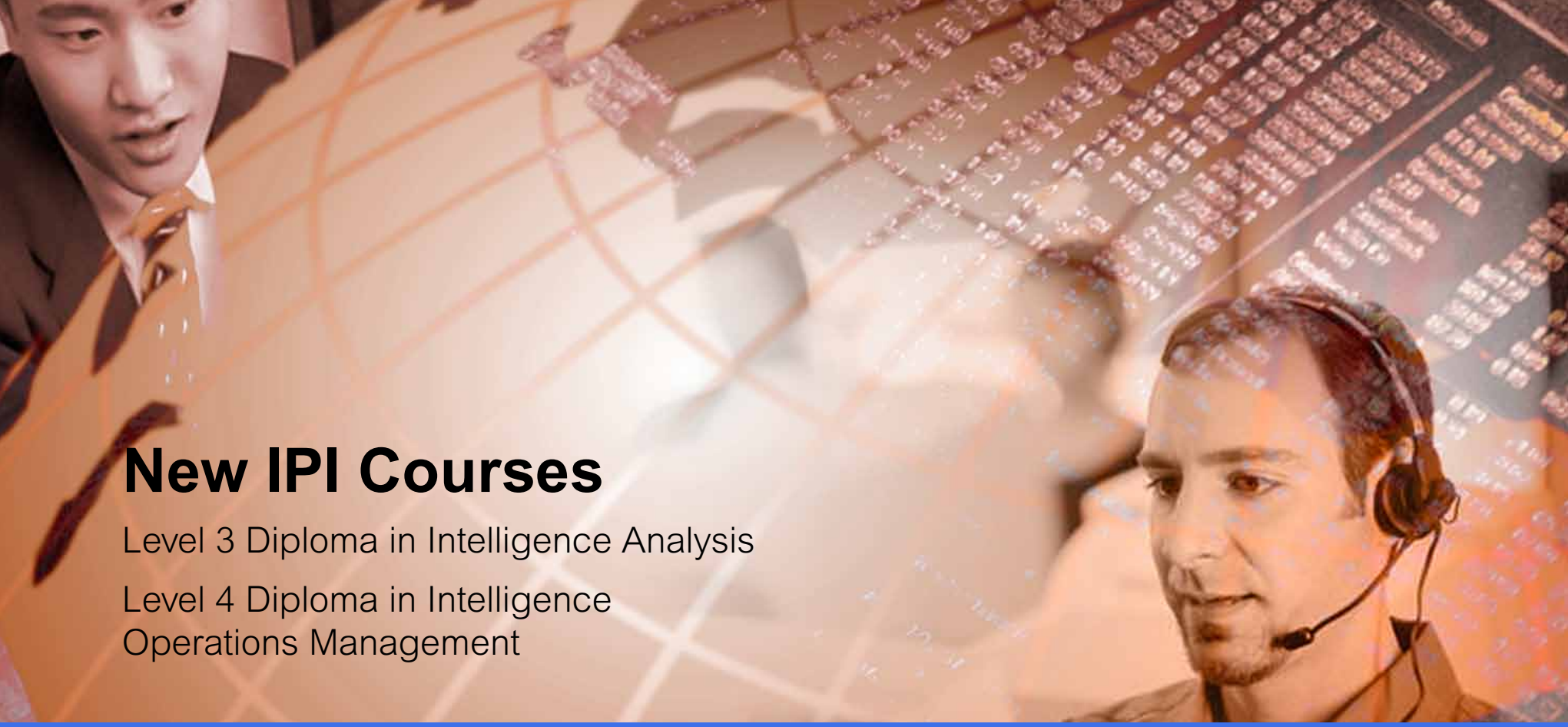


New IPI Courses

Level 3 Diploma in Intelligence Analysis

Level 4 Diploma in Intelligence Operations Management

The Professional Investigator

Spring 2018

FULL SCREEN

The Institute of Professional Investigators

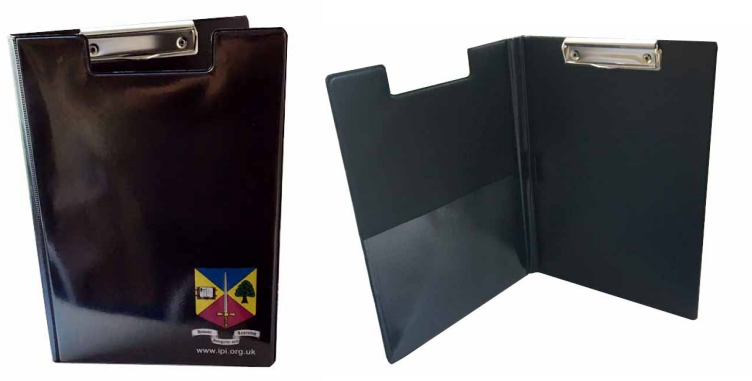
IPI
Jubilee House
3 The Drive
Brentwood
Essex
CM13 3FR

Tel: 0870 330 8622
Fax: 0870 3308612
Email: admin@ipi.org.uk

David Palmer FIPI
Editor

Contents

IPI Wallets and Folders for Sale



The Institute has wallets and folders for sale.

Wallets for ID cards at **£6.00 each**. They are made of Chelsea leather, with a discreet logo. They are very practical for our ID cards and Oyster cards etc.

Clipboards at **£7.00 each** (pictured above). They are folding and open to reveal the clip on the right and the perspex on the left. You can put instructions, letters of authorisation or, for the Bailiffs amongst us, Warrants of Distress, under the perspex, so people cannot grab them to tear them up

If you are interested in either of these items please contact the Institute admin@ipi.org.uk

New Board Meets First Time!

Your new Board of Governors met for the first time in the 21st of February, in London, and a read of this edition of the journal will make it plain that discussions resulted in quite a lot of interesting discussion and decision-making.

Rather than reiterate everything that was discussed we leave a lot of it to be discovered in the following pages, so we encourage a deep dive into the sea that is Mare Investigataris Professionale* for some exciting revelations about future initiatives.

