the location, which in turn allows a researcher to identify the profile and to fully explore the user on the appropriate social media site. For example, a successful geo-location fence placed around the subject address may reveal an image that was posted online, which in turn then identifies the user profile.

Once the relevant profiles known to be attributable to the subject and family members have been identified, then a full analysis of the social media sites can be undertaken. The intelligence gleaned from these enquiries forms the basis of the pre-surveillance intelligence that is of value to the surveillance team.

The following is not a definitive list of intelligence gathering sources and there are numerous alternatives in existence, but, these are sources that have longevity in the investigative industry, they have been tried and tested and they provide a stable and reliable digital output for the investigator.

To effectively illustrate the techniques and relevant intelligence sources, and to demonstrate their effect on the planning, preparation and outcome of surveillance, the relevant title headings that were highlighted within Chapter 4: '*The value of pre-surveillance intelligence to the surveillance team'* will be replicated below with relevant commentary.

Risk Assessment:

Streetview and *Google Maps* will highlight any sensitive areas within the vicinity of the subject address.

Media searches may reveal articles that identify problems within the neighbourhood that may affect the surveillance team decisions, such as a high level of criminality, or a scheduled street demonstration by civil rights activists.

Social media searches of *Facebook, Twitter* and other sites may reveal online comments or photographs of the subject of the enquiry, or family members, that portray them as potentially violent individuals. Online comments may also indicate that the subject may be of a criminal disposition and, therefore, may be watchful for Police surveillance.

Electoral Roll databases such as *GB Insights* will provide details of the subject of the enquiry and any other occupants over the age of eighteen. This will provide details that may lead to the identification of social networking profiles. Residency searches will serve to indicate to the surveillance team the number of likely occupants of the address that they are observing.

Deployment of surveillance units:

Streetview and *Google Maps* are a useful source of pre-surveillance intelligence and can provide both aerial views and street views of the address and the immediate vicinity. This enables the surveillance team to identify prime positions for the deployment of observation units and minimises the exposure of their physical presence during a reconnaissance.

Start times for commencement of surveillance:

Profiles identified on *Facebook, Twitter* and others social networking sites may provide online comments from the subject that indicate their likely pattern of life and daily routine.

Locking the attributable social networking profiles into a monitoring platform such as *X1 Social Discovery, Geofeedia* or *Media Sonar* will provide a historic timeline of activity for the subject which can subsequently be analysed to predict the most likely times of activity.

Occupation of the subject:

A review of a subjects *Facebook* or *Twitter* profile may reveal information in relation to the occupation of the subject. Searches of any attributable *LinkedIn* social networking profile will also identify current or previous occupations.

Employment:

Facebook, Twitter and *LinkedIn* are sources that can identify the specific employer of a subject. The subject may post his employers details within his social networking profile, or they may comment on recent new employment within their profile timeline.

Known Family Members:

Images and comments contained within social networking sites such as *Facebook, Twitter, Instagram, Pinterest* and others may identify family members, which will assist the surveillance team in identifying occupants, confirm that they are watching a live address and this intelligence will further assist if they need to identify the subject by association with family members.

Attributable Vehicles.

Images and comments contained within social networking sites such as *Facebook, Twitter, Instagram, Pinterest* and others may identify attributable vehicles of the subject and/or family members.

Streetview will show the make, model and colour of any potentially attributable vehicles at the address, although VRN's are pixelated at source and unreadable.

Mapilary is a variant of Streetview. User take up is on the increase within the UK. Although lacking in coverage, occasionally it has a positive use as attributable vehicles can be identified and, at the time of writing, *Mapilary* does not pixelate VRN's.

Lifestyle:

Pattern of life assessments undertaking during the targeted social networking monitoring of *Facebook, Twitter* and any other identified user profile accounts may reveal lifestyle indications. Regular attendances by the subject at known locations may assist in establishing contact for the surveillance team.

The subject may link online applications that they use in daily life to their social networking profiles, such as *Strava, Map My Run* or *Map My Ride,* which will provide information on their daily exercise routine.

Information relating to lifestyle also assists the surveillance team if the subject is followed to a location that they are known to hold an interest in or a connection to, as it serves to further confirm identification of the subject.

Collateral Intrusion.

Streetview and *Google Maps* are useful for the risk assessment of potential collateral intrusion within the area of operation.

Chapter 6: Ongoing intelligence gathering during surveillance

The same operational methodology applied to pre-surveillance enquiries also has valuable applications to ongoing intelligence gathering during a live, on-going surveillance operation. An experienced surveillance operative will always be seeking any details that improve the chances of successful surveillance and of minimising a detection of their presence.

There are numerous practical examples of physical intelligence gathering during a surveillance operation.

