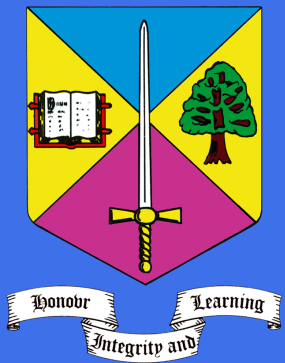


# Open Source Intelligence Course

4th - 5th May 2016



## The Professional Investigator

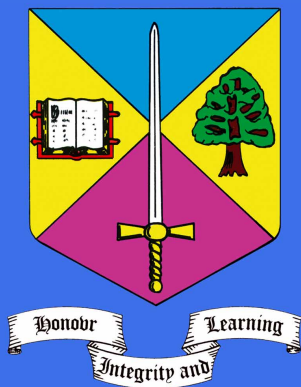
Spring 2016

The Institute of Professional Investigators

IPI  
Jubilee House  
3 The Drive  
Brentwood  
Essex  
CM13 3FR

Tel: 0870 330 8622  
Fax: 0870 3308612  
Email: [admin@ipi.org.uk](mailto:admin@ipi.org.uk)

David Palmer FIPI  
Editor



## Contents

[From the Secretary General ►](#)

[Tracking Devices ►](#)

[Open Source Intelligence & RIPA ►](#)

[Continous Professional Development ►](#)

[SIA Update ►](#)

[Training Warning ►](#)

[BSI Update ►](#)

[Open Source Intelligence Course ►](#)

## Principal's Address



The Board are continuing to work towards further courses that members can apply to complete. One such course will be an Open Source Intelligence Course run at the Civil Service Club. This all depends upon us being able to attract sufficient numbers to make running the course viable. We invite members to let us know if they are interested in attending and once we have sufficient numbers we will then be able to arrange the course and provide details of the cost.

If any member has any suggestions for courses they would like to attend please let the Secretariat know through [adm@ipi.org.uk](mailto:adm@ipi.org.uk) and we will endeavour to run any that are viable.

On another note, Byron Davies MP is continuing to seek confirmation of when or if licencing is to happen. Yet again, an article in the local press in Croydon shows the necessity of licencing, giving details of a private investigator being convicted of criminal offences and being able to rise from the ashes like a phoenix to carry on trading in another company name. The answer to these problems is in the governments hands if only they would pick up the ball and run with it.

We continue to promote and support the introduction of a licensing regime, either through the SIA or any other route if it comes to that. Watch this space!

**James Harrison-Griffiths FIPI**  
**Principal**

# From the Desk of the Secretary General



## ***Subscriptions***

Once again it is time to collect the dues from the members. Thankfully, the Board of Governors have been able to agree that there is no need to increase fees again, this year. I look forward to being able

to report the same in 2017, in which case we will have been in the fortunate position of having held membership fees static since we ceased registration for VAT. While those with VAT registered businesses were unaffected by that decision, individuals have benefited from smaller outlay.

The Board has, however, considered the delay in recovering subscriptions and they, and the AGM participants, all noted the remarkable slowness with which some dues were paid. In other organisations, non-payment results in rapid loss of membership. We, however, appreciate our members and their challenges, and while we are able to keep our heads above water, nothing is certain in life. We also have to factor in the ongoing licensing question. And the potential for the main organisations to start organising self-regulation if and when the SIA finally does its job.

So I would encourage all members to swiftly respond to the receipt of their invoices. Last year I had to send out 33 reminders. That is nearly a quarter of the membership and it is not, with respect, a reflection of the professional organisation that we consider ourselves to be. One of our watchwords is, after all, integrity! Perhaps part of that integrity is answering (correctly) the question, "Have I paid, yet?" This year, members who have not paid after 3 months risk loss of their membership (and having to remove all references to the IPI from their paperwork and publicity materials, which offsets any savings!). Nobody would be sadder about this than me, so please don't let this happen.

## ***Identity Cards***

With your prompt payments, those who wish for an updated ID Card should send their photographs for the very professional looking, but free-to-members card.

## ***Insurance***

The brokers, Kerry London, remain on standby to ensure that your insurance requirements are met. Do not hesitate to contact them, or us, to discuss your needs.