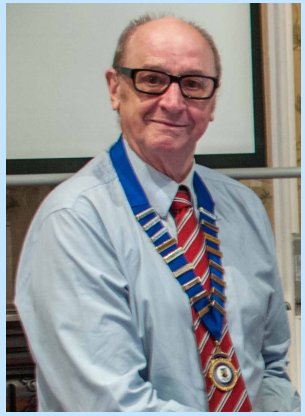
Oh, one other thing – subscriptions will remain unchanged for another year.

*(*Completely made up words.)*

Life Memberships Awarded

It gives the Board great pleasure to announce that your Immediate Past Principal James Harrison-Griffiths FIPI, and your retiring Secretary-General Simon Smith FIPI, have been awarded Life Membership of the Institute of Professional Investigators for their valued assistance in maintaining the status and health of the Institute over many years.

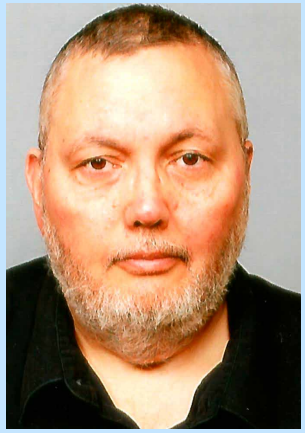
James not only acted as Principal but also did a lot of work in making the Distance Learning Course a formerly accredited product, in representing the Institute with the media and in training investigators at our pre-examination Refresher Courses.



James Harrison-Griffiths FIPI

Simon, for his part, managed the affairs, liaison, publicity and finances of the Institute to the degree that we went from borderline insolvency to having a healthy bank balance, due in no small part to the very small amount of salary he took from us for doing so. He maintained that level of service through some very challenging personal times and that did not go unnoticed.

While formally retired, both gentlemen have stated their intent to continue assisting the Institute in whatever way they can. Happy retirement, gentlemen!



Simon Smith FIPI

IPI Launches NEW Qualifications

The Institute – YOUR Institute, is proud to acknowledge the work of Board Member Stephen Langley MIPI LLB (Hons)(Open) MSc CECI MCMI in the creation of a new Course for delivery by the Institute.

The awarding organisation for both qualifications is ProQual Awarding Body and the regulatory body is the Office of Qualifications and Examinations Regulation (Ofqual).

Both courses are being prepared with distance learning and face-to-face training delivery methods in mind.

The Level 3 Diploma in Intelligence Analysis
The Level 3 Diploma in Intelligence Analysis is aimed at candidates working in an intelligence analysis role and provides them with a nationally recognised qualification to demonstrate competence.

Individuals will gain advanced competencies in:

- In-depth understanding of the intelligence cycle
- Comprehensive understanding of collection methods and capabilities
- Understanding of audit trails relating to intelligence analysis
- An understanding of the security and intelligence handling requirements relating to national legislation
- Detailed analytical techniques training (theory and practical) – to include link analysis, analysis of competing hypothesis, cone of plausibility, backcasting and SWOT analysis

Both courses are being prepared with distance learning and face-to-face training delivery methods in mind.

- Additional analytical techniques training as required by the candidate's role
- The ability to create and disseminate products or reports based on the results of data analysis
- Training will also focus on developing the ability to effectively disseminate intelligence

Level 4 Diploma in Intelligence Operations Management
The Level 4 Diploma in Intelligence Operations will aid the development of strong analytical and presentation skills which are required for work in Intelligence Operations, which involves comprehensively collecting and collating data from a wide range of sources in order to provide detailed assessments.

Candidates will gain advanced competencies in intelligence analysis to support decision making, including:

- In-depth understanding of the intelligence cycle
- Comprehensive understanding of collection methods, collection planning and intelligence capabilities

continued ▶

- Understanding of audit trails relating to intelligence analysis
- An understanding of the security and intelligence handling requirements relating to national legislation
- Detailed analytical techniques training (theory and practical) – to include link analysis, analysis of competing hypothesis, cone of plausibility, backcasting and SWOT analysis
- The ability to create and disseminate products or reports based on the results of data analysis and to specific customer requirements
- Training will also focus on developing the ability to effectively disseminate intelligence
- Training in the formation of assessments and recommendations to support organisational goals
- Additional analytical techniques training as required by the candidate's role

If you would like more information on either of these courses please contact the Institute ***courses@ipi.org.uk***

Change of Accreditation for The IPI Distance Learning Course 'Level III Award in Investigations'.

Subject to confirmation, the IPI will shortly be changing Awarding Body certification from IQ Ltd to ProQual. Our relationship with IQ has been excellent but the time has come to 'change ship' and the current contract was due to end in June of this year

This has come about in order for us to change the manner in which the students are assessed from a multiple-choice examination held in

The assessment process can be carried out without the need to travel or take an examination

London to an Assessment Process which can be carried out without the need to travel or take an examination. This process will involve the completion of a portfolio of 'evidence', allied to a Skype or personal interview with an Assessor to check the knowledge of the student. We are advised that this new method will be acceptable to the SIA in the event of licensing.

Current students will be advised that they can take the IQ examination by the end of June, or they can wait until after the current IQ contract expires and take the alternative qualification.

Principal Represents Institute at International Level

Following an invitation from a representative of the Institute to attend a two-day conference, I travelled to Kiev on 18th October 2017 and attended the 2nd International Congress of Private Detectives

By Brendan Tolan MIPI, Principal

The conference was attended by 234 delegates from Eastern European countries.

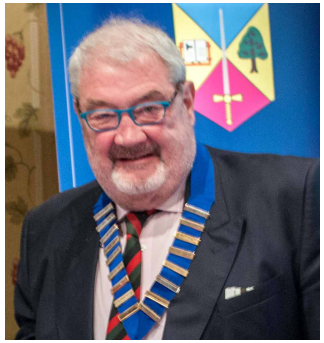
On the first day, I was tasked to talk to Congress on “From school desk to Detective work”. Basically, the progression via distance learning to practical investigations within the private industry.

The talk gave the delegates an insight into the Institute’s “Distance Learning” Package, examination and subsequent application process to join the Institute as a Full or Associate Member.

