THE GOVERNMENT RESPONSE TO THE
THIRTEENTH REPORT FROM THE HOME AFFAIRS
COMMITTEE SESSION 2010-12 HC 907

Unauthorised tapping into or hacking of mobile communications

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

September 2011

Cm 8182

£ 6.00

THE GOVERNMENT RESPONSE TO THE
THIRTEENTH REPORT FROM THE HOME AFFAIRS
COMMITTEE SESSION 2010-12 HC 907

Unauthorised tapping into or hacking of mobile communications

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

September 2011

Cm 8182

£ 6.00

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

Police Transparency Unit
Home Office
5th Floor
Fry Building
2 Marsham Street
London SW1P 4DF

This publication is also available for download at www.official-documents.gov.uk

ISBN: 9780101818223

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

ID P002453689 09/11 14950 19585

Printed on paper containing 75% recycled fibre content minimum.

THE GOVERNMENT RESPONSE TO THE THIRTEENTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION 2010-12 HC 907

UNAUTHORISED TAPPING INTO OR HACKING OF MOBILE COMMUNICATIONS

1. Introduction

1.1 This document sets out the Government's response to the Thirteenth Report of the Home Affairs Committee on "Unauthorised tapping into or hacking of mobile communications", published on 20th July 2011.

1.2 The Committee's report draws attention to a number of different issues arising from the unacceptable activities of journalists at News International and their associates to intercept phone messages illegally, and the failings of the police investigations relating to those activities. The report poses some serious questions around the governance and leadership of the police service and highlights concerns around the relationship between the police and the press. In doing so, it mirrors public unease about these relationships. The Government therefore welcomes the report as a valuable contribution to the wider debate around the changes needed to police culture. As a consequence, the Leveson Inquiry will explore the issue of police officers' employment by companies they have been investigating.

1.3 The report also makes the case for improving the regulatory authority, and increasing the flexibility of the criminal and civil sanctions that are currently available, in relation to phone hacking. Whilst the Government does not agree, we will ensure that the Committee's concerns around how the independent Commissioners work together are reflected in our work to develop the Commissioners' roles and functions. Section 2 provides more detail on these points. The Government also broadly agrees with the Committee's conclusions that both the mobile phone industry and network providers should increase the awareness of the security of mobile communication and that the latter should take proportionate action when personal data is intercepted. Section 4 contains a more detailed response to these points. Sections 3 and 5 contain our response to the Committee's other conclusions and recommendations.

2. Legislation and regulatory framework covering phone hacking

2.1 Section 2(7) of the Regulation of Investigatory Powers Act 2000 is particularly important and not enough attention has been paid to its significance. The lack of a regulatory authority under the Regulation of Investigatory Powers Act has a number of serious consequences....We therefore recommend the extension of the Information Commissioner's remit to cover the provision of advice and support in relation to chapter 1 of the Regulation of Investigatory Powers Act. (Paragraph 39).

2.2 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a regulatory framework for public authority use of a range of investigatory techniques. Part 1 of RIPA concerns the interception of communications and the acquisition of

communications data. The statutory oversight authority is the Interception of Communications Commissioner. He is required to review the exercise of powers and duties under sections one to eleven and Chapter two of RIPA. He is also responsible for administering a new civil sanction, which came into force in June 2011, which can be imposed for unlawful interception of electronic communications where the interception does not meet the threshold of the existing criminal offence.

2.3 Chapter one of RIPA includes a criminal offence of unlawful interception which is, quite rightly, for the police to investigate and enforce.

2.4 Interception is an area that requires a level of expertise and detailed subject matter knowledge which more appropriately sits with the Interception Commissioner than the Information Commissioner. Where there are issues before the Interception Commissioner that he thinks would more properly be dealt with by the Information Commissioner, insofar as they relate to the Data Protection Act 1998, then the Interception Commissioner will, as now, refer those issues to him.

2.5 However, following the Committee's recommendation, we are exploring whether the Interception Commissioner could provide further guidance in relation to his statutory duties in this area. The guidance would assist those who might be in need of independent advice, by further clarifying who would be the appropriate Commissioner they should direct their enquiries to.