## ***The Information Commissioner***

Hopefully, following my warning, everyone who needs to be is registered under the DPA. The ICO continues to look very hard at private practice

## **The ICO has been worrying about tracker devices on the basis that data from such devices is data within the meaning of the DPA**

investigators, for some reason. Sometimes the ICO concentrates for a period of time on a particular sector, just to see who's doing what. Sometimes, it's less random. I don't know which applies in our case, but it is a fact. The ICO has also been worrying about tracker devices on the basis that data from such devices is data within the meaning of the DPA. Again, reasons unknown. The data is, after all, exactly the same data that a surveillance team would 'see' if the expense was met for 5 people to follow when one tracker could do the work. (See also the article in this issue on that very subject.)

However, the point remains that as we urge licensing by the SIA through the Home Office, it's good if we are all licensed appropriately under the existing legislation. Let's not score an own goal.

I hope all of you are doing well. As I repeatedly say, anything we can do for you, we will. Don't hesitate to contact us whenever you feel we can help.

**Simon Smith** FIPI MSyl(Dip) MIPSAMIFM

# Do **you** use tracking devices?

Members may recall that in late 2014 I reported that the ICO's office had decided that the placement of tracking devices onto a target's vehicle, as it was often a trespass to property, was illegal as the data obtained was obtained unfairly, and therefore unlawfully in terms of the Data Protection Act.

The ABI and IPI argued that such a trespass was a legitimate investigatory method, and to think otherwise meant that not the ICO had summarily decided that not only did RIPA regulate surveillance by the authorities, it actually partially restricted surveillance to the authorities.

On the 9th of February, the Daily Mail reported on a situation which should give rise to some concerns amongst those of you who use tracking devices for private investigations. Two men, a father and son, had used a surveillance device on the father's wife. They were undergoing a divorce and the son wanted to discover where his wife was going and to find out if she was having an affair. The two men were convicted of stalking her, and given community penalties and a restraining order.

One factor that may have influenced the court's conviction was that they told people outside the family 'circle' what they were doing, and those parties told the wife – as did the Police, apparently. She claimed distress, fear and intimidation was caused by her discovering that that she was under surveillance. A surveillance which, incidentally, may have been encouraged by the men's solicitor.

All of which now raises the inevitability of actions being taken against and restrictions being placed on

**A father and son used a surveillance device on the father's wife. The two men were convicted of stalking her, and given community penalties and a restraining order**

private investigators who, in the course of legitimate enquiries, consider surveillance to be justified in the prevailing circumstances. It may also lead to the ICO reinforcing its position.

We watch this situation with interest, but in the meantime remain satisfied that legitimate surveillance is still a necessary tool for the private sector investigator. However, given the change in environment that this case may create, emphasise the advice the Institute has been providing since RIPA was enacted. This is a quote from the IPI Manual:

**"It is the recommendation of the professional bodies in the private sector that investigators pay heed to the intention and objectives (spirit) of RIPA to avoid unnecessary challenge to their investigatory product. This can be achieved by**



using the following mnemonic when planning a surveillance.

**PLAN – Proportionality, Legality (or Lawful), Accountability and Necessity.**

Proportionality – is the surveillance a sledgehammer to crack a nut or is it the only way to obtain the information sought? If not the only way, is it the most effective or cost-effective?

Legality – is the investigation lawful? Are the objectives 2012 it was established the private investigators surveilled MPs and lawyers who were

continued>>

challenging the Murdoch/News International stance on 'blagging' and phone hacking. To be blunt, the surveillance was not illegal but whether it was ethical in the circumstances would be a question asked under this heading.) **(Editor's note: The same level of thought now needs to be given to any potential vulnerabilities of the subject to be surveilled. A woman living alone would have to be 'assessed' differently to a male truck driver who may be scamming a customer, for example.)**

Accountability – in an authority the investigator is accountable to that authority and to law. For the private investigator they are essentially accountable to their client – and still, to law. They are liable for any criminal acts or civil torts, just as anyone else would be.