It transpires that ALL investigations undertaken within the Ukraine (and a number of other Eastern European countries) are illegal although tolerated by the government.

Members of the Congress, together with local politicians, were working together to put the Private Investigation industry on a legal footing and regulated by Parliament (sounds familiar?). Unlike the UK, the road to regulation was well advanced and expected to be enshrined in law later this year – 2018.

The vast majority of those attending had little command of English, and my knowledge of Ukraine was even less, thus in the event discussions, during breaks and subsequent Gala Dinner, were limited.



It transpires that all investigations undertaken within the Ukraine are illegal although tolerated by the government

The Congress continued the following day during which my contribution was to talk on UK legislation relating to use of video camera footage, both covert and overt, in evidence. Also, the deployment and use of tracking and bugging devices.

I believe my attendance and contribution to the Congress was well received, despite my talks, followed by Q & A sessions, being assisted by use of interpreters.

All in all, a useful invitation which may well be extended in the future.

British Standards Institution – Update on BSI 102000 Review

For the BSI 102000-2013 Review Panel, the Deputy Principal asked the panel to review the Data Protection Act 1998 for the purposes of deciding what pre-employment screening checks were justified. This is an edited version of the report that was submitted. The result of the panel's deliberations from the 22nd of February will be at the end of the article – if it made any.

BSI 10200-2013 – Data Protection/Integrity Checks. In response to Chris Brogan's very reasonable suggestion that we review the DPA as a way of discovering, understanding and interpreting the Act so as to justify any decision to include some of the questioned elements of the BSI-102000 (and possibly 7858) vetting section, I obtained and reviewed a copy of the Act, which I believe should be up to date as it was downloaded from the Legislation.gov.uk website in entirety and should, one would expect, be a wholly amended version.

The objective of the research was to address the one question which vexes us, which is whether the vetting recommendations are fair and legal. Therefore, my research is focused on the obtaining and retention of the personal data of an applicant for an investigatory/security post.

To clarify the basis for the following statements, and respectful of Chris' request that the whole Act be reviewed, my considerations were:

a) Legal interpretation. Statutes should be read in 'order' of presentation, and any impact to one section on another should be made clear in the text.

b) In the absence of such a reference, a section can be interpreted in and of itself.

The objective of the research was to address the one question which vexes us, which is whether the vetting recommendations are fair and legal

c) the following sections were read but NOT considered relevant in my review.

i) Ss 7-15 as they applied to subject access rights and we are not considering them.

ii) Ss16-26 as these relate to the powers of the OIC.

iii) Part V as this related to enforcement.

Interpretation of the Act

The following are my observations:

1. For the purpose of vetting procedures, the employer will be the Data Controller. They want the data, they obtain the data either directly or through an employee or contracted Data Processor, and they will use the data. (S.1(1))
2. Personal Data includes opinion about a subject, which would imply that references obtained about an applicant may include personal data, notwithstanding any factual information disclosed in the reference. (S1(1))

continued ▶

3. Sensitive personal data includes information about the ethnic or racial origin of a data subject; information relating to their physical or mental health or condition; the commission or alleged commission of offences, and details of any proceedings or disposals in such proceedings relating to such commission. (S.2)

Therefore, it is accepted that CURRENT vetting procedures routinely involve the obtaining of personal data AND sensitive personal data in our sector.

4. The 8 Data Principles, which most relevantly include the First Principle that Data should be obtained (etc) fairly and lawfully, are all encompassing. Adherence to the First Principle is done through compliance with the conditions in Schedules 2 (all data) and 3 (sensitive data). Schedule 4 states where the 8th Principle is not subject to Schedules 2 and 3 but this relates to transfers out of the UK and is not overly relevant.

5. It is the First Principle which the committee is trying to address. I have the following observations:

    a. Schedule 1, Part 2 S.1(2) states that data is fairly obtained if it is obtained from a person who is authorised under any enactment to supply it (etc.) I suggest that this includes any data obtained from a body such as the insolvency register and the courts. **I suggest it is fairly obtained 'by definition'.**

    b. Section 2 then goes on to address processing of data provided by the subject or obtained through other routes. Schedule 1, Part 2 S.2.1(a) states that data is processed fairly if it is obtained from the data subject when said subject is aware of the identity of the controller, the purposes of the intended use of their data, and any additional relevant circumstances in which the data will be processed. If it is NOT obtained from the data subject it is processed fairly if they are made aware of the information required by S.2.3. **There is no reference to informed or 'free' consent in this section other than being informed about these specific facts, but I will return to this later.**

Moving on to Schedule 2 and general personal data.

As stated earlier, data is processed fairly if only one of the 6 conditions apply.

6. First is consent. **An applicant is consenting by definition, and this is routinely compliant with Sch 1 Part 2 S1 above.**

7. Second is that the processing is necessary for the performance of a contract to which the subject is party, or when the subject requests steps be taken to allow them to enter into that contract. **As we are talking of an employment contract or contract for services, this condition can also apply.**

8. Third is that the processing is required for compliance with any legal obligation other than contract. **I do not see an obvious exemption here.**

9. Fourth is to protect the vital interests of the subject. **I do not see an obvious exemption here, but I imagine there may be some.**

10. Fifth relates to the administration of justice, exercise of statutory function and any public function. **I do not see an obvious exemption here except for the SIA in the event of licensing.**

11. Sixth is the one most likely to be of relevance. This allows for processing which is necessary for the purposes of the legitimate interests of the data controller (employer) or by those to whom the data may be disclosed, except where unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the subject. **It can reasonably be argued that an employer in this sector needs to assess an applicant as to honesty and integrity. This MUST be viewed in the light of Leveson and HASC observations unless or until there is a stated case that dictates otherwise. I also refer to SRA/Law Society/CILEX declarations as to prior conduct, which I assume are considered to be lawful because of the bodies that implement them.**

continued ▶

Schedule 3, and sensitive personal data (SPD).

