

NEW ZEALAND HOUSE OF REPRESENTATIVES
PRIVILEGES COMMITTEE

Written evidence from Sir Robert Rogers KCB,
Clerk of the House of Commons, United Kingdom

Use of Intrusive Powers within the Parliamentary Precincts

1. Thank you for your letter of 20 September 2013 inviting me to contribute to your Committee's inquiry into a question of privilege regarding use of intrusive powers within the parliamentary precincts.
2. The incident which led to the referral of the case before your Committee included the release of information from parliamentary information and security systems to the authors of an external inquiry. The information released included metadata information relating to emails, the substantive content of emails, telephone logs, and swipe card information relating to movements of certain individuals through the parliamentary precincts.
3. The overall aim of your Committee's approach is not to examine that incident as a contempt, but to study the incident as a practical example of how any policies and procedures which govern access to, and release of information from parliamentary information and security systems are applied.
4. Your Committee has identified some questions which it intends to consider further. Where I hope I may be of assistance, I have replied to each question in turn below. I am greatly indebted to my colleague Michael Carpenter, Speaker's Counsel for permission to use material from the recent paper he delivered to the Association of Parliamentary and Legislative Counsel in Canada, which I am sending to you with this submission.

How should information and security protection principles intended to safeguard data apply in a parliamentary context?

5. New Zealand shares with the United Kingdom the absence of a unitary constitutional document. Our two countries have a common heritage of constitutional arrangements, and we continue to have much in common despite diverging developments in each country since the establishment of the New Zealand Parliament.

6. The key concept in the parliamentary context relevant to your Committee's inquiry is that of exclusive cognisance. Parliament itself exercises control over its own proceedings, which may not be questioned or impeached in any court or place out of Parliament (Article 9 of the Bill of Rights). Furthermore, Parliament controls its own precincts. This exclusive cognisance does not extend to making Parliament a haven from the criminal law.¹ As may be seen in, for example, the Canadian case of *Vaid* [2005] 1 SCR 667 and the UK case of *Chaytor* [2010] UKSC 52, where there is doubt about the existence or scope of a privilege the court will test the claim against the doctrine of necessity.
7. In United Kingdom, government ministers will have access to two official e-mail systems: the government's own internal network, which is entirely separate from the House, and the parliamentary network. I cannot comment on how far the Government would consider it appropriate to release data about a Minister's e-mail to an official leak inquiry. As far as the parliamentary network is concerned, I would regard Ministers as being no different from any other Member.
8. Under the Parliamentary Corporate Bodies Act 1992, the Clerk of the House is the Corporate Officer of the House of Commons. I am the Accounting Officer for the whole of the House of Commons Administration Estimate, which funds all the House's support services. Following the expenses scandal of 2009, the Parliamentary Standards Act 2009 transferred Members' pay, Members' pensions, Members' staff salary and pension costs and Members' other business costs to the Independent Parliamentary Standards Authority. I remain Accounting Officer for the residual House of Commons Members Estimate, which covers, for example, financial assistance to support the parliamentary activities of Opposition parties. Part of my role as Corporate Officer of the House and Chief Executive of the House Service is to be the registered Data Controller for the House of Commons, in accordance with the UK statutory data protection regime. (Each Member of Parliament is required to be registered individually as the data controller for the information they may hold about other people, notably their constituents).

¹The UK Supreme Court decided in *R v Chaytor and others* [2010] UKSC 52 that parliamentary privilege was not an obstacle to the prosecution of Members for false accounting in relation to their parliamentary expenses.

9. The Freedom of Information Act 2000 applied the provisions of the Data Protection Act 1998 to Parliament from 1 January 2005, and I have been appointed Data Controller for the House of Commons. I take my personal responsibilities as Data Controller very seriously. At Board level in the House of Commons Service, our Director General of Human Resources and Change (Andrew Walker) is the Senior Information Risk Owner; he submits an annual information assurance statement to me which draws upon the assurance statements he receives from the Information Risk Owners in each of the Departments in the House of Commons Service. It is their personal responsibility to ensure that all staff are aware of, and apply, our policies on the appropriate handling of information, including its protective marking, authorised archiving and disposal practice, and the protection of sensitive and less sensitive personal data held about individuals including Members. This includes personal data held in all forms, whether paper or electronic, and of all kinds (written, spoken or visual).
10. I have set out in a text box an extract from the latest Annual Governance Statement which I am required to make as Accounting Officer for the House of Commons Administration Estimate, and which is published with our Annual Resource Accounts, as audited by the Comptroller and Auditor General.