Necessity – is the surveillance necessary to obtain information? If you know someone goes to work every day using the same route, then surveillance carried out every day, with the same result, would not be necessary. Part of the planning includes narrowing down the time and geographical considerations. (As you can see there is a cross-over between Proportionality and Necessity.)

Utilising the **PLAN** mnemonic, if nothing else, absolutely underpins the motive behind the intended

surveillance, and identifies what consideration was given to alternative methods of achieving the operational intention.

All that said, it would be interesting to receive the opinions of those IPI members' and their associates on this situation, and how they intend to combat it. Email [ipitrain@aol.com](mailto:ipitrain@aol.com) with your views, please.



# Open Source Intelligence – Do You Need RIPA?

While the ICO is wringing his hands with glee over the tracking device issue, in what one may consider to be further interference with legitimate investigation, the Surveillance Commissioner has entered the fray in respect of open-source intelligence gathering by those authorities to whom RIPA applies.

I do not want to spread doom and gloom, but this is something about which investigators who conduct enquiries for such authorities should know.

Hitherto, the view was that information obtained through 'open-source' routes was fair game. It was out there, on t'Internet, placed there (usually) by the subject under investigation and therefore (arguably) public domain.

At this point let me distinguish between two routes to finding this data. First of all, there is 'truly' public stuff. This may be accessed by you, the investigator, using your own real internet identity, without necessarily alerting the subject to your interest. So David Palmer accessing Facebook publicly in order to investigate Neil Smith (a pointless exercise given his expertise!) is not and never could require a RIPA authority/approach. This open-source data remains free to use, but **ONLY** if you aren't hiding. It is open source data obtained overtly.

Unfortunately, as reported in Professional Security magazine, the Commissioner has taken a view about when an investigator uses a false identity to search sites like Facebook – because at that point a covert method is being used, even though the data being mined is public. The SC has 'decided' that Facebook entries (as an example only) available to the public

**This open-source data remains free to use,  
but ONLY if you are not hiding. It is open  
source data obtained overtly**

nevertheless derive from a level of expectation that some privacy and ownership still lies with the poster. Notwithstanding the poster's expectation of privacy, the potential for collateral intrusion on data submitted by friends of the poster means that the RIPA considerations apply IF a covert identity is being used by the investigator.

The SC stated: "Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remains of the view that the repeated viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation (*by anyone but the press? My italics, Ed.*) should be considered within the context of the protection that RIPA provides to such activity."

Note that the SC takes this view while the debate apparently continues.

This means that information available to the 'real' David Palmer is not available to his alter-ego

'David Marple' without RIPA criteria being applied – but remember, this only applies to 'authority' investigations. PI Marple can still do what he likes for a private client BUT – and here's the big BUT – how long that remains so, and what approach a court may take when hearing a matter in which social media data was obtained through stealth, remains something to be answered as time goes by.

Views, please, to [ipitrain@aol.com](mailto:ipitrain@aol.com)

# Continuous Professional Development

## How do you do yours? If you do any at all!

Bye Law 18 of the Institute states:

### 18. CONTINUOUS PROFESSIONAL DEVELOPMENT (CPD)

(i). All UK based members of the Institute with less than 9 years' membership will, having joined on or after 1 January 1997, be required to accumulate and prove a total of 25 CPD points per 3-year period, that proof to be submitted with membership renewal.

(ii) Points will be accumulated at the following rates:

Attendance at a one day Seminar presented by the Institute - **10 points**

OR

Attendance at other approved training functions (per day) - **5 points**

OR

Presenting a lecture/paper (minimum 1 hour) at an approved

Seminar/Conference - **15 points**

OR

Authorship of an acceptable educational text on an investigator  
subject published in a recognised Journal (per 1,000 words) - **5 points, max. 15 points**



**To be frank, the only person the  
editor knows is 'doing' CDP is  
himself**

To be frank, the only person the editor knows is 'doing' CDP is himself. The IPI has not pursued recording of Members' CPD points, mainly because despite the occasional request and reminder that you (a) tell us what you have done – and you haven't - and (b) the lack of CPD-addressed articles sent to the Journal, the failure to 'do' CPD could only really have one or two penalties for the errant investigator

and those penalties would not engender compliance so much as resignation.