12. First condition. SPD is obtained lawfully if the subject has given explicit consent, an important distinction and extension from the informed consent mentioned in Sch 2. **By providing a DBS Certificate, an applicant demonstrates consent – however, Chris' question about free consent remains unanswered by this condition. Post-licensing the question may be moot.**

13. Second condition relates to exercise of a right or obligation imposed by law, perhaps only relevant to specific contracts with public bodies.

14. Third condition is that processing is necessary to protect the vital (undefined!) interests of the data subject or other person where consent cannot be given by the subject or the data controller cannot reasonably be expected to obtain that consent or in order to protect the vital interests of another person where subject consent has been unreasonably withheld. This may justify the obtaining of SPD, insofar as criminal convictions may reasonably be seen as a potential threat to the interests of employer or client. In terms of medical consents, it could be argued that the question can be asked because of the risks represented if a specific disability threatens the health and safety of others, e.g. eyesight (driving, surveillance), hearing (surveillance), mobility (all sorts). In addition, Article 8 of the GDPR includes: (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

15. The fourth condition relates to non-profit bodies and is excluded subject to the observations of others.

16. The fifth condition applies if the data subject has made the data public of their own volition.

17. The sixth and seventh conditions appear to parallel Ss29 and 35 of the Act **and therefore are unlikely to apply to the vetting process, except if legal advice may be required as to the risks/legalities of employing or not employing the subject.**

18. The 8th condition relates to processing by a health professional or someone with equivalent confidentiality 'rules'.

19. The 9th condition relates only to racial/ethnicity data and is allowed for ensuring equality regulations are monitored.

Other Issues

Other exemptions exist which would only apply in cases of national security (S.28).

S.31 relates to exemptions applicable in the public interest exercised by persons (legal persons) who have powers conferred by law, in the main, but also 'any other function which is of a public nature and is exercised in the public interest'. **I would not profess to extend that exemption to general private sector work except where public body contracts may apply. I would also argue that this exemption may apply in terms of regulated bodies such as banks and insurers.**

S.56 appears to be an anomaly, at least as far as it has been applied to the security industry. It states, quite clearly and without reference to any other condition that a person, in connection with recruitment, continued employment, or a contract for services, cannot be required to supply or produce a 'relevant record', except where permitted by law OR where the circumstances show that the imposition was justified as being in the public interest (rarely defined). To cut a long story short, a relevant record includes a conviction record and (I believe) health records. **This means that an employer needs to justify requesting and using a conviction record in the recruitment/vetting process. It cannot be 'routine'. Nor can it be a**

continued ▶

condition of employment/contract that such a record be provided. Note that this applies to a requirement that the subject provides it, and not to the data controller discovering that data legitimately off his own back. (Article 10 of the GDPR seems to absolutely prohibit non-governmental conviction processing.)

Observations

Chris' concerns, in the main, relate to obtaining data 'in general' (including consent issues) and the obtaining and use of data that can be brought under the heading of Integrity Checks.

The DPA does not address, on the face of it, 'freedom of consent', something about which Chris Brogan is concerned. His point is that if a negative consequence exists that means consent is effectively given under duress (sic), it is not consent. As stated above, the Act does not make such a reference.

In a submission to BSI in/around 2012, Chris used as his authority The Article 29 Working Body, which 'has taken the view that where as a necessary (my italics) and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment."

Chris himself stated that this was an opinion, but since then GDPR has been finalised and comes into effect next year.

Article 7 states:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The 4th paragraph is relevant to Chris' observation.

In my assessment, it is as clear as mud, in that it says that the issue of 'free' consent will only be 'taken into account' when deciding whether or not the personal data processed was relevant to the contract – and it does not bar its use, it only states it will be taken into account. However, for our purposes, if we interpret this 'consent' through the Act, my prior observations on consent must apply. It is 'free' if the data controller provides the statutorily listed information. If we further interpret the Article through the expectations of investigation employers and clients, consent is trumped by the Schedule 2 conditions.

In any case, data provided by consent is obtained fairly.

In relation to integrity checks, Chris is concerned that obtaining CCJ data is unlawful. For the reasons stated in paragraph 5.a above, I respectfully suggest that the obtaining of such data from a public body authorised to provide it is, by virtue of the words of that section, automatically fair. I would extend that summation to any publicly authorised data source.

As for processing, data provided by consent or obtained through other means is fairly processed if the subject is made aware of the identity of the controller, and the purposes (and sometimes the how) of the processing. This is or should be routinely catered for in the consent section of application forms, and the standard may need to be amended to mention that.

continued ▶

Finally, a brief look at GDPR seems to indicate a 'compatibility' with the 1998 Act and therefore the above arguments may be 'future proof'.

Conclusions

I therefore submit that the current BSI section on employment screening be allowed to stand subject to semantic adjustment, with the possible rewording of 5.1.1 as to the provision by a prospective employee of a conviction certificate, which apparently needs to be justified.

End of Report

RESULT OF DELIBERATIONS:

The Panel re-convened on the 22nd of February 2018. After the written submission was made to the panel three members appeared to support it, and one did not. At the meeting itself, the clauses which caused so much debate were reviewed and with one exception the recommendations were accepted, and the relevant clause was adopted and so the use of CCJs as a reasonable enquiry remained. There were some amendments in other sub-clauses which clarified the use of criminal record disclosure and the different vetting levels expected to apply to an investigator, as opposed to other non-investigatory staff whose vetting levels would be lower but still BS 7858 compliant.

A valiant attempt by your Deputy Principal to have BS 7858 included in BSI 102000 (to save you £100) failed.

It would be prudent for all to read the consultation document and comment on it, whether those comments are favourable or otherwise

The Standard will now go out for public consultation, which may well give rise to even more debate. Further debate is welcomed because it will result in a broader perspective which the Panel may not have considered.

While the Deputy Principal's ego welcomed the support of the majority of the Panel, the ultimate objective of the review will be to get the Standard right. In due course members will be advised on how to comment on the Standard's revision. **In light of the remaining objection and the esteemed gentleman's openly stated (and accepted) intent to seek support for his view, it would be prudent for all to read the consultation document and comment on it - whether those comments are favourable or otherwise.**

Additional Course to be Produced by Your Institute

The IPI has started development on a stand-alone course on Time Management. The basis for the Course will be the book 'Police Time Management' by the Deputy Principal, and course income will be split equally between him, our IT provider, and the Institute itself.