House of Commons Administration Annual Governance Statement for 2012/13 (extract)

Information security

Information security continues to be an important concern for the House Service. Further effort is needed to embed effective information security behaviour in the organisation: more needs to be done on reporting information losses and the information security aspects of mobile technology and social media need more consideration. Progress has been made, including in conjunction with the House of Lords administration, in strengthening the controls which are in place to help ensure information is maintained securely. These include: running training and awareness-raising events for staff; implementing an electronic document and records management system (SPIRE) to ensure among other objectives the secure storage and timely disposal of electronic information; improving the security of our record management system; engaging a qualified Accreditor to provide an independent assessment of the information security risk posed by new systems or services; and compiling a comprehensive set of Registers of Sensitive Information Assets (RSIAs) for all departments. A process for reporting incidents of equipment and information loss or misuse is in place. During 2012-13 no incidents involving personal data required the Information Commissioner's Office (ICO) to be informed.

Are the information and personal privacy principles set out in applicable legislation (such as the Privacy Act, the Official Information Act, and the Evidence Act) relevant to the committee's

inquiry in the context of parliamentary privilege? If so, which principles are relevant?

11. In the United Kingdom, the relevant legislation takes account of, and is largely shaped by, the Directives on data protection agreed by the European Union. Schedule 1 to the Data Protection Act 1998 sets out the data protection principles, which were amended by the Freedom of Information Act 2000 to put beyond doubt that the processing of personal data, including sensitive personal data, is lawful where such processing is necessary for the exercise of any functions of either House of Parliament.
12. In its 14th Report of Session 2010–12, on *Privilege: Hacking of Members' mobile phones*, the Committee on Standards and Privileges addressed the question of whether the **unauthorised** access to voicemail messages left for Members could constitute a contempt of the House. The Committee considered the evidence that such "hacking" might obstruct or impede (or that it may tend to obstruct or impede) the business of the House or its Members in carrying out their Parliamentary functions. The then Clerk of the House, my predecessor Sir Malcolm Jack, suggested that there were six questions that needed to be answered when considering whether an act of hacking might be a contempt:
 - Does such interception impede a Member in the performance of his or her duty?
 - What significance is there to a Member knowing or suspecting hacking? (i.e. how can an interception unknown to a Member impede his or her activity?)
 - Does "impeding" result because Members' confidence in the confidentiality of communications with each other is undermined by the knowledge or suspicion of interception?
 - Does "impeding" result because Members' confidence in pursuing parliamentary activities (such as tabling questions) with staff of the House and advisers is undermined by the knowledge or suspicion of interception?
 - Does "impeding" result because Members' trust with constituents in pursuing parliamentary activities (such as tabling questions, raising matters in adjournment debates etc.) is compromised by the knowledge or suspicion of interception?
 - Does interception interfere with a Member's right to private life under Article 8 of the European Convention of Human

Rights (as imported into domestic UK law by the Human Rights Act 1998)?²

13. At least some of the questions posed by my predecessor, I would suggest, might be relevant to your Committee's consideration of the use made of metadata communications information by an **official** Government leak inquiry. The Committee on Standards and Privileges concluded that a series of acts of hacking which, by creating a climate of insecurity either generally in the House or in one of its committees or for a Member or group of Members or officers of the House, could be shown to have interfered with proceedings in Parliament could be a contempt. The Committee noted that demonstrating to a reasonable standard of proof a causal relationship between the acts of hacking and the climate of insecurity might be difficult.³
14. The case which has prompted your Committee's inquiry is one where information was provided to an officially-sanctioned inquiry. We have had some recent experience, which may be relevant, of assisting the police with their inquiries. Our principle is that House officials do not obstruct a criminal investigation, but neither do they participate in them.
15. In the wake of the arrest of an Opposition front-bencher (Damian Green) and the search by police of his offices on and off the parliamentary estate (which included the seizure of his computers) in November 2008, the House of Commons established a Committee which reported in March 2010.⁴ The Speaker's Protocol of 8 December 2008 (annexed) was principally intended as a set of instructions to House officials as to the procedure they should adopt in the event of a search warrant being presented. In giving such instructions, the Protocol addressed two problems which the Damian Green case had highlighted.⁵