Nevertheless, the Institute, as a PROFESSIONAL body, encourages and indeed expects the taking of action that ensures that a professional investigator remains up to speed on legislative and operational developments that are relevant to her or his particular field.

continued>>

Any activity that leads to new learning is CPD – thus states the Chartered Institute of Legal Executives, and that's as good a definition as any. This means that CPD is easily obtainable, even if just through the purchase and reading of a magazine or book on a relevant subject. Such an easy approach is not necessarily desirable, but it is, at least, something. On the job training (for those employed and lucky enough to get it) is better, but researching and writing an article (a thesis, perchance?) is even better. It requires thought, application, deliberation and discussion.

And CPD need not be solely focused just on 'investigation. CPD can just as easily be obtained in

respect of skills such as general computer usage, business and management theory, leadership, and so on.

I'd gamble that most of my IPI colleagues do something in respect of CPD, even if they do so by accident as a situation demands. But here's another point.

If you learn something valuable, could you please pass that information on to your professional body so that the rest of us can benefit while marvelling at your professional acumen? Thank you.

**This means that CPD is easily obtainable, even if just through the purchase and reading of a magazine or book on a relevant subject. Such an easy approach is not necessarily desirable, but it is, at least, something**



## SIA Update

### Great News... **Not!**

The following has been received by the ABI from Peter Selwyn-Smith of the SIA.

“Hi Eric

The information about the Home Office review is available on our web site:

<http://www.sia.homeoffice.gov.uk/Pages/sia-review.aspx>

The position on licensing Private Investigators is as I set out below – if the review outcome is that we should license the sector we will be pleased to work with partners to find an acceptable system to do so. It would be inappropriate for us to say anything further at this stage. When the review reports (there isn't a set time, but we would expect it to be by the end of the calendar year) I will be happy to engage further with you and your members.

I appreciate your desire to keep your membership informed, but this is as far as we can go at the moment.

I wish you all the best

Peter”

In other words, a consultation that took a month to 6 weeks is going to take 10 months to analyse before anyone ventures to make a decision about whether or not PIs shall be licenced, and then the suggestion is that the whole sorry process might be undertaken again.

Meanwhile, congratulations to the SIA on a detailed, 20-page corporate plan published before the review result (eh?), which doesn't mention PIs; and on their holding a 'diversity declaration' launch on the 11th of March.

Again – **NOT**.

**A consultation that took a month to 6 weeks is going to take 10 months to analyse before anyone ventures to make a decision**



# Training – Take Care!

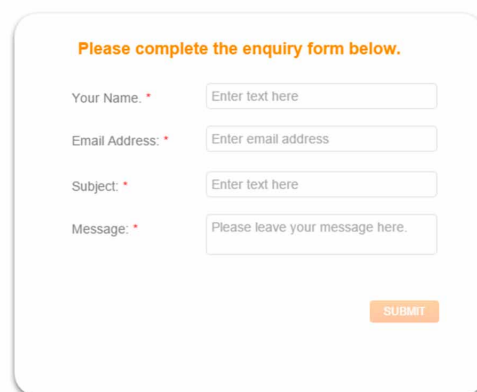
The Institute and other reputable associations have long been concerned that the onset of licensing has inevitably resulted in the creation of a multitude of training offerings, as indicated in the last issue.

The latest addition to the plethora of companies that have come to our attention has resulted in this article, which adds to our ad hoc 'Guide to NOT Getting Defrauded'. It is, if you like, a reminder of the common fraud identifiers otherwise listed in these pages in earlier issues, but nevertheless bears repeating (and placement on our website front pages). An IPI Member recently identified "a company", which contacted him about training. Here, for us, were the markers for suspicion.

**1.** A Skype telephone number - always iffy. While possession of a Skype number isn't illegal, and geographical numbers are no longer worth the paper upon which they are written, a Skype number leading to nothing more than an email address means no immediate ability to access the true details of the subscriber laying claim to the business. That would require a RIPA application (authorities) or a Court Order. Because telecom companies aren't interested in protecting the public, only themselves and their money. (Did I say that out loud .....?)