IPI Course income is a (the?) major source of funds for the Institute and we believe that the continued provision of courses related to our sector enables us to absolutely comply with the original and continuing mission of the Institute to develop better investigators. An announcement will be made when that Course becomes available. It will not be supported by a formal qualification but completion will result in the issue of an Institute Certificate.

GDPR and Private Investigators

Chris Booth of Palatine Group, well known in the industry as a fervent pursuer of data beneficial to investigators, is running a GDPR 'Group' of interested parties. In February, he advised that group that Roger Bescoby, from Conflict International, had posed some valid and pertinent questions to the ICO, and Timothy Morgan from the ICO (Lead Policy Officer, Policy & Engagement (Private and Third Sector) had responded as below.

Chris wrote: "Mr Morgan expresses some "opinions" on the DPA/GDPR which we think are wrong and before we reply to him, I wondered whether anybody has any comments or queries that they may like to be raised. I was planning to reply to him on behalf of the group.

I will of course provide a draft copy of the intended reply to those in the group for you to consider, before it goes back – and maybe you can decide then!

Anyone wishing to assist can contact Chris at chris@palatine.co.uk.

For ease of reading, the questions are italicised while Tim's replies are not.

Q. *Can you advise on the "Appropriate technical and organisational" measures Data Controllers will be looking at Processors to have in place?*

A. We can't endorse specific measures to comply with the requirements, but the draft guidance we have published on contracts and liabilities is likely to be helpful.

Q. *What information will suffice, when engaging another Processor, to provide general authorisation to the Controller? For example, some Processors have a USP in that they have built up a reliable and trustworthy list of Processors who they can rely upon in certain circumstances and they do not wish to name these Processors to their client (The Controller).*

The instructing organisation and the private investigators will be joint data controllers as between them they are determining the purpose and manner of processing

A. It's difficult to provide an answer at present, as the forthcoming Data Protection Bill has not been finalised but may provide for these circumstances.

Article 28(3)(h) requires that data processors must provide data controllers with sufficient information that the data controller can demonstrate compliance

My understanding is that the instructing organisation and the private investigators will be joint data controllers (Article 26), as between them they are determining the purpose and manner of processing. Article 28(3)(h) requires that data processors must provide data controllers with sufficient information that the data controller can demonstrate compliance. In the case of joint controllers where one employs a processor, it is unclear how the other data controller could demonstrate compliance without knowing the identity of the processor. In the event that the private investigator data controller ceased trading, it's also unclear how the processor could return/delete personal data under Article 28(3)(g) at the end of the investigation.

It would be worthwhile considering if third parties that the private investigator hires are in fact data processors, or if they will also be data controllers in respect of the investigative work. If the third party would be a field worker who would decide what data to collect or prepares reports for the private investigator, then they seem likely to be a data controller in their own right, as they would determine the manner of processing. In that situation, there

continued ▶

is scope to consider if they may be a joint data controller, and information about them would need to be made available to individuals in accordance with Article 26(2).

As we discussed in our previous emails, it's unlikely that private investigators would be data processors in most cases. However, if a private investigator were to be a data processor, and if the third party were also a processor, then the private investigator would be required to inform the instructing company of which processors they had engaged in order to comply with Article 28(2).

Q. *It is a matter of genuine concern to Investigators that full contact details of a network of protected individual contacts and intellectual property providers that have been built up over a lifetime would need to be divulged to our instructing clients. Such disclosure could become significantly damaging to our businesses if our clients decide to 'go direct' for instance. It could never be in the legitimate interests of our businesses for such disclosure to be required in every instance.*

A. While I appreciate your point, I should clarify that the legitimate interests condition is a basis for processing personal data, rather than a factor in compliance with the data controller/processor relationship. If a data controller subcontracts to a data processor, then it will need to be done in compliance with the requirements of the GDPR. It may be worthwhile considering if there would be scope for managing the participation of third parties in the contract between the instructing organisation and private investigation company.

Q. *Do you have any suggestions how we may work around this? We have considered we could give general notice upon acknowledgement that we may instruct 3rd party Processors but will only engage from a list of Law Society endorsed ABI members for instance?*

A. Naturally, as the regulator, we can't provide a way to 'work around' legal obligations. The requirements around a general notice that data processors may be engaged are set out in Article 28(2). As above, it may be worthwhile considering whether the contract between the investigator and the instructing organisation might provide an avenue for setting out the relationships between the parties.

Q. *I am aware of the ICO's understanding of 'collateral intrusion', particularly in surveillance matters. Can you advise whether under GDPR such similar tolerance will be applied to non surveillance cases (i.e. status enquiries, pre sue litigation asset location checks etc) where it becomes relevant, pertinent and justifiable to report upon the activities of other third party individuals during that report? These may be spouses, family members or co Directors etc who's relevance and activity would be identified and considered of legitimate interest to the core enquiry.*

A. 'Collateral intrusion' is not a term appearing in either the Data Protection Act 1998 or the GDPR. If a private investigator is processing an individual's personal data, then they will need to be able to justify that processing. If a private investigator records personal data about an individual's friends, family, and associates, they will need to consider what their basis for processing that data is under Article 6, and how to provide transparency information under Article 13. If seeking to rely on the legitimate interests basis under Article 6(1)(f), then the private investigator will need to balance the individual's legitimate interests against their own legitimate interests.

It's worthwhile considering whether special category data would be collected about these third parties. If it is central to the investigation, such as a person visiting their extramarital lover during an investigation in to alleged infidelity, then the investigator will also need to consider what Article 9 condition might be met. If it is incidental to the case, such as an individual accompanying their parent to a medical appointment, then it may be worthwhile to consider whether the data needs to be recorded at all.