² Fourteenth Report of Session 2010–12 from the House of Commons Committee on Standards and Privileges, *Privilege: Hacking of Members' mobile phones*, HC 628, paragraph 41

³ Fourteenth Report of Session 2010–12 from the House of Commons Committee on Standards and Privileges, *Privilege: Hacking of Members' mobile phones*, HC 628, paragraph 52

⁴ First Report from the Committee on Issue of Privilege, Session 2009–10, *Police Searches on the Parliamentary Estate*, HC 62. In November 2008 Damian Green, an Opposition frontbencher, was arrested on suspicion of aiding, abetting, counselling or procuring misconduct in public office in relation to leaks to him of classified information by a Home Office civil servant. His constituency office, his homes in London and the constituency, and his office on the parliamentary estate were searched.

⁵ The Protocol was concerned with circumstances where a warrant was required by law for a search, not with those where a search could be conducted without a warrant.

16. First, it made it clear that in future a warrant would always be required to conduct a search of a Member's office or gain access to a Member's parliamentary papers, including electronic records. The Speaker's Protocol puts beyond doubt that consent to such a search will not be granted by the parliamentary authorities in the absence of a judge's warrant. In the most recent case of a search warrant executed on 19 May 2013, the Speaker's Protocol was one of the documents exhibited to the circuit judge hearing the application in order to show that consent to search would not be given and that therefore the issue of a warrant, if justified, would be necessary.
17. Secondly, the Speaker's Protocol requires certain named officials to be informed of any case where a House official becomes aware that a warrant is to be sought. This was intended to avoid the situation where an individual official fails to consult relevant colleagues through accepting any inappropriate obligation of confidentiality towards the police. The Speaker's Protocol therefore provides that "In all cases where any Officer or other member of the staff of the House is made aware that a warrant is to be sought the Clerk of the House, Speaker's Counsel, the Speaker's Secretary and the Serjeant at Arms must be informed. No Officer or other member of the staff of the House may undertake any duty of confidentiality which has the purpose or effect of preventing or impeding communication with these Officers".
18. In contrast to the situation we were in with the Damian Green case in 2008, there is now a clear and well-known statement of practice in the form of the Speaker's Protocol. This Protocol was followed to the letter in the most recent case, when a search under a warrant was executed at the House of Commons on 19 May 2013 by the Lancashire Constabulary. That episode showed the value of having the Speaker's Protocol as a published document, well known to the relevant police forces as a source of guidance.
19. The need for police searches of offices occupied by members of the legislature seldom arises. In the House of Commons at Westminster there have been only two instances in five years: one with a warrant (May 2013, mentioned above) and one without (November 2008, the Damian Green case). The *United States v. Rayburn Office Building* case decided in 2008 [497 F3d 654] appears to have been the first involving a search of the office of a US Congressman. More common, at least at the United Kingdom House of Commons, are cases where documentary evidence or data is

sought by way of subpoena or Production Order in the course of a criminal investigation.

