THE GOVERNMENT RESPONSE TO THE FOURTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION 2012-13 HC 100

Private Investigators

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

July 2013

Cm 8691 £6.25

THE GOVERNMENT RESPONSE TO THE FOURTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION 2012-13 HC 100

Private Investigators

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

July 2013

Cm 8691 £6.25

Any enquiries regarding this publication should be sent to us at:

SIA Policy & Sponsorship Team
Safeguarding & Public Protection Unit
Home Office
4th Floor
Fry Building
2 Marsham Street
London
SW1P 4DF

This publication is also available for download at www.gov.uk/home-office

ISBN: 9780101869126

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2579696 07/13 32420 19585

Printed on paper containing 75% recycled fibre content minimum.

Opening statement

This Command Paper is published in response to the Home Affairs Select Committee's Fourth Report of Session 2012-13 entitled: 'Private Investigators': HC100, which was published on 6 July 2012.

The Home Affairs Select Committee conducted an inquiry into the role of private investigators, and the risks of an unregulated sector. The Committee made a number of useful suggestions, including the statutory regulation of the private investigations sector. The Government's full response to the Committee has pended following the Government's ongoing consideration of the Leveson Inquiry, as explained by the Home Secretary in her letter of 16 October 2012.

The Government can confirm its intention to regulate the activities of private investigators by requiring them to be licensed by the Security Industry Authority. It will then become a criminal offence to undertake private investigations without a licence, which would only be issued following satisfactory criminality and identity checks, and competency-based training. Furthermore, it will become a criminal offence to breach the conditions of a licence for private investigation, as per section 9(4) of the Private Security Industry Act 2001 (PSIA).

It is the Government's intention that the regulation of the private investigations sector would be rolled-out from the autumn of 2014. The Government provides full responses to the Committee's conclusions and recommendations below.

The role of the private investigator

Bolstering law-enforcement

Recommendation 1 (Paragraph 15)

The business of private investigators is essentially the gathering and reporting of information, with a premium paid for information that is more difficult to obtain, confidential or important to the buyer. They undertake tasks that are important to an individual and to a business and often fulfil an important social role. In future, it is possible that increasing numbers of investigations that are now undertaken by police will fall to private investigators, though whether this is desirable is a matter for further debate.

Recommendation 2 (Paragraph 16)

In its response to this Report, we recommend the Government sets out its assessment of which policing roles could appropriately be undertaken by private investigators and which should not; how it believes cuts to police funding will affect the involvement of private investigators in law-enforcement; and what part private investigators will have in the new landscape of policing. In particular, given the evidence we received, it will be important that this assessment includes an analysis of the role of private investigators in fraud detection, recovery of stolen goods, maintenance of public order and major investigations, such as murder inquiries, with a statement of the risks associated with the involvement of private investigators in each of these areas.

Decisions about engaging the private sector are matters for the locally elected Police and Crime Commissioners to take, in conjunction with Chief Constables.

However, we have made clear that there is no intention to allow private companies to carry out police activities which require warranted powers, except to the extent that has already been achieved for detention and escort officers by the Police Reform Act 2002, legislation passed under the previous Government. Therefore private companies, such as those who deploy private investigators, will not be able to carry out police activities which require warranted powers.

It is up to the police to decide the best way to achieve transformation in order to maintain and improve services for the public as they face the challenge of reduced budgets. We support the police in considering the value of the private sector to achieving this. The private sector has the skills to drive more efficiency in policing, delivering some services better and at lower cost.

The risks of unregulated investigation

A market in information

Recommendation 3 (Paragraph 26)

Easy access to information poses a double risk. Personal data is easier than ever to access and a private profile of a person can be built from a desktop. The ease of access has also opened the information market to new and unscrupulous suppliers, who may not be registered with the Information Commissioner and are unlikely to understand the rules under which they ought to operate. Phone-hacking appears to be the tip of the iceberg of a substantial black market in personal information. This is facilitated by the easy availability of tracking and digital monitoring devices at very little cost.