The operative could 'walk the plot' and attempt to identify any attributable vehicles. If the subject is known to be disabled, then any vehicles parked nearby and displaying a disabled badge would be of interest. An inspection of a vehicle interior may reveal a walking stick lying on the rear seats or on the parcel shelf.

If pre-surveillance intelligence has already established that the subject of the surveillance enquiry has a particular sporting interest or an affinity to a club, then any vehicles with stickers or emblems that relate to the same club or activity will be of interest.

If intelligence has established that the subject follows a particular hobby or past-time, then any contents within the interior of a vehicle that match the hobby could indicate that the vehicle is attributable to the subject.

Intelligence may already have established the occupation or trade of the subject. The exterior and interior of vehicles parked in the vicinity can be checked to see if there are any attributable sign-written vehicles or any trade items within the interior of a vehicle that would indicate the vehicle is of interest to the operatives.

The above examples are a small selection of the practical and physical checks that can be undertaken during surveillance.

But, there is a far greater wealth of intelligence available during the live surveillance operation that can be fed to the Team Leader, or information that the surveillance team can pass back to an intelligence researcher for further investigation.

If we consider the surveillance scenario outlined within Chapter 4, then we are already aware of the vast amount of information that would have assisted the surveillance team in undertaking an otherwise challenging assignment. But what if the team did successfully identify the correct subject, followed him on a morning school journey to transport his son, but then the team has

a total loss of contact as the subject drives away from the school? The following examples will illustrate the value of ongoing intelligence.

If the surveillance team suspects a particular vehicle of potentially being attributable to a subject of a personal injury claim, then an online HPI check will identify if that vehicle is subject to finance. If the finance provider is Motability, then the vehicle is known to be associated with an individual that is disabled or restricted.

Assuming that intelligence has not already established a predicted pattern of life for the subject, then real time monitoring of any attributable social networking profiles of the subject may yield new information that assists the team in re-establishing contact. The subject may 'post' online a new comment or message, via *Twitter, Facebook* or similar, that provides an indication of his current location.

Many retailers actively encourage customers not to set the privacy settings on their devices. A customer that enters the premises may be choose to 'check in' at that location, which in turn updates their social networking profile to show friends and family where they are at that time. So, the subject of surveillance may 'check in' online as he personally attends a high-street coffee retailer and his updated *Facebook* profile timeline would then indicate his exact location. This provides valuable intelligence to the surveillance team to travel to that location and re-establish contact.

If, during the live surveillance, the operational team notes information that may be worthy of further research then they should relay this back to a research team, who will in turn seek to enhance the known intelligence. For example, the surveillance operative may have noted a sporting club sticker on the vehicle, such as a Karate club, gymnasium or similar. Further research may reveal the location of the club, the opening times and any upcoming events that may afford an opportunity for ongoing surveillance.

Throughout an ongoing surveillance operation, the subject of enquiry may visit several residential addresses. Real time research into the occupants of the address, via Electoral Register and consented consumer searches, may identify the occupants to be relatives of the subject. This is vital information to the team as it establishes a pattern of life for the subject and, in the event of a total loss of contact, it provides a further familial address that can usefully be checked during a search pattern.

The subject may be followed to a business address. Real time database research may reveal the subject to be a proprietor of the business or a Director of a Limited Company. This information also assists in pattern of life enquiries and may provide additional information such as the registered office of the business and the residential address supplied by the subject to Companies House.

Chapter 7: Evidencing the intelligence findings

The evidential value of intelligence gathering and the subsequent impact on the settlement of a claim or dispute cannot be over-stated. As highlighted previously, there has been a huge shift in the way that evidence is presented when defending litigated matters, particularly insurance claims.

The historic reliance on securing damning surveillance evidence in order to repudiate a claim or reduce the final settlement is no longer prevalent. Due to the vast amount of intelligence that can be found online, combined with the huge costs savings by not adopting surveillance, the end user client now chooses intelligence gathering as a preferred method of claims management.

In the same way that surveillance findings need to be evidenced in a compliant format, the same applies when submitting intelligence findings to the Court. If the intelligence evidence is detrimental to the Claimant, then his legal team will seek to undermine the evidential integrity of either the findings or of the methods used to obtain the intelligence. The same rules of full disclosure prior to trial apply to intelligence evidence and, therefore, the opposing legal team will have ample time and opportunity to look for flaws in the evidence and run their own searches to corroborate if the evidence was obtained legally.

It is, therefore, of vital importance that the investigator obtains the intelligence ethically and submits the evidence in an appropriate and compliant manner. The investigator should expect to be called to Court to provide evidence of their findings and will be subject to examination and cross-examination regarding the techniques employed to secure the evidence.