20. The criminal investigations following the scandal over Members' expenses in 2009 have led to a reasonably well understood doctrine over how to respond to requests from the police for records held by the House authorities which relate to individual Members. Its principles have been adapted to deal with the increasingly important question of access to electronic records.
21. In the administration of Members' expenses, the House of Commons (in the form of my predecessor as its Corporate Officer) held a number of relevant records, such as claim forms and supporting receipts. These are, of course, capable of containing personal data for the purposes of the Data Protection Act 1998. Although the 1998 Act provides a 'gateway' which permits the disclosure of personal data if this is necessary for the detection of crime or otherwise for the administration of justice,⁶ my predecessor took the view (on advice) that data held on Members should not be disclosed to the police, except with the Member's consent or pursuant to a court order. The reason for such advice was that this policy would provide the closest analogy to the Speaker's Protocol on the execution of a search warrant. The relevant court order, known as a Production Order, is generally obtained from a District or Circuit Judge under the Police and Criminal Evidence Act 1984 and has the features of a *subpoena*. In the event, no Production Order has yet been made against me as the Corporate Officer of the House of Commons in any case involving expenses. In all cases so far, the relevant Member has given consent to the disclosure.
22. A Production Order will specify a time (generally at least seven days) within which the specified records must be produced to a constable or be made available for inspection. A Production Order may be applied for without notice to the subject, but in practice there will have been discussion by the police with the House authorities so as to establish, for example, whether the records are in fact held and in order generally to limit the scope of the order, so that it does not become a 'fishing expedition'. In any event, unlike the case with a search warrant, there remains the opportunity of applying to the court for a variation of the terms of the Production Order, or even to set it aside, before its execution.

⁶ See sections 29 and 35 of the Data Protection Act 1998.

23. Increasingly, the relevant records are held in electronic form. These may either be held on electronic devices such as laptops, mobile phones or tablets or are retrievable from a communications network, such as the network operated for both Houses by Parliamentary Information and Communications Technology (PICT), a joint Department of the two Houses. Where such devices are seized in a search, the issue arises as to how the content of the devices is to be examined, either at all, or in such a way as to enable any issue of Parliamentary privilege to be asserted. A similar issue arises under a Production Order, although here the question is one of whether a record need not be produced by reason of any privilege.⁷ A further example is that where a Member gives consent to the examination of his records held in the PICT system, but where those records contain material which may be subject to Parliamentary privilege. In such cases, it is not within the power of the individual Member to waive such privilege (and, indeed, the House itself has no power to ‘waive’ the provisions of Article 9 of the Bill of Rights).⁸
24. The following methods have emerged from the practice at Westminster. In the Damian Green case, the paper records which had been seized were kept in sealed bags until they could be examined in a ‘sift’ for issues of privilege by House officials in the presence of the suspect’s solicitors. An essentially similar ‘sifting’ operation has been carried out in more recent cases of electronic records which are either produced by the Member voluntarily, or contained in a device seized under a warrant, or produced pursuant to a Production Order. In such cases, it has become the practice for the police, or PICT as the case may be, to produce a copied or ‘cloned’ version of the electronic records in consultation with the PICT or police, which copy or clone is then subsequently examined. The copy or clone is, in effect, the electronic equivalent of the sealed bag of documents.
25. In devising such arrangements, the view has been taken that it is neither lawful nor practicable to seek to prevent the police from seizing devices on the grounds that they might contain privileged material. It might be possible for a House official present at the search to make representations in respect of the seizure of hard copy

⁷ This would be on the ground, essentially, that the evidence would not be admissible rather than being privileged from disclosure.

⁸ Compare the remark of Lord Clarke JSC in *R. v. Chaytor* [2010] UKSC 52 referring to the doctrine of exclusive cognisance that ‘unlike the privilege provided for in Article IX of the Bill of Rights, Parliament can waive or relinquish it. It seems to me to follow logically from that conclusion that it is for Parliament, and not the individual Member, to rely on it’.

material, but this is plainly impractical with devices. Moreover, the view has also been taken that the material is not privileged from disclosure, even though its use as evidence might lead to impeaching or questioning in breach of Article 9 of the Bill of Rights. As a former Clerk of the House, Sir William McKay, has explained “the prohibition in the Bill of Rights...is directed at argument in the courts—that is, at the use made of protected material which, if admitted, might open the way to judgments inhibiting Members’ right of free speech. It does not confer a sacrosanct status on the documents themselves on which an absolute denial of police access may be based...I am driven to the conclusion that there are no grounds to prevent papers and records passing into police custody before being sorted into sheep and goats”.⁹ The good sense of the view taken by my predecessor Sir William McKay is supported by the fact that extracts from Hansard and other public records of proceedings in Parliament are matters which may be admitted to prove the fact of the occurrence of such proceedings, but not as to the truth of their content. (It is quite possible that a Hansard extract might prove, for example, a Member’s alibi.) It is, therefore, impossible to state *a priori* that evidence of Parliamentary proceedings could never be admissible.¹⁰