Q. *When an investigator is deemed a Data Controller by an instructing Solicitor, and the investigator receives a subject access request, on what grounds can the investigator decline? Could the investigator decline on the same 'legal privilege' grounds as a Solicitor? I ask this question as I anticipate SARs will be a frequently utilised tactic by opposers in litigated cases. Could the investigator be exploited as a 'back door' route to gaining access to legitimate enquiries where* ***solicitors have legitimately declined?***

continued ▶

A. In most cases, private investigators will not be able to claim legal professional privilege in response to a subject access request. However, if an investigator is instructed by a solicitor, and if the information would be subject to litigation privilege if requested from the solicitor directly, then it **might apply for that specific case, as long as litigation privilege applies.**

Q. *With regards to data retention, we propose to use the following paragraph at the foot of all reports going out to clients:-*

"Data Protection - GDPR

Please assist us in complying with our GDPR obligations by advising as and when this matter becomes settled and or completed. Upon such notification, we will then ensure that all data created in this matter is destroyed and that the data is not retained for any longer than is necessary, as is required under the Act. If we are not advised, we reserve the right to destroy all data contained in this report after a period of (3?) years. Please advise if you have any alternative or specific requests with regards to the retention of this data."

Please can you comment as to whether this is an acceptable request to make?

A. It seems likely that retention periods might be included in the contract between the instructing company and the private investigator. However, it seems sensible to have a policy in place in the event that a relationship breaks down or retention cannot be discussed. Some consideration would need to be given to whether the data needs to be held at all. If an investigation has concluded and the investigator has provided the personal data to the instructing company, and the instructing company has confirmed receipt, then it's not immediately apparent why the investigator would need to continue to hold the data at all.

If an investigator chose to continue to hold data for that time, they would need to be able to demonstrate that it was necessary to do so in relation to their lawful basis for processing under Article 6

Three years seems a long time to hold personal data if there is no clear reason to do so. If an investigator chose to continue to hold data for that time, they would need to be able to demonstrate that it was necessary to do so in relation to their lawful basis for processing under Article 6. It may be that for different investigations, different retention periods are appropriate.

Q. *Further, does the paragraph 'stand up' whether we are Data Controllers and or Data Processors?*

A. I can't comment on whether this would be appropriate to all agreements, as I may not be able to envisage all the circumstances where an organisation would engage a private investigator.

Disclosure and the Courts

No professional investigator will have missed the repeated news articles surrounding the properly-founded collapse of several rape trials, where the police have failed to disclose material that would have assisted the defence, a requirement under the Criminal Procedures and Investigations Act 1996.

However, as a professional investigator more than familiar with the disclosure provisions as a result of being the only Disclosure Officer on the biggest murder investigation ever conducted in my area, and in connection with some large-scale fraud investigations, I consider myself to be sufficiently experienced as to have an opinion which I hope is reasonably objective.

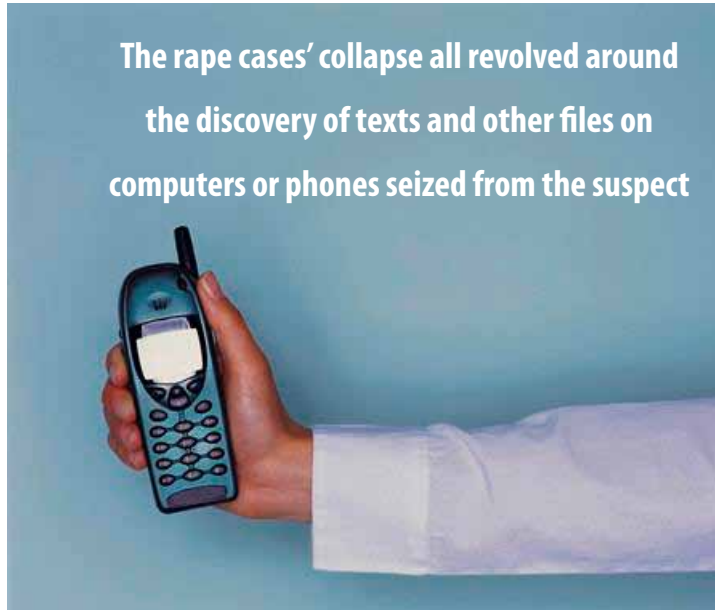
For anyone shut in a room and unable to access the news, the rape cases' collapse all revolved around the discovery of texts and other files on computers or phones seized from the suspect, which the defence can fairly state – given the law - should have been discovered by the investigators.

But let me pause here for a second. Note that the Act came in 22 years ago. I recall that my own telephone was probably a Nokia 3310, with no internet access. Facebook was launched in 2004 (I was surprised to read). Other social media platforms came into common usage after that. So, the ability and willingness of subscribers to such facilities were in their infancy when the Act was imposed upon investigators. Everything that was 'discovered' by investigators up until that Act – and be realistic, it was what had happened before that caused it to be drafted, not what the legislators expected would happen later – was probably on paper or was recorded on paper.

22 years on, almost everything discoverable is in digital form. People are familiar with, and ardent users of social media and computers. They film stuff at the drop of a hat and they communicate through Facebook, Messenger, Snapchat, WhatsApp, text, Skype and who knows what else. Whereas in 1996 even CCTV was something that could be collected in an hour from the one shop that had it, it is expected that all retail outlets and many residential premises have CCTV. Not to mention passing cars and their dashcams. And, of course, a lot of simple business is digitally recorded.

So, consider that for a moment. If you arrest a suspect (or defend a client) for something where you can reasonably expect a phone or computer's content to have relevance, you seize/obtain it. Obviously, you search it for relevant evidence, and you are also obliged to look for anything which undermines/assists the parties to a trial.

An example. A colleague seized a phone and was, after these trial issues, told to look at all the content, and also 'told' by the CPS that it wasn't unreasonable (a relevant word under said Act) to look. And it was suggested somewhere that keyword



searches were not allowed. (I'm paraphrasing, but that was the message.)

He counted the files for me, and I calculated that if he looked at each text/video/picture for 1 second, and took no breaks, it would take about half a day. Two seconds, a day. Four seconds, two days. The length of a 1-minute video – well, you can imagine.

continued ▶

For a fraud, you'd have to reach each piece of digital paper in entirety.