**2.** Website – when I dealt in Fraud, a key commonality with the fraudulent companies' websites was the bit where YOU entered YOUR

contact details and 'they'd get back to you'. They had no meaningful contact details on the site, if any. Like this:



**3.** An impressive looking address, in this case 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ. Addresses like these are invariably accommodation addresses even if they do exist, and more often than not they use the same address for the Director, which means apart from a slot in the wall you have no immediate connection to a checkable name/address. Always iffy. ALWAYS Google the address without the company name, and see just how many plumbers, florists, accountants, electricians etc. work from that building. Do a Google Maps Street View and wonder at how they must all get their works vans through the front door. Look at

this pic – indications are that 12,131 companies work from there..... Oil and Gas, Scandinavian Homes, a pine warehouse (bit of a squeeze), another home furnishings company, umpteen consultancies, lawyers, and so on.

Quick Google - <http://www.gardenstudios.com/>



**The NEW Centre of Investigatory Excellence?**

Again – not illegal in itself – but why? WHY? Why have a business address that is NOT your place of business, unless the only other address you have is your home? (And even then, why miles away? And at a cost?)

continued>>

**4.** ICO and Company Registration – often at the same accommodation address, and therefore equally useless as a guide to probity. These days, so much can be done online without identity and probity being properly and objectively checked it makes a lot of sense to treat entries with some disdain.

**5.** They will EITHER claim you don't need a formal qualification OR will claim an accreditation, which should be checkable. If the former, and licensing comes in, you have to pay twice. Duh. In this case, the company was not accredited by IQ Limited, and never have been, as they claimed at the time our member contacted me.

**6.** Prices are usually way higher than the IPI and ABI. And while some place a syllabus list on the website, you have no idea of the amount, or quality, of the materials – or whether they've pinched it from someone else.

**7.** A training company that 'guarantees work' is lily-gilding at best, lying at worst. In our experience. Also claiming access to a special network is complete fluff. There is a network. It's called The Yellow Pages and costs nothing.

**8.** The name of the company director and/or staff should be checked against the IPI, ABI, WAPI, WAD and CII. If they aren't members of a legitimate

organisation you'd have to ask yourself - why not? In this case, there were no salient links to investigation work evident.

In a nutshell - If someone comes to you and asks about training, please make your recommendations based on this article and send them to your Institute. In a similar vein, read <http://www.croydonadvertiser.co.uk/Croydon-Advertiser-expos-perfect-example-private/story-28745573-detail/story.htm> for an example of (a) why we need licensing and (b) what rubbish police will say to avoid investigating these frauds.

Believe it or not, we then recruited a student, who paid up, then took the manual and demanded a refund. We looked into the name provided and identified a website with exactly the same hallmarks as I have listed above – except they didn't even bother with the Skype phone number. They just didn't bother with any contact details at all. We have sent them this:

“Sir, as a professional investigator I am intrigued as to why your website contains all the hallmarks of a fraudulent enterprise: no faculty details, no names at all, a 'contact us' page but no contact details. Your company address is evidently an accommodation facility, and you seem to have set up in the last couple of weeks. Are you P\*\*\*\* T\*\*\*\*\* the Twitter account holder, L\*\*\* M\*\*\*\*\* the

company director, or H\*\*\*\*\* Z\*\*\* the resident at C\*\*\*\*\* R\*\*\*? Do you have a course or will you be using ours? In which case, we would respectfully suggest you don't. Suffice to say that in the absence of some proof as to your probity the IPI will consider passing your details to all contacts and Trading Standards.”

They replied to our Principal James Harrison-Griffiths within 24 hours, swore they had no intention of using our material despite having NO investigative background of their own to support their delivery of any qualified course, and that the website was published by mistake. They closed their limited company and the site started emptying itself of content.

Something good was done. Something the SIA could do for us IF they got their .....s into gear.

# BSI 102000-2013



The Institute remains a member of the British Standards Institute 'GW3' committee, aka Private Security and Management' Committee, which oversees the drafting of security related standards, their public consultations and ultimate publication.

The Institute was one of the consulted parties in respect of BSI 102000-2013, the 'Code of Practice for the Provision of Investigatory Services'. As the BSI has a standard 5-year review cycle the Standard is not due for review until at least 2018.