2.6 We also strongly recommend that the Government reviews how the Act must be amended to allow for a greater variety of penalties for offences of unlawful interception, including the option of providing for civil redress, whilst retaining the current penalty as a deterrent for serious breaches. (Paragraph 40)

2.7 There is already a comprehensive framework of legislation to deal with the unlawful hacking of communications. As noted in the Committee's report, there are a number of pieces of legislation which establish criminal offences, including the criminal offences in s.1 of RIPA for unlawful interception, s.1 of the Computer Misuse Act 1990 relating to unauthorised access to computer material, and s.55 of the Data Protection Act 1998. A person found guilty of an offence of unlawful interception is liable on conviction in the Crown Court to imprisonment of up to two years, and on summary conviction to a fine not exceeding the statutory maximum - £5000 in England, Wales and Northern Ireland, and £10,000 in Scotland.

2.8 In addition to the criminal offences, the Government has introduced regulations to implement changes to RIPA, which came into force in June 2011. As a result, RIPA now provides a civil sanction for unlawful interception of electronic communications where the interception does not meet the threshold of the RIPA criminal offence. This is administered by the Interception Commissioner. The Committee will also be aware that there are other means to obtain civil redress, for example taking a civil action before the courts.

2.9 In addition, the Data Protection Act 1998 contains a number of regulatory powers and penalties for those instances where the requirements of that Act have been breached.

2.10 The Government will continue to keep this framework under review in light of changing technologies, but at present we are satisfied that the existing legislation provides a comprehensive set of criminal and civil sanctions for the unlawful hacking of mobile communications.

2.11 ***We note that most of our witnesses claimed to be unaware at the time of the Information Commissioner's two 2006 reports, 'What price privacy?' and 'What price privacy now?'. We are disappointed that they did not attract more attention among the police, the media and in government, and hope that future such reports will be better attended to. (Paragraph 41)***

2.12 The Government always carefully considers reports produced by the Information Commissioner, particularly where they make recommendations for legislative change or touch on aspects of government policy.

2.13 In addition, the Ministry of Justice, the Home Office, the Department for Culture, Media and Sport and other departments work closely with the Information Commissioner's Office (ICO) on policy and operational matters relating to, among other things, data protection, electronic marketing and surveillance. On data protection policy, which was the substantive subject of the Information Commissioner's 2006 report, Justice Ministers regularly meet the Information Commissioner to discuss his work.

2.14 We are concerned about the number of Commissioners, each responsible for different aspects of privacy. We recommend that the government consider seriously appointing one overall Commissioner, with specialists leading on each separate area. (Paragraph 42)

2.15 The Government believes the current spread of independent Commissioners ensures proper regulation of different aspects of privacy. The range of statutory functions carried out by each Commissioner varies significantly. It includes the provision of guidance, investigation of public complaints, serving and enforcing monetary penalty notices, making decisions over the deployment of technical devices, authorisation of some forms of surveillance and property interference, and oversight and inspection across different specialisms and under different legislation. Each Commissioner and his staff work in specialist, technical areas that require extensive knowledge of relevant legislation, equipment and procedures. Although the work they do can be related, it is also quite distinct.

2.16 The Government believes that the benefits the Committee is seeking can be delivered through existing arrangements and those proposed in the Protection of Freedoms Bill. The existing Commissioners already co-ordinate their work to ensure the right expertise is utilised in the right context and that wherever possible there is consistency between them. However, while respecting their independence, the Government will take note of the Committee's concerns in the way we develop and co-ordinate the roles and functions of the Commissioners.

3 Police investigations

3.1 Mr Hayman's conduct during the investigation and during our evidence session was both unprofessional and inappropriate…. We deplore the fact that Mr Hayman took a job with News International within two months of his resignation and less than two years after he was – purportedly – responsible for an investigation into employees of that company. It has been suggested that police officers should not be able to take employment with a company that they have been investigating, at least for a period of time. We recommend Lord Justice Leveson explore this in his inquiry. (Paragraph 69)

3.2 At present, a serving police officer is able to take outside employment or pursue business interests, but must disclose these to the relevant chief officer. It is then for chief officers to determine whether the employment or business interest is compatible with the individual's status as a police officer. Once an individual leaves the police service there are no specific restrictions on their employment or business interests.

3.3 The Government does not believe this position is satisfactory. For example, by comparison, in the case of civil servants and other Crown servants there are procedures in place to scrutinise appointments taken in the first two years after leaving. This is done in order to maintain public trust and to avoid the risk or suspicion of corruption or of the misuse of information gained in the course of official duties.