And, of course, that is the only case the officer has going on, isn't it? Three rapes, three times the work. To be blunt, finding a phone or Facebook account with two messages on it is rare. And we haven't addressed the use of the Cloud, either. Just for perspective, a common laptop has 1TB of memory available. It is estimated that 85,899,345 pages of Word documents would fill one terabyte. It could contain 30 hours of HD video, or 500 hours of less detailed footage. Or 310,000 images. I agree that it is unlikely that any seized device would be so full but let your own experience temper your own calculations.

Asking an investigator to read everything and banning keyword use is ridiculous. It is untenable in terms of work patterns, skill-sets and any other measure you can think of. Guess what – the police don't have a department just looking at phones, and if it did it would have to know the case sufficiently in order to make the disclosure assessments. And it would have to be paid for.

The point I am making here is that the Act was not designed with the digital explosion in mind and is therefore no longer fit for purpose. Its objectives are perfectly valid, and I am in no way suggesting it is 'wrong law'. It is just being re-interpreted in a way that often can no longer be reasonably be applied. It must be looked at in a way that makes it usable.

Which brings me on to the second issue for me, one

The Act was not designed with the digital explosion in mind and is therefore no longer fit for purpose

which is exemplified by the rape trials themselves, and relates to what I consider to be an obvious question I heard no-one ask in the media I saw or read.

In the three cases described, content was found on the defendants' phones (I understand). So, the question in these cases must be:

Whose phone was it, and didn't the defendant say that the content that would help them was present?*

I am not a defence lawyer, but surely their obligation to provide the best defence for their client should include their asking their client if such material exists, and to then suggest to the investigators where it can be found? Doesn't the caution cover defences? Of course, in these cases they may well have complied with that suggestion and therefore the police will be manifestly at fault, I don't know. The press missed that question and the police didn't answer it, either.

Asking an investigator to read everything and banning keyword use is ridiculous. It is untenable in terms of work patterns, skill-sets and any other measure you can think of

(Sudden thought – an abject defence failure like that might be a good reason to sue the defence for the costs of proceedings. Moving on….)

I do know, from experience, that defence lawyers will befuddle and perplex with irrelevant demands for disclosure of material the police don't possess and which they could get all by their lonesome. This undermines their professionalism and ethics to my mind, but that is another article. Very often, and respect where it is due, they do a damned fine job and find things which justify their fees, which an investigator may not have considered – if only because they are not experts in anything. For example, I once asked a witness something like, "I don't know your systems and procedures or the laws and practices which govern them as well as you do, so you're going to have to do some work for me." Is it not unreasonable to ask the defence to apply their expertise?

All of which brings me to the Act. I suggest that it be amended by someone far cleverer than me in such a way as to add a defence responsibility to search for material that will assist their defence, and to declare what efforts they have made. Defence lawyers are officers of the Court and should have a reasonable duty to do their bit in the disclosure process. (I draw the line at their having to seek material to assist the prosecution, but it's a thought!)

Perhaps a police disclosure would take place first,

continued ▶

following which the defence could do theirs – I leave the practicality of any processes to those clever minds. I do know that such a process is catered for in civil cases, where the consequences of miscarriages are primarily financial rather than penal.

This would increase the likelihood of discovery of defences in cases of the type mentioned, result in people not being charged when inappropriate to do so, lessen the burden in terms of time on a police service that is 80% or less than it was in 1996, and stop wasting everybody's time.

I'd be interested in your thoughts.

***Update.** It transpired that the phone that was inefficiently analysed was, in fact, the victim's phone and that the messages were NOT between victim and suspect, a natural filter for a keyword or time-based search. This raised the follow-up question as to what power the police had to seize and examine the phone, and since there is none (unless specific criteria applied), and the only practical route is consent, what happens when a victim does not consent to handing over their phone – will the CPS stop prosecuting rapes where the victim exercises their right to privacy and elects not to hand over their phone? Another article in itself, and one which I am not prepared to write just now.

Private Police Force - Concerns Raised

Rebecca Camber, Crime Correspondent For The Daily Mail, reported in February that a private police force, paid for by resident's in the area patrolled, was investigating and prosecuting crimes more successfully than the local police service. Their investigations included three murders, which is worrying, and other crimes such as stalking, burglaries and rape. They've also investigated cases of reported missing persons.

She reported that TMEye, run by former senior Met officers, had successfully prosecuted 400 criminals, although how many of these were formal court proceedings is unclear. That said, 43 have gone to prison so their success rate is pretty impressive.

Prosecutions are funded by costs awards from the courts, which is therefore not a cost borne by the client. TMEye use all the technical facilities that are available to police services, too. Their hope is to encourage local authorities to outsource some policing services to them.

This has raised concerns with the regulars, naturally.

Camber wrote, "Metropolitan Police Federation chairman Ken Marsh described the rise of private detectives as a 'staggering indictment' of the state of policing. Eventually there will be a two-tier system with the haves and the have-nots, and if you have money and live in a £20 million house in Chelsea you can pay for private security,' he said. 'My concern would be, where is the public scrutiny if it goes wrong? If they are allowed to go and do police's job for them, that is a dangerous status quo.'"

Further concerns around managerial oversight, accountability and recourse in the event of misconduct were also raised, although it might be argued in return that civil recourse is always available, as a re criminal sanctions, the investigation of which would not presumably, allow some of the protections enjoyed by regular officers when they are investigated. (As for a hierarchy, most serving officers would argue that outside operational oversight, manager's task is to slow people up and increase paperwork requirements. Ed)

It will be interesting to see if future events add fuel to the licensing fire – these staff are conducting what would be licensable activity under the PSI Act if implemented, and they are already doing so in terms of their patrol duties.

Read the full story: http://www.dailymail.co.uk/news/article-5346699/First-private-police-force-caught-400-criminals.html#ixzz5655JwWWN

ID Fraud Reaches Epidemic Levels

By John Bateman MIPI

Identity theft and in particular 'on line' versions of it, has rocketed to 'epidemic' levels with possibly up to 500 frauds a day! – it is feared that the 'Hire industry' are a soft target as their systems and procedures are not robust enough to prevent, detect or reduce the possibilities of being a victim.