The Committee makes an important point. In recent years there have been numerous technological developments, notably the expansion of the internet and the emergence of social media networks, which have seen changes to the ways that personal data is handled and processed. With the ease with which data can now be processed and shared we agree that it is important that there are up to date rules and guidelines in place to ensure that data is used appropriately.

The Data Protection Act 1998 (DPA) requires every organisation or person who has overall responsibility for deciding how computerised personal data is used, stored or otherwise processed to register with the Information Commissioner (unless they are specifically exempt). The flat-rate annual notification fee of £35 covers the majority of organisations, although a higher fee of £500 is paid by data controllers with a turnover of £25.9 million and 250 or more members of staff (or public authorities with 250 or more members of staff). The ICO issues extensive guidance on notification, which is available on its website. Failure to notify is a criminal offence and could lead to a fine of up to £5,000 in a Magistrates' Court, or unlimited fines in the Crown Court. The Committee will be aware that the fines available to Magistrates for these offences will be unlimited in the future after commencement of section 85 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012.

Commercial companies can legally access data relating to individuals in a number of ways, for example by obtaining it from the electoral register. The sharing of personal data is governed principally by the DPA, but the requirements of the Human Rights Act 1998 and administrative law are relevant as well. The purpose of the DPA is to ensure that the handling of personal data, including disclosing it to third parties, is conducted in a lawful and proportionate manner, with appropriate safeguards in place. This does not mean that personal data should never be shared or disclosed, but it means that, where it is, the legal framework provides an appropriate degree of protection to individuals' information that is sufficiently flexible to respond to the different circumstances in which data may be shared.

For those that are uncomfortable with what data others hold about them or the way in which it is shared they can raise the matter with the Information Commissioner's

Office, who will advise on the legality of data sharing and take such action as he sees fit as the independent regulator of the DPA.

Involvement in the justice system

Recommendation 4 (Paragraph 29)

We were very surprised that the Minister responsible for regulation of the private security industry had not even read the report of the Serious Organised Crime Agency on private investigators. The Government should set out a strategy on mitigating the risks posed by private investigators as soon as the Minister has read and reflected on the report.

We can confirm that the (then) Home Office Parliamentary Under Secretary of State for Equalities and Criminal Information, Lynne Featherstone MP, appeared before the Committee to give oral evidence on 22 May 2012, and she subsequently reviewed the report of the Serious Organised Crime Agency. Our strategy for mitigating the risks posed by private investigators is detailed in our response to the Committee's recommendation 11.

Recommendation 5 (Paragraph 35)

In order to garner "premium" information that commands the highest prices, we heard troubling allegations that private investigators maintain close links with contacts in public service roles, such as the police forces. These links appear to go beyond one-off contacts and therefore to constitute an unacknowledged, but deep-rooted intertwining of a private and unregulated industry with our police forces. The Independent Police Complaints Commission should take a direct control over investigations in cases alleging police corruption.

The National Policing Counter Corruption Advisory Group provides oversight and governance of force anti-corruption units.

Police forces and Police and Crime Commissioners are required by law to refer complaints or conduct matters to the Independent Police Complaints Commission (IPCC) if the allegation includes serious corruption. This includes any attempt to pervert the course of justice and passing on confidential information in return for payment or other benefits.

The IPCC has made work on police corruption a priority for the past three years. The IPCC report 'Corruption in the police in England and Wales: Second report – a report based on the IPCC's experience from 2008-2011' concluded that corruption in the police is not widespread, or considered to be widespread, but that where it exists it is corrosive of the public trust that is at the heart of policing. The Government welcomes the IPCC's commitment in the report to tightening up current

arrangements for rooting out and dealing with allegations of police corruption and to conducting an increased number of independent investigations into corruption cases.