3.4 As the Home Secretary mentioned in her letter to the Chair of the Home Affairs Committee, on 22 July, the Government agrees with the Committee's recommendations that this issue could be explored in the Leveson Inquiry. In the meantime, the Home Secretary has asked Her Majesty's Inspectorate of Constabulary (HMIC) to include this issue in their report to her on police corruption.

3.5 The Government also draws the Committee's attention to Part 1 of Tom Winsor's Report of his Independent Review of Police Officer and Staff Remuneration and Conditions of Service, in which he made two recommendations relating to serving officers' business interests. The first called for improved guidance on the types of outside jobs and business interests likely to be rejected as incompatible with the officer's status, while the second related to the appeals process. The Government is currently considering the response of the Police Advisory Board (PAB) for England and Wales in relation to these recommendations alongside other reports that have been commissioned from HMIC and the Independent Police Complaints Commission (IPCC).

3.6 We note with some alarm the fact that only 170 people have as yet been informed that they may have been victims of hacking. If one adds together those identified by name, the number of landlines and the number of mobile phone numbers identified (and we accept that there may be some overlap

in these), that means up to 12,800 people may have been affected all of whom will have to be notified. We accept that there are a number of reasons why progress may have been slow so far, but at this rate it would be at least a decade before everyone was informed. This timeframe is clearly absurd, but it seems to us to underline the need for more resources to be made available to DAC Akers. We understand that in the current situation of significant budget and staff reductions, this is very difficult. However, we consider that the Government should consider making extra funds available specifically for this investigation, not least because any delay in completing it will seriously delay the start of the public inquiry announced by the Prime Minister. (Paragraph 93)

3.7 The resourcing of the Metropolitan Police Service (MPS) operation is a matter for the MPS and the Metropolitan Police Authority (MPA) to consider. However, the Home Office does make additional funding available to authorities facing exceptional or unpredictable events or emergencies. These Special Grants are provided where there is clear evidence that the expenditure incurred creates a serious threat to the authority's financial stability and their capacity to deliver normal policing. Should they consider it necessary, it is open to the MPS to make an application for additional support, which Ministers will consider.

4 The role of mobile phone companies

4.1 We welcome the measures taken so far to increase the security of mobile communications. However, with hackers constantly developing new techniques and approaches, companies must remain alert. In particular, it is inevitable that companies will think it in their interest not to make using technology too difficult or fiddly for their customers, so do not give as much prominence to the need to make full use of all safety features as they should do. We would like to see security advice given as great prominence as information about new and special features in the information provided when customers purchase new mobile communication devices. (Paragraph 111)

4.2 The Government agrees that the mobile phone industry should take steps to increase the public's awareness of the security features available on mobile communication devices and support designs that make those features easier to use. The Home Office works closely with the mobile communications industry and will continue to do so in taking this recommendation forward. In addition, as the Information Commissioner pointed out in his evidence to the Committee, he has a role in working with the mobile phone companies to help ensure personal data is protected and with consumers in highlighting how they can protect their own information.

4.3 The companies cannot escape criticism completely. Neither Vodafone nor Orange UK/T-Mobile UK showed the initiative of O2 in asking the police whether such contact would interfere with investigations (and O2 told us that they were given clearance to contact their customers only ten days or so after being informed of the existence of the investigation). Nor did either company check whether the investigation had been completed later. They

handed over data to the police, Vodafone at least sent out generalised reminders about security (Orange UK/TMobile UK may not even have done that), they tightened their procedures, but they made no effort to contact the customers affected. (Paragraph 117)

4.4 We find this failure of care to their customers astonishing, not least because all the companies told us that they had good working relationships with the police on the many occasions on which the police have to seek information from them to help in their inquiries. (Paragraph 118)

4.5 We expect that this situation will be improved by the coming into force of the new Privacy and Electronic Communications Regulations, which provide that when companies discover a breach of data security, they have to notify not only the Information Commissioner but also their affected customers. (Paragraph 121)

4.6 The Government agrees that phone companies should take appropriate steps to ensure their customers' personal data cannot be accessed improperly. The Government is pleased networks have improved security since this problem came to light and expects them to continue to work to ensure personal data is not compromised, and to follow appropriate procedures when it is.