As you can imagine, there are many sectors which BSI deals with, and there is a huge opportunity for overlap between sectors - to make up an example, the Transport sector may have an overlap with the customer services sector. This means that when a Code or Standard is created that can and should be influenced by different overarching sectors, a decision has to be made as to where it will sit, and be overseen, in terms of a committee such as GW3. Without going into detail, a situation has arisen of that nature where investigators in another sector, who were not aware of BSI 102000, have proposed a sector- and situationally-specific new investigatory Standard be drawn up. It has also been proposed that a Standard be drawn up in respect of Open-Source Intelligence.

The Institute's current position in respect of the former proposal is that whatever the rationale and ultimate purpose of an investigation, the

**There is a desire on our part to ensure that 102000 remains the over arching, one-stop investigation 'shop'**

investigatory process remains 'as it is', in terms of (for example) the SIA-accepted core competencies, i.e. an incident, event or suspicion occurs, witnesses are interviewed, evidence is collected and analysed, conclusions are drawn and the result reported. There is greater detail in terms of specifics, but if we were to explore that we would end up with (expensive) Standards for all kinds of interviews, exhibit handling, cyber/photographic evidence gathering – if we had time the list would start to equal the 169-item list of 'investigations' supplied to the SIA in 2002. Imagine a Standard for investigations into missing pets?

In any event, there is a desire on our part to ensure that 102000 remains the overarching, one-stop investigation 'shop'.

The position in respect of a Standard for OSI is less pressing as the proposer has yet to make a

case. In broad terms the Institute's position would remain that OSINT is an investigatory process and would (like specialist investigations) come under 102000, but OSINT is used outside the sector, e.g. in journalism, so the alternative view may be that a separate Standard is called for.

An alternative – which is viable but heavily work-intensive – would be to create Annexes to the main Standard. But the question would then be – how long is a piece of string? How many specialisms would need to be Annexed? How big would BSI 102000 eventually get, and how much would it cost the applicant for BSI accreditation?

***The Board would be interested in hearing the views of members on these points. Please forward responses to [ipitrain@aol.com](mailto:ipitrain@aol.com) as soon as possible.***

# Open Source Intelligence Course

Civil Service Club, London  
4th - 5th May 2016

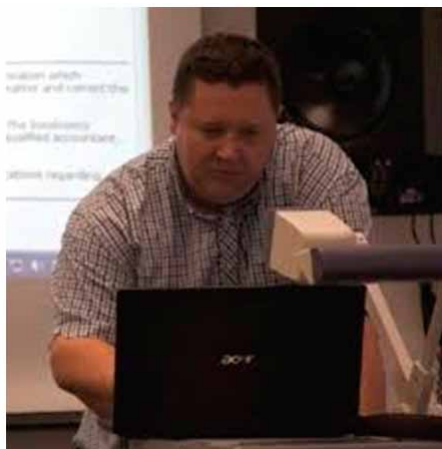
The Institute is pleased to announce that it in partnership with Neil Smith of UK-OSINT, ([www.uk-osint.net](http://www.uk-osint.net)) it will be holding a two-day Open Source Intelligence Course at The Civil Service Club, London on the 4th and 5th of May 2016.

The course will include detailed input on Utilising Search Engines and Social Media Investigation, with practical exercises that will allow participants to learn 'hands-on' how to investigate people and their activities (and location!) through their laptop, tablet – even on their phone.

Anyone who has attended an input from Neil will know just how good he is at what he will teach YOU, and just how useful what he teaches will be in your investigations.

Further details will be circulated shortly, but be aware that the Board (who will be paying as individuals, I assure you) are already filling up the seats!

The cost of this course is **£200** (no VAT payable), but you will be responsible for your own accommodation. The venue is easily accessed from Charing Cross so hotels outside the expensive city centre are highly recommended.



Neil Smith of UK-OSINT





# The Professional Investigator

Institute of Professional Investigators  
Jubilee House  
3 The Drive  
Brentwood  
Essex  
CM13 3FR

Tel: 0870 330 8622  
Fax: 0870 3308612  
Email: [admin@ipi.org.uk](mailto:admin@ipi.org.uk)