The Police (Complaints and Conduct) Act 2012 gave the IPCC further powers to interview officers and reinvestigate matters previously investigated by the Police Complaints Authority. In addition to this, the Anti-social Behaviour, Crime and Policing Bill currently before Parliament will confer on the IPCC five new powers to: extend their remit to include contractors; obtain information from third parties; require responses to their recommendations; assume certain powers set out in PACE codes; and, direct unsatisfactory performance procedures measures after a death or serious injury investigation.

On 12 February, the Home Secretary made a statement to Parliament which outlined a package of measures to improve police integrity, including equipping the IPCC to investigate independently all serious and sensitive allegations. We are working closely with the IPCC, the police and other partners in planning the implementation of these measures. They will make a significant and positive contribution to the ongoing programme of police reform and to further professionalisation of policing.

The remedies

Data offences

Recommendation 6 (Paragraph 41)

Personal privacy would be better protected by closer working between the Information Commissioner, the Chief Surveillance Commissioner and the Interception of Communications Commissioner. We recommend that the Government aim, before the end of the next Parliament, to co-locate the three Commissioners in shared offices and introduce a statutory requirement for them to cooperate on cases where both the Data Protection Act and the Regulation of Investigatory Powers Act are relevant. In the longer term, consideration should be given to merging the three offices into a single Office of the Information and Privacy Commissioner.

The Commissioners already work closely together. The Information Commissioner has been working closely with the Chief Surveillance Commissioner and the Interception of Communications Commissioner (ICC) to ensure a common understanding on the responsibilities of all three Commissioners. The Surveillance Camera Commissioner and the Intelligence Services Commissioner have also been involved. This on-going co-operation will include the new Biometrics Commissioner.

The Commissioners have been co-operating on the production of a ‘roadmap’ – this will clarify the roles and responsibilities of the bodies involved in overseeing legislation concerning surveillance in the United Kingdom. The draft roadmap was submitted to the Joint Committee of the draft Communications Data Bill on 21 August. The roadmap is a work in progress, and it will be updated in light of regulatory developments.

Both the ICC and the Office of Surveillance Commissioners have quite focussed and limited remits. The former reviews warrants for the interception of communications issued by the Security Service and other intercepting agencies. The latter oversees the conduct of covert surveillance and covert human intelligence sources by public authorities. On the other hand, the focus of the Information Commissioner's Office (ICO) is to oversee compliance with the obligations imposed by the DPA and Freedom of Information Act 2000. In the case of the DPA the obligations relating to personal data apply where an individual's personal data is shared or used by an individual or organisation in the UK, other than for transit purposes.

Each Commissioner and their staff work in specialist, technical areas that require extensive knowledge of relevant legislation and procedures. The work they do can often intersect and it is important that the Commissioners work closely together to ensure that overlapping issues are dealt with in the right way. However, the functions are quite distinct and do not duplicate one another.

Since the Home Affairs Select Committee report, both the Joint Committee on the draft Communications Data Bill and Lord Justice Leveson have reported. Similar to the Home Affairs Select Committee, the Joint Committee has made recommendations in respect of rationalising the seven organisations which are currently involved in surveillance (including the three mentioned by the Home Affairs Select Committee). The Joint Committee has proposed a new, unified Surveillance Commission. Meanwhile, Lord Justice Leveson has recommended a fundamental restructure of the governance and powers of the Information Commissioner.

Section 55 offences

Recommendation 7 (Paragraph 46)

Confiscation orders should be sought where a person is convicted of data and privacy offences and has sold the information for profit.

Recommendation 8 (Paragraph 47)

We recommend that the Home Secretary exercise her power under section 77 of the Criminal Justice and Immigration Act 2008 to strengthen the penalties available for offences relating to the unlawful obtaining, disclosure and selling of personal data under section 55 of the Data Protection Act. The current fine – typically around £100 – is derisory. It is simply not an effective deterrent.