26. As for the examination of evidence seized or otherwise recovered in electronic form, there is plainly a difficulty in resolving any question of Parliamentary privilege when the material is in the exclusive custody and control of one party. To meet this problem, a system of ‘chaperoning’ the examination of the evidence seems to have worked well, at least in Westminster. The system involves the creation of a forensic image or copy of the material being created (by the police, or by PICT) which image is then opened in the presence of both parties and examined using search terms to identify material which might be so closely connected to Parliamentary proceedings as to raise an issue of privilege. When such material is identified, it is tagged in the presence of both parties so as to indicate a possible claim to privilege and is put to one side. It therefore closely follows the sifting procedure used for seized papers in the Damian Green case.

Should the collection and release of metadata information be treated differently from information which contains substantive content?

⁹ HC (2009–10) 62 Ev 150 paragraph 18

¹⁰ See the comments by the Metropolitan Police Service on the Speaker’s Protocol HC (2009–10) 62 Ev 159

27. Our approach to metadata such as e-mail or telephone logs is fundamentally the same as for data which might be regarded as substantive content (such as the body of an email, or the voice recording of a telephone conversation). Some such metadata may be virtually meaningless on its own but, when combined with other data (whether other metadata or substantive data), it may become part of a more significant data set. Such aggregation may have the effect of turning non-personal data into part of a personal data set, or turning non-sensitive data into a sensitive data set. A simple example would be the time-stamps on e-mails, when added to the core data.
28. The collection of metadata may be no more than an automatic and passive consequence of how an information technology system operates. Such metadata are referred to as 'communications data' in Chapter II of the Regulation of Investigatory Powers Act 2000 and the processing of such data by the House is done within the terms of the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.¹¹ The selective mining and release of such metadata could constitute the processing of personal information of the kind that ought not to be released without a good and lawful reason. We need to bear in mind that bulk metadata can be very revealing about individuals and organisations; in some situations such bulk information can be more revealing even than content.

Are there particular sets of information held on parliamentary information and security systems that should be treated differently from other information?

29. Yes. The House of Commons is a public authority under the Freedom of Information Act 2000, but individual Members of Parliament are not. So information held by Members of Parliament does not become information held by the House of Commons just because the information is physically or electronically located on the parliamentary estate — in a Member's pocket or handbag, in an office or desk drawer or in an e-mail or document held electronically in the Parliamentary Network. House of Commons Service staff, who are employees of the statutory House of Commons Commission, are bound by the terms and conditions of their employment. A number of policies, including on the acceptable use of information

¹¹ SI 2000/269.

technology, are published in our Staff Handbook.¹² Members' staff are personally accountable only to the Member of Parliament who is their employer. Access to the Parliamentary Network is granted only if the individual consents to respect our information security policies including on its acceptable use.

30. Many hundreds of other people who are issued with photographic swipe cards, giving them access to the Parliamentary estate, do not qualify for a Parliamentary e-mail account. These categories of people include civil servants who need frequent access to Parliament, people working as contractors for the House of Commons, journalists and broadcasters. All these pass-holders are made aware of our security policies and their own personal responsibilities if they apply for and are granted a Parliamentary photo-pass and other facilities on the Parliamentary estate.

31. We do not of course make any public comment on security measures taken to protect the Parliamentary Estate. It is nonetheless readily apparent to any passer-by that we deploy closed-circuit television cameras, that armed police are present within the perimeter and that holders of photo-passes gain access the precincts either by presenting themselves to uniformed police officers or by tapping in a PIN code to use automated swipe-card machine-readers of their photo-passes.

What is the status (including ownership) of the different types of information held on parliamentary security and information systems (including information relating to proceedings of the House, and information relating to Members, Ministers, journalists, staff and others)?