4.7 The Government has introduced changes to the Privacy and Electronic Communications Regulations 2003, as part of the implementation of amendments to the European Framework on Electronic Communications, including the e-Privacy Directive. These came into force on 26 May 2011. Changes include a new requirement on communication providers to notify all breaches of personal data to the Information Commissioner and, in certain circumstances, a duty to notify the data object as well. The Information Commissioner's Office is expected to issue guidance on the new requirements shortly. These changes will help improve awareness and quality of the processing of personal data.

4.8 The Government has made clear its view that the requirement to notify breaches of personal data should be proportionate and pragmatic, and tied to the harm and distress caused, and to the size of the breach.

5. Other conclusions and recommendations

5.1 A number of the Committee's conclusions and recommendations are directed at the Metropolitan Police Service. In summary they are:

i) the limitations and failings of the original investigation (Paragraphs 34, 52, 55, 73, 80) and the subsequent reconsideration of the evidence (Paragraphs 81 and 82);
ii) the relationship between senior police officers and the press (paragraph 67) and between senior police staff and the press (Paragraph 86);
iii) police leadership and governance issues (Paragraphs 61 and 66); and

iv) the current and ongoing investigations (Operation Weeting) (Paragraphs 91 and 92) and the investigation into allegations of payments being made to the police by the media (Operation Elveden) (Paragraph 94).

5.2 Whilst it would be inappropriate for the Government to comment on ongoing investigations, we would like to draw the Committee's attention to the following:

5.3 Failings of the original investigation and the subsequent reconsideration of the evidence by the police

5.4 The Prime Minister announced that there would be an independent judge-led Inquiry to Parliament on 13 July. The Inquiry will be led by Lord Justice Leveson, assisted by a panel of senior independent figures with expertise in media, broadcasting, regulation, government and policing. It has broad-ranging terms of reference and will have powers to summon witnesses to give evidence under oath before reporting jointly to the Home Secretary and the Secretary of State for Culture, Media and Sport.

5.5 The Inquiry, which was launched on 28 July, will be in two parts. Whilst the first part will focus mainly on the ethics and behaviours of the press, the second part will examine the extent of unlawful or improper conduct at the News of the World and other newspapers, the way in which management failures have allowed it to happen, and also crucially the original police investigations and their failings.

5.6 **The *relationship between senior MPS officers and staff and the press***

5.7 Ensuring the integrity of the police is vital for their work and any allegation of corruption undermines public confidence.

5.8 That is why the Leveson Inquiry will, amongst other things, look at relations between the police and the press. The Home Secretary also announced in her statement to Parliament on 18 July, that she has asked for:

- a report from the Independent Police Complaints Commission on its experience of investigating corruption in the police service and any lessons that can be learned for the police service; and
- a report, with recommendations, from Her Majesty's Inspectorate of Constabulary considering instances of undue influence, inappropriate contractual arrangements and other abuses of power in police relationships with the media and other parties.

5.9 Both reports are due to be received by the Home Secretary this year. The HMIC report will be wide ranging, covering all police forces in England and Wales. It will include: existing governance arrangements and control measures; the relationship between the police and the media; existing guidance on information disclosure; instances of abuses of power in relation to procurement, contracting, recruitment and vetting; gratuities and hospitality in relation to police officers and staff; additional employment; the police's own ability to investigate and prevent corruption in forces; and public perceptions of police behaviour in relation to police integrity issues.

5.10 In the meantime, the MPS is also taking steps to increase the transparency and ethical underpinning of its relationship with the media. This includes commissioning advice from Elizabeth Filkin, the former Parliamentary Commissioner for Standards, on ensuring maximum transparency and public confidence, and agreeing to record meetings and hospitality, and publishing them on the internet.

5.11 Police leadership and governance

5.12 The report poses serious questions both for, and about, police leaders. The Government recognises there is a need to look again at police culture and leadership and there is now a greater need for openness and stronger corporate governance in the service. The Government is already working to make the police more accountable – through the introduction of Police and Crime Commissioners – but we believe we need to look more widely at how openness and accountability can be strengthened. For example, the Home Secretary has already asked Tom Winsor to look at entry routes to the service and, as the Prime Minister said in his statement to the House on 20th July, the Government wants to see radical proposals as to how entry could support improved openness in the service.

5.13 The Government had already begun to look at some of these areas in its work on leadership, training and development following the consultation on Peter Neyroud's review. We now think the events of recent months should also be brought into consideration in deciding how best to proceed.

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
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

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

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-181822-3