The usual method of submitting intelligence evidence is for the researcher to compile a Witness Statement detailing their investigation and exhibiting the various relevant findings in stages within the statement. It is important to understand that the exhibits will be printed in paper form and added to the Court bundle to be used by the Judge and the opposing sides, and for the witness to refer to when they provide their evidence in Court.

The use of paper Court bundles can become problematic if the investigating researcher is asked questions relating to the integrity of the evidence, as much of the supporting evidence to corroborate the methods by which the intelligence was obtained lies within the metadata contained within the digital document version of the evidence. This can become an issue if, during examination as a witness, proof is required of the integrity and provenance of the

evidence. The researcher providing evidence must be prepared to assist the Court in understanding the concept of metadata, as the Court will be working from physical paper versions. If questioned on the veracity of the evidence, the researcher should draw the attention of the Court to the watermark data shown on the header or footer of the PDF paper version print out of the digital document and explain what the metadata represents. They should also be able to explain how, by examining the properties of the digital document, the metadata can be examined. It is useful in these circumstances to already have a screen print-out of the properties of the digital document to refer to if required.

When a website page, social networking profile or online content is captured during research and secured within a digital evidence folder, the digital printing process carries across metadata which lies with the properties of the document. Examination of this metadata will reveal information such as the web page that has been printed, the date and the time and the http:// link to the page. The document properties will also reveal the digital author of the document, which will either be the researchers name or the personal computer identification number of the machine used for online searches.

Metadata is, therefore, of vital importance to corroborate the source of an investigation and the date that it was obtained, as it effectively date stamps the evidence and shows that it was contemporary on the date it was obtained. This is useful in cases where the subject of enquiry is made aware, at disclosure stage, that compromising evidence exits on their social networking profile and they subsequently delete the profile content and change their privacy settings.

End user clients can place huge demands on the investigator to evidence the findings in the correct way. A subject of enquiry who uses several social networking profiles and posts updates to them on a regular basis may have so much content on their profiles that capturing the evidence is extremely time consuming and printing it can result in hundreds of pages of a PDF document, which then has to be copied and added to the Court bundle. The matter is further complicated when clients ask for the full online ‘comments’ to be evidenced and secured. Comments are online replies or responses to a message or image posted by a user. For example, the user may post a photograph of themselves undertaking some activity and all other online persons that see the photograph can type a personal comment, which then appears in chronological order in the user profile at the bottom of the image. This can result in hundreds of comments, including further comments and ‘replies to replies’ by the original user, who is the subject of the enquiry. Many times, these comments have a bearing on the case, but, unless

the researcher manually clicks on each comment to expand the content, they will not all be depicted on the screen. This can be challenging in cases where the client wants all comments to be included within the intelligence report.

Each social networking site is unique and stores data in a different way to their counterparts. Understanding and adopting the best way to extract the evidential intelligence and converting it into a usable format for the Court is a prime requisite for any researcher. In the case of Facebook, if the researcher uses a software installation called '*Extract Face'*, then this allows the researcher to ingest the data from a Facebook profile into an evidential format. *Extract Face* will allow the user to obtain a 'screen dump' of the entirety of online images from the user timeline; to extract all of their social networking online friend's data and, crucially, to expand all of the comments that exist on the profile page. Other social networking sites have their own variations of extracting the relevant data.

Converting the online findings into a PDF (Portable Document Format) digital document, either by print screen functionality or by using a software package such as Acrobat PDF Writer, is the most secure and best way of evidencing online findings and, evidentially, the process carries the metadata across into the PDF document.

The *X1 Social Discovery* software has the ability to extract every part of an online social media profile and convert the content into a PDF document, Excel sheet or CSV file. *X1 Social Discovery* also separates the image from the metadata and provides a link between both, so if 100 images are downloaded, by clicking on the metadata link of a single image the reader is immediately taken further into the PDF document to the metadata page that is attributable to the selected image. The metadata page will show all of the evidential information and, in some cases, will also show the GPS co-ordinates attributable to the location that an image was taken. Other suppliers such as *Geofeedia* and *Media Sonar* offer the same functionality.

It should be noted that the file size of social media outputs to PDF can be extremely large and, as a consequence, this creates further problems in terms of digital file storage and evidence retention.

Evidentially, whichever of the numerous options a researcher chooses to adopt in order to convert the onscreen intelligence into a digital format, it must carry the metadata onto the evidential output, for the aforementioned reasons.

Chapter 8: The Future

Technology is moving at such a rapid rate that it is sometimes difficult for an investigator or intelligence researcher to keep track of what is still current and what has been made redundant.

There are a number of very well established online sources that are extremely unlikely to disappear, such as *Facebook, Twitter* and *Instagram*. These providers are continually enhancing their product or adding new features in order to retain their current users and attract new users. They are heavily reliant on selling advertising space on their sites for continued revenue and, therefore, the more users they have on the site, the more attractive they will be to businesses that wish to advertise their services on to their public users.