32. The status and ownership of the different types of information held on parliamentary security and information systems has not been codified in the manner suggested by the question. Factors to be taken into account would include —

- Article 9 of the Bill of Rights which applies to proceedings in Parliament
- The Parliamentary Papers Act 1840 which applies to reports ordered to be published by Parliament
- The exclusive cognisance which Parliament exercises over its own affairs

¹² Available on the www.parliament.uk internet site—perhaps most easily accessible via the A to Z link at the foot of our homepage.

- Our statutory responsibilities under applicable freedom of information and data protection legislation.
33. The “Wilson doctrine” was set out in answer to questions in the House of Commons on 17 November 1966. The then Prime Minister, the Rt Hon Harold Wilson, said that he had given instructions that there was to be no tapping of the telephones of Members of Parliament and that if there were a development which required a change of policy he would at such moment as was compatible with the security of the country make a statement in the House about it.¹³ The Wilson doctrine has been maintained under successive administrations.¹⁴ The Wilson doctrine is no more than an undertaking by the Prime Minister of the day, albeit reiterated by his successors, which was framed when information and communications technology was primitive compared to today. The Wilson doctrine is not rooted in statute and could be revoked or adapted by Prime Ministerial decision. If construed very strictly, it could be read as applying only to Members’ telephones.

34. In the text box below I set out a recent written Answer responding on behalf of the House of Commons Commission to a Question tabled by an opposition front-bencher about of the security and privacy implications of moving Members' ICT services onto the Cloud. In the future, Parliamentary data will increasingly held by third parties (in the “Cloud”) rather than on our own secure servers. An important priority for me as Chief Executive and Data Controller is to make sure that we have the necessary assurances and safeguards in place with regard those arrangements.

House of Commons Official Report, 28 October 2013 column 337W

ICT

Chi Onwurah: To ask the hon. Member for Caithness, Sutherland and Easter Ross, representing the House of Commons Commission what assessment the Commission has made of the security and privacy implications of moving hon. Members' ICT services onto the Cloud. [172675]

John Thurso: While it is not the practice of the Commission to comment on security matters in any detail, the high-level position is that Parliamentary ICT, working with the Parliamentary Security Director, the Senior Information Risk Owners of both Houses, Speaker's Counsel, other parties and the supplier, has assessed the risks of the proposed new arrangements for the security and privacy of parliamentary data.

¹³ HC Deb 17 November 1966 vol 736 cols 634-41 annexed to this paper

¹⁴ Erskine May 24th edition (2011) page 264 annexed, with more recent Ministerial answers

These are generally assessed as positive in relation to conventional cyber attack and negligible in relation to potential cross-jurisdictional action (for example, under the USA PATRIOT Act).

The biggest risk to the security and privacy of parliamentary data is poor user behaviour and non-compliance with rules, policies and best practice. Any new arrangements will be accompanied by refreshed guidance and a substantial awareness-raising campaign.

Members can access current guidance via the ICT security pages on the parliamentary intranet. If the hon. Member has any particular issues that she would like to discuss, the Parliamentary Security Director would be happy to meet her.

How should the collection and release of information relating to specific groups with roles within the parliamentary context (such as Ministerial staff, Members' staff, parliamentary staff or journalists) be treated?

35. The collection and release of information relating to specific groups with roles within the parliamentary context (such as Ministerial staff, Members' staff, parliamentary staff or journalists) would in the United Kingdom have to be treated strictly in accordance with data protection principles, which provide for personal data to be used only in appropriate circumstances for legitimate investigations or other legitimate purposes..
36. In the parliamentary context, the public interest in maintaining the integrity of the democratic process sets a very high standard for any purportedly over-riding imperative to seek, retrieve and release such data. Where important principles come into conflict, it may be sensible for them to be resolved by a judge making a production order or issuing a search warrant. Such judicial action may be challenged in court. I am aware that your Committee has recently been examining the agreements for policing, execution of search warrants, and collection and retention of information by the New Zealand Secret Intelligence Service.
37. The Joint Committee on the Draft Communications Data Bill agreed with the Home Office in December 2012 that there was no need for new criminal offences to punish minor administrative errors made by officials in public authorities while seeking to acquire communications data as, where appropriate, disciplinary action should suffice. In the Committee's view, wilful or reckless conduct would be another matter. The Committee noted that there were already several relevant offences, including—