We agree that, in the context of the increasing availability and use of personal data by organisations, any misuse of that personal data needs to be treated very seriously. The Information Commissioner and the Committee have pointed out that, in practice, the fines handed down by the Courts for offences committed under section 55 of the Data Protection Act (DPA) are relatively low. The first principle in relation to fines is that they should reflect the seriousness of the offence. However, it is important to emphasise what the Committee acknowledges (at paragraph 43) that these fines must take account of defendants' means; many of the cases cited as

resulting in low fines relate to one-off, opportunistic actions, rather than the persistent, systemic illegal activity which appears to be the subject of the Committee's report.

In relation to the more organised activity carried out by (for example) unscrupulous private investigators, we agree that the use of the Proceeds of Crime Act 2002 is an effective way of depriving offenders of the financial benefits obtained from their criminal conduct. The Committee will also be aware that the fines available to Magistrates for these offences will be unlimited in the future (as they are currently in the Crown Court) after commencement of section 85 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012.

The issue of the penalties available for section 55 offences is being looked at in light of Lord Justice Leveson's Inquiry into the culture, practice and ethics of the press. In his report, published on 29 November 2012, Lord Justice Leveson made a number of recommendations in relation to the existing data protection framework, including a recommendation to introduce custodial sentences for s55 offences and the enhanced public interest defence.

Section 77 of the Criminal Justice Act 2008 creates a power to alter the penalty (which can include a custodial sentence) for the unlawful obtaining of personal data, which is an offence under section 55 of the DPA. Section 78 of the 2008 Act creates a new defence for journalistic, literary or artistic purposes.

These provisions were introduced by Government amendment to the Bill but custodial penalties were not introduced nor the new defence commenced by the previous Government after the Bill received Royal Assent.

Given the potentially far-reaching nature of Lord Justice Leveson's proposals in relation to data protection, in particular for the conduct of responsible investigative journalism, it is the Government's view that the recommendations require careful consideration by a wide audience. It is therefore our intention to conduct a public consultation on the full range of data protection proposals, including the introduction of custodial penalties, which will seek views on their impact and how they might be approached.

The Committee may wish to note that there are a range of offences that cover the misuse of personal data which may be relevant here. The report mentions the Regulation of Investigatory Powers Act 2000, which would apply to a private individual who had unlawfully intercepted communications and unauthorised access to computer material under the Computer Misuse Act 1990 is also relevant to this activity. Both offences carry a maximum penalty of a two year prison sentence. Under the Fraud Act 2006, it is an offence to dishonestly make a false representation (including as to identity) with a view to financial gain, which could cover the activity of "blagging", depending on the circumstances of the case. The maximum sentence is ten years' imprisonment. Bribing another (or being bribed), contrary to the Bribery Act 2010, is an offence which carries a maximum penalty of ten years' imprisonment. Further, a custodial sentence can be imposed for the common law offence of misconduct in public office, which could apply where public officials, such as police officers, were complicit in releasing information illegally to private investigators.

Policing

Recommendation 9 (Paragraph 50)

The Metropolitan Police's system of safeguards for reducing the risks of serving police officers being corrupted by conflicting interests – including declarable associations policies, a register of business interests and a list of incompatible interests – should be standardised across the country. However, these checks alone might not be enough to solve the problem. The Government must act to sever the links between private investigators and the police forces. We recommend that there should be a cooling off period of a minimum of a year between retirement from the police force and working in private investigation. Any contact between police officers and private investigators should be formally recorded by both parties, across all police forces.

The National Policing Counter Corruption Advisory Group is currently actively progressing work on the form of declarable association policies and related preventative measures.

The Police Regulations 2003 set a duty for all police officers to declare any business interest that they may have. It is then for the chief officer to decide whether the business interest is compatible with service as a police officer. The Regulations do not set out the matters that should be taken into account in taking that decision, but relevant factors will include the impact on the officer's impartiality, the impact on the efficiency and effectiveness of the force, the officer's current performance, the seniority of the officer, the impact on the health, safety and wellbeing of the officer, and any equality and diversity issues that arise.