Furthermore, and traditionally, the 'Hire Industry' have suffered a lack of interest from the Police when they report a loss or suspicious event because the force will often blame it on a 'poor business transaction' rather than the reality that dishonesty, fraud or deception has taken place at the point of hire.

Usually the 'Hire Company' does not have the time, resources or expertise available to 'investigate' the matter themselves or gather enough evidence to show to the police that the documents produced or methods used to 'Hire' the property are in fact fraudulent and therefore it is NOT a bad business deal. Even if the Company push the matter and gather the appropriate data or proof, then the offence will probably be recorded just with 'Action Fraud' (launched in October 2009), be lost within this system and never be truly investigated and / or ever be detected!!

The Hire Company will then 'write off' the loss and inevitably this 'shrinkage' will find itself being passed onto the good, loyal and paying customers.

The Hire Companies staff are often not trained to spot the illegal applications – particular the 'on line' ones ... where they are repeatedly being 'hit' by the same offenders

The Hire Companies staff are often NOT trained to spot the illegal applications – particular the 'on line' ones - and as importantly see a pattern where they are repeatedly being 'hit' by the same offenders because they are dealing with such volume and probably not able to spot the forged driving licence, passport or other forms of fraudulent ID, which are scanned in and so easily manipulated so as to look genuine.

Equally one Hire Company is not readily sharing the information about the offender(s) with ANOTHER Hire Company i.e. their competitor because this is not how the industry works and yet P&D Investigations Limited has set up a Forum of Hire Companies AND a 'warning system' where they can make other members aware of the rogue names / businesses etc, attempting and / or succeeding in obtaining property by deception from them and yet this is so easy, with a simple circulation by email.

Like so many preventative measures it is impossible to know exactly how many attempts or successes you have stopped but with the police doing less, the

commercial world HAS to be savvy and develop its own methods to disrupt or stop the villains!

Criminals are making fortunes by using victims' personal details to apply for loans or buy goods online and other scams – the police show little concern as the number of events are so high and their resources cannot cope and yet the cost of identity fraud in 2016, was estimated at £5.4 billion.

New research by the fraud prevention body Cifas reveals that 89,201 ID frauds were registered in the UK from January to June this year (2017) and the figure is 5% UP on the same period in 2016, with the vast majority of crimes committed via the internet.

Cifas says that the criminals are "relentless" in targeting consumers and businesses – they have called for more to be done to protect personal data. Fraudsters are able to easily get hold of information such as names, dates of birth and addresses through a variety of routes including companies house, stolen mail, hacking or using information victims posts on social media.

The chief executive of Cifas, Mr. Simon DUKES, said: "We have seen identity fraud attempts increase year on year, now reaching epidemic levels. These frauds are taking place almost exclusively online and the vast amounts of personal data that is available either online or through data breaches, is only making it easier for the fraudster.

"..... for smaller and medium-sized businesses in particular, they must focus on educating staff on good cyber security behaviours and raise awareness of the social engineering techniques employed by fraudsters"

"We have seen identity fraud attempts increase year on year, now reaching epidemic levels. These frauds are taking place almost exclusively online"

In the majority of scams, fraudsters assume a victims' identity to buy or hire a product or take out a loan in their name. Then people or businesses often do not even realise that they have been targeted, until a bill arrives for items they did not buy or hire or they have problems with their credit rating.

As an example in Greater London alone, in past 5 months only (researched in Sept 17):

Cheque, Plastic Card & Online Bank Accounts (not PSP*)	4318
Other Fraud (not covered elsewhere)	3174
Application Fraud (excluding Mortgages)	2039
Online Shopping and Auctions	1953
Telecom Industry Fraud (Misuse of Contracts)	1739

*PSP = Payment Service Providers

By John BATEMAN MIPI
P&D INVESTIGATIONS LIMITED

Are PIs only for the Rich and Famous?

From Ron Harrison, Surelock

A question I was recently asked "Are private investigators only hired by the rich and famous?" and my answer "Absolutely no, not at all!"

In this day of ever stretching resources, private investigators certainly fill a very important gap in many different areas. We are experts in our field, qualified, accredited and professional but with something a little bit special, we are approachable. I've chatted to people who just want to tell someone that something awful has happened to them and get some direction of how to deal with it. Sometimes it's just that old saying of a problem shared.

There are companies that know they are losing money through fraudulent activities but just don't know where to start unravelling and making sense of what is taking place, how to prevent it happening in the future or putting a package of evidence together to obtain the desired outcome. That's when we are more valuable than you could have envisaged, and absolutely worth thinking about.

Known for tenacity! We have assisted in many a court case where just that extra search provided the evidence that swung the case in the client's favour, saving the possibility of huge costs awarded against them. There is something quite rewarding in knowing you are right and succeeding in proving it, sometimes you just need the help of someone who

knows which direction to channel the investigation to prove that fact for you.

Budgets get cut and the thought of hiring a private investigator may feel hard to justify but what if "ghost workers" are your scary thought? You'll be amazed how often it takes place and how easy it is to task us to prove their existence for your company. Ultimately an investigation could save you more than money in the long run; a company's reputation is often priceless.

Unfortunately, it is a sad fact that sometimes the police just don't have resources to find the evidence needed to classify a crime as worthy of investigation. That is where we can make a major difference. We can investigate and package the necessary evidence that makes that crime committed against you or your company one which shows there is evidence supporting the crime classification and the eventual outcome may be the difference of a prosecution.

Health and safety audits can be put into place to check workers are adhering to company policy, how much can that save you in a court case? We have experience of regular checks with various companies where we report back failures and successes. Look at the bigger picture of what can be achieved; sometimes a pat on the back will keep that workforce you have trained, happy and content, sometimes it can save a life. Again, that's priceless.

Peace of mind is sometimes invaluable. Surveillance can be performed to give you peace of mind, to prove something or to negate something, remember its values are endless. Our eyes and ears become your eyes and ears. Pictures save a thousand words – that could be a strapline!

So, how long is that piece of string? I'm not saying rich and famous are not welcome, but don't ever let it think you are not worthy of our services because you are not rich and famous!

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