- unauthorised access to computer material, contrary to section 1 of the Computer Misuse Act 1990, which carries a maximum sentence of two years' imprisonment;
- unauthorised access with intent to commit another offence, such as fraud, contrary to section 2 of the Computer Misuse Act 1990, which carries a maximum sentence of five years' imprisonment;
- knowingly or recklessly obtaining, disclosing or procuring the disclosure of personal data without the consent of the data controller under section 55 of the Data Protection Act 1998, which carries a maximum penalty of an unlimited fine but not, at present, a custodial sentence.

In addition, the common law offence of misconduct in public office is committed when the office holder wilfully acts (or fails to act) in a way that he knows is wrong and is calculated to injure the public interest. The maximum penalty for this offence is life imprisonment.¹⁵ According to guidance published by the Crown Prosecution Service, a charge of misconduct in public office should be reserved for cases of serious misconduct or deliberate failure to perform a duty which is likely to injure the public interest.¹⁶

38. Although its draft Bill on the matter was subjected to pre-legislative scrutiny by the Joint Committee in 2012, the coalition Government has not yet introduced a Communications Data Bill in the present Session. The recent Protection of Freedoms Act 2012 provides for the Secretary of State to draw up a code of practice containing guidance about surveillance camera systems (section 29) and also makes provision in section 37 about judicial approval for obtaining or disclosing communications data.

39. The unauthorised publication of “wikileaks” material unlawfully disclosed by Bradley Manning and the further unauthorised disclosures by Edward Snowden have kept the issues around data control and surveillance high on the political agenda in the UK, as elsewhere.

Who should have authority over the release of information and how should that oversight be exercised?

¹⁵ Report from the Joint Committee on the Draft Communications Data Bill, Session 2010–12, HC 479/HL Paper 79, paragraph 225

¹⁶ Cited at First Report from the Committee on Issue of Privilege, Session 2009–10, Police Searches on the Parliamentary Estate, HC 62, paragraph 44

40. Whatever the formal arrangements, the Speaker of the House will inescapably be drawn into any major dispute over the release of parliamentary information, not least because it is in the nature of Parliament for political rows to erupt in the Chamber. In practice, it is hard for the Government to evade the blame for unpopular courses of action.
41. As Clerk of the House, I am Mr Speaker's chief procedural adviser. In my judgement, the House of Commons is best served by a unitary service headed by a Chief Executive who works closely with the Speaker in handling the political process in the Chamber every sitting day. New Zealand has taken a different path, by separating the Office of the Clerk from the wider Parliamentary Service. A similar division was considered, and rejected, by both of the last two major external reviews of the structure of the House Service, conducted by Michael Braithwaite (1999) and Sir Kevin Tebbit (2007)—extracts annexed.
42. Formally, authority lies with the Data Controller: that is to say, with the Clerk of the House as Corporate Officer of the House of Commons. Politically, the Speaker will probably be drawn into any political row over the rights of the legislature. In the United Kingdom, we have had lessons to learn from the Damian Green case, where the Committee looking back over those events considered on the evidence available to them that seriously inadequate communication between the three key figures — the former Speaker, the former Clerk of the House and the former Serjeant at Arms — resulted in a complete misunderstanding about the proper process for allowing a search of a Member's office. The Committee agreed with the former Speaker that the House officials should have served the Speaker better, and noted that the then Clerk of the House had ("rightly") apologised that matters had not been better handled. The Committee concluded that it was inescapably the Speaker's responsibility to make sure that the right questions were asked. In the Committee's view of the particular case in those specific circumstances, the Speaker had failed to exercise the ultimate responsibility, which had been his alone, to take control and not merely to expect to be kept informed.¹⁷
43. A judicial process, such as the issue of a warrant or a production order, is probably the best route to adjudicating the

¹⁷ First Report from the Committee on Issue of Privilege, Session 2009–10, *Police Searches on the Parliamentary Estate*, HC 62, paragraph 115

competing claims of the public interest in the release of information, and in maintaining its confidentiality. When disclosure itself is at issue, applying the normal rules of disclosure may pre-empt and frustrate the confidentiality that one side seeks to preserve. A legal process provides a forum for the rival claims to be determined fairly.