Following the publication of the report 'Without Fear or Favour: A review of police relationships' by Her Majesty's Inspectorate of Constabulary, the Home Secretary asked the Police Advisory Board of England and Wales (PABEW) to consider the guidance for forces when looking at business interests. Consequently the guidance on the management of business interests and additional occupations for police officers and staff has been revised. Although it is not possible to provide a definitive list of occupations incompatible with the role of police officer, the guidance does include a suggested list which encompasses private investigators.

We are currently considering whether it would be appropriate for members of the police to have formal restrictions on employment after leaving the service, and what such measures might entail, particularly as the Leveson report also contained a recommendation to this effect, in connection with employment in the media. As part of this work the Government will consider very carefully the recommendation that any contact between police officers and private investigators be recorded. Furthermore the Government will also consider whether any such restrictions or requirements that are placed on the police should be extended to other agencies with investigative or covert powers and with the potential for contact with private investigators.

The College of Policing has now been established. It is a new police professional body supporting the fight against crime and safeguarding the public by ensuring professionalism in policing. It will set standards to ensure excellence in operational policing – including setting a national policing curriculum, and providing training and promotion standards and guidance. Throughout their careers, officers and staff will have to demonstrate that they meet the relevant standards in order to progress through the profession.

On 12 February, the Home Secretary made a statement to Parliament which outlined a package of measures to improve police integrity, including publishing national registers of gifts and hospitality, interests and second jobs. The College of Policing is now developing these registers, with the aim of promoting consistency of approach between forces and visibility of police practice in this area.

The timetable for action

Recommendation 10 (Paragraph 72)

"Private Investigator" should be a protected title – as in the case of "social worker" – so that nobody could use the term to describe themselves without being subject to regulation.

The activity of private investigations is already defined under schedule 2, paragraph 4(1) of the Private Security Industry Act 2001 (PSIA). It is the Government's intention to enable the Security Industry Authority (SIA) to license private investigators, by designating private investigation activities for the purposes of requiring those undertaking private investigation activities to be required to apply for a licence. It will then become a criminal offence to undertake such activities without a licence, which shall only be issued following satisfactory criminality and identity checks, and competency-based training. The SIA has the power to grant a licence subject to conditions, as well as modifying a licence. Therefore, as the SIA regulates activity rather than professions or job title, it is not necessary to make 'private investigator' a protected title.

Recommendation 11 (Paragraph 73)

We recommend the introduction of a two-tier system of licensing of private investigators and private investigation companies and registration of others undertaking investigative work. Full licensing should apply to individuals operating or employed as full-time investigators and to private investigation companies. Registration should apply to in-house investigation work carried out by employees of companies which are already subject to regulation, such as solicitors and insurance companies. Both should be governed by a new Code of Conduct for Private Investigators, which would also apply to sub-contracted and part-time investigators. A criminal record for breach of section 55 should disqualify individuals from operating as private investigators.

The Government can confirm its intention to lay a designation order to bring into force schedule 2 paragraph 4 of the Private Security Industry Act 2001, to introduce the licensing by the Security Industry Authority (SIA) of individuals involved in the activity of private investigations. As set out in the Home Office's consultation of November 2012 on a future regulatory regime for the private security industry, the Government proposes introducing a phased transition to a business regulation regime.

However, we do not agree with the proposal that there should be a two-tier system of registration and licensing. We believe that the protection of the public requires that all those working in private investigations need to be regulated to the same standards. As with other sectors of the private security industry which are already licensed by the SIA, all workers undertaking licensable activity will need to meet the same standard to receive a licence, and to be included in the SIA's register of licensed individuals. This will apply regardless of whether they work part or full time.

Therefore, the Government does not intend to introduce individual registration (which would require primary legislation) as the SIA already licenses individuals. However, the public would still be protected, as any contractors working on private investigation activity for such in-house companies, whether full or part-time, would be licensed by the SIA.

As part of the SIA's licensing criteria, all private investigators applying for a licence to conduct private investigation activities, would need to attend and successfully complete competency training. Such competency training would require an applicant to have the skills and knowledge to conduct investigations; conduct interviews; search for information and preserve evidence; conduct surveillance; and understand, and work to, relevant laws and standards. Applicants would also be subject to the SIA conducting satisfactory identity and criminality checks. We do not, therefore, agree that there is a need to introduce a Code of Conduct.