Due to these continual changes, it is crucial that researchers and investigators employ some form of research and development in order to remain current and, more importantly, to learn how to ethically use the systems to their advantage when undertaking investigations.

Advances in the way that retailers communicate with consumers should be monitored and explored to see if they hold any new intelligence gathering options. Facial recognition software, the 'Internet of Things' and automated online check-ins to retail locations are technological innovations in the immediate future that will have a direct influence on the way the public and businesses use online services and, in turn, the way that we as an industry investigate and research those users.

One of the major blocks to online intelligence gathering is when the device user sets their security settings to private. Retailers are quickly developing incentives that actively encourage and reward a user for switching from secure private settings to a public setting. This assists retailers in several ways, not least a vast amount of data that will provide personal shopping preferences for a customer, which creates opportunities to enhance a customers shopping experience and to 'feed' similar products of interest to the customer. Amazon already adopt this approach and very quickly inundate a customer with '*If you liked this item, you may also like this item'* options. So, if users are incentivised to keep their profiles public, then valuable intelligence will become available.

Given the huge amount of intelligence available, it becomes very challenging for an investigator be an expert in every area. Intelligence gathering and surveillance are two specific areas of expertise and, as the available technology and the ensuing intelligence pool grows

exponentially year on year, it requires a dedicated expert to remain abreast of current and new developments.

The ultimate investigator of the future for the investigation of the type of cases detailed herein may transpire to be a hybrid of the two specific areas. An expert in intelligence gathering on their own personal caseloads, who is also an expert in surveillance, would be an extremely valuable commodity to the investigation industry.

Chapter 9: Conclusions

The subject matter of this thesis was chosen to demonstrate that thorough and effective pre-surveillance intelligence gathering has a positive bearing on the likelihood of the successful outcome of a subsequent surveillance operation.

Although the two investigative disciplines discussed herein, namely online intelligence gathering and surveillance, are distinct areas of specialist expertise, they are inextricably linked and both serve the same ultimate purpose. To gather intelligence and evidence in relation to the subject of an ongoing enquiry.

Pre-surveillance intelligence gathers the information remotely and the resultant findings affect the way that surveillance is undertaken. In turn, fresh intelligence gathered in real time by the surveillance team during the course of the direct, physical observations can serve not only to corroborate the evidential integrity of the original intelligence provided but also to create new lines of enquiry.

The rapid growth of social media monitoring platforms is clear evidence that this intelligence is of value to law enforcement agencies and private investigators and it is apparent that intelligence gathering technology solutions will continue to be developed.

All investigators have a duty of care to their clients to undertake the most diligent investigation possible in the most cost-effective manner. Pre-surveillance intelligence allows the client and the surveillance team to make informed decisions regarding the best approach to take to achieve a positive outcome and to determine how to make the best use of the available resources in terms of manpower and budget.

The investigative supplier that adopts pre-surveillance intelligence on instructed cases is maximising the opportunity to instil confidence in their client that they are dealing with surveillance experts. The quality of the surveillance findings and investigative output will have a direct bearing on whether the client continues to use the investigator as a service provider. Pre-surveillance intelligence serves to enhance the reputation of the investigator.

The 21st century investigator would be remiss if they chose to ignore the rich level of intelligence that is readily available to them.

Bibliography

Books and Publications

JENKINS.P. – 'Surveillance Tradecraft'. Intel Publications

PALADIN PRESS – 'The Professionals Guide to Covert Surveillance'. Paladin Press

BAZZELL. M. – 'Resources for Searching and Analysing Information'. CreateSpace

PALMER.D. – 'Tracing – An Investigators Guide'. Institute of Professional Investigators

Online OSINT training courses and resources

Qwarie http://www.uk-osint.net/

IntelTechniques https://inteltechniques.com

Intelligence Gathering Sources

X1 Social Discovery: www.x1.com

Geofeedia: www.geofeedia.com

Media Sonar: www.mediasonar.com

Echosec: www.echosec.net

Facebook: www.facebook.com

Twitter: www.twitter.com

Instagram: www.instagram.com

Pinterest: www.pinterest.com

Strava: www.strava.com

Map My Run: www.mapmyrun.com

Map My Ride: www.mapmyride.com

Mapilary: www.mapilary.com

Dogpile: www.dogpile.com

IxQuick: www.ixquick.com

Pipl: www.pipl.com

ExtractFace: Extractface.codeplex.com

Regulatory sources

Information Commissioners Office (ICO): ico.org.uk

Data Protection Act (DPA): www.gov.uk/data-protection/the-data-protection-act

Regulation of Investigatory Powers Act: www.legislation.gov.uk/ukpga/2000/23/contents