We can confirm that a criminal record for breach of section 55 of the Data Protection Act 1998 could prevent an individual from operating as an investigator. This is already included in the SIA's licensing criteria, so the SIA would take this into account when considering any application.

The SIA would retain the right to refuse or revoke licenses of all current or potential private investigators, regardless of employment status. In these circumstances, we do not consider that a separate Code of Conduct would be necessary.

Recommendation 12 (Paragraph 74)

Whereas licensing will impose an additional regulatory burden on the industry, it could also provide the new safeguards necessary to provide some potential benefits. We recommend that the Government analyse the risks and benefits of granting increased access to certain prescribed databases for licensed investigators, in order to facilitate the legitimate pursuit of investigation activities. For example, a licence may confer the right to access the on-line vehicle-keeper database in certain circumstances. It should consider how this would interact with the changes

proposed to data protection laws by the European Commission. The United Kingdom has rightly moved to a situation of information management rather than merely looking at data protection. We also recognise that appropriate sharing of data can prevent crime and contribute significantly to other outcomes that are in the public interest. However, any new access should be carefully monitored.

The Government is in favour of wider data sharing in an appropriate context where it is in the public interest and takes account of the safeguards set out in the existing legislation.

There is no direct interaction between these proposals and the EU's data protection proposals published in January 2012, save that those authorised to share data will be subject to the new framework once it is agreed and implemented. The European Commission believes that technological developments since the existing legislation was agreed in 1995 demand an update of European data protection legal rules for general data processing to bring it in line with 21st century realities of data sharing. In addition, a Directive covering law enforcement is also being negotiated. The Directive, as drafted, would apply only to "competent authorities", such as the police, prosecutors, courts and prisons, whilst the general data protection rules set out in the proposed Regulation [COM(2012)11], would cover the activities of most other data controllers and processors. Once agreed and adopted, the new data protection framework will apply two years from its entry into force. This file is subject to co-decision between the Council of the EU and the European Parliament. Given the legislative process, the earliest this would be implemented would be by 2016, but it may well be later given the complexity of the file and the short timescales until the end of this commission term and European Parliamentary elections in June 2014.

Recommendation 13 (Paragraph 75)

In terms of skills, we are convinced that competency does not ensure conscience. The core of any training regime for investigators ought to be knowledge of the Code of Conduct and the legal constraints that govern the industry. With this in mind, any contravention of data laws should result in the suspension of a licence and prohibition from engaging in investigation activity, linked to meaningful penalties for the worst offences.

Our response to recommendations 7 and 8 make clear that there are already criminal offences relating to the contravention of data protection laws. In line with the changes to the regulation of the private security industry outlined in our response to recommendation 11, we will need to look carefully at how best those offences are factored into any future training and regulation of private investigators. However, there is power in the Private Security Industry Act 2001 for the Security Industry Authority (SIA) to revoke a licence. In deciding whether to revoke a licence, the SIA has to apply its licensing criteria, which includes fit and proper considerations, as well as training and skills considerations, as outlined in our response to recommendation 11.

Recommendation 14 (Paragraph 76)

It should be possible to implement such a regime quickly after the creation of the new Security Industry Authority, by the end of 2013 at the latest. The Government should include a timetable for implementation in its response to this Report. In view of the repeated delays, on-going abuses and the risks we have identified, the Government should take action quickly. There is no need to wait for the Leveson Inquiry to report before work to set out the principles of regulation and registration begins. Early publication of a draft bill could allow for public and Parliamentary consideration of potential legislation alongside the Leveson report.

We agree that we will not introduce the regulation of private investigations until after the transition to the new Security Industry Authority regime. It is the Government's intention that regulation of the private investigations sector would be rolled-out from the autumn of 2014.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call: 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Houses of Parliament Shop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents

ISBN 978-0-10-186912-6