What thresholds or principles should apply to releasing this information, including where a security issue is cited?

44. We do not have a comprehensive protocol covering the release of information. Consideration should be given to a number of principles, which may sometimes come into conflict with each other:
- Parliament is not a haven from the criminal law.
 - The exercise of freedom of speech in Parliament is fundamental to democracy and the liberty of the subject.
 - Parliament exercises exclusive cognisance over its own precincts and processes.
 - Parliament should be exemplary in abiding by the rule of law, including the applicable legislation relating to police and criminal evidence, freedom of information, and data protection.

Other issues relevant to the Committee's consideration

45. The custody of data ought to be a high priority for any Parliament. In the United Kingdom, the expenses scandal of 2009 was a huge blow for the standing of Parliament. That scandal was precipitated by the theft of a huge quantity of data from the premises by a contractor whom we had hired for the purpose of removing sensitive and irrelevant personal information prior to its publication in accordance with a court decision in a Freedom of Information case. Lessons have been learned from the investigation (which as Clerk assistant I carried out) of the circumstances.

46. In the United Kingdom Parliament, we are beginning to recognise the potential cyber-threats of disruption, data theft and espionage. Appropriate counter-measures are already being taken and further measures are planned. Technological changes form one part of the mitigation actions for the cyber-security risk which we have to face. The measures taken to mitigate the cyber-security risk overlap with those already addressing the information security risks referred to above.

47. Managing parliamentary data well, in order to meet our obligations and to meet the expectations of Members, the media and the wider public, is an important priority for the House of Commons Service. We are by no means complacent. I am grateful to your Committee for having posed us these penetrating questions, which will cause us to reflect on how we might have fared had a comparable situation arisen here.

48. I am of course happy to answer any further questions your Committee may have.

SIR ROBERT ROGERS KCB
Clerk and Chief Executive of the House of Commons

31 October 2013

ANNEX: UK House of Commons Speaker's Protocol of 8 December 2008

1. In my statement of 3 December 2008 (HC Debates col 3) I said I would issue a protocol to all Members on the searching of Members' offices. In future a warrant will always be required for a search of a Member's office or access to a Member's parliamentary papers including his electronic records and any such warrant will be referred to me for my personal decision.
2. Though much of the precincts of the House are open to the public, there are parts of the buildings which are not public. The House controls access to its precincts for a variety of reasons, including security, confidentiality and effective conduct of parliamentary business.
3. Responsibility for controlling access to the precincts of the House has been vested by the House in me. It is no part of my duties as Speaker to impede the proper administration of justice, but it is of equal concern that the work of the House and of its Members is not unnecessarily hindered.
4. The precincts of Parliament are not a haven from the law. A criminal offence committed within the precincts is no different from an offence committed outside and is a matter for the courts. It is long established that a Member may be arrested within the precincts.
5. In cases where the police wish to search within Parliament, a warrant must be obtained and any decision relating to the execution of that warrant must be referred to me. In all cases where any Officer or other member of the staff of the House is made aware that a warrant is to be sought the Clerk of the House, Speaker's Counsel, the Speaker's Secretary and the Serjeant at Arms must be informed. No Officer or other member of the staff of the House

may undertake any duty of confidentiality which has the purpose or effect of preventing or impeding communication with these Officers.

6. I will consider any warrant and will take advice on it from senior officials. As well as satisfying myself as to the formal validity of the warrant, I will consider the precision with which it specifies the material being sought, its relevance to the charge brought and the possibility that the material might be found elsewhere. I reserve the right to seek the advice of the Attorney General and Solicitor General.

7. I will require a record to be provided of what has been seized, and I may wish to attach conditions to the police handling of any parliamentary material discovered in a search until such time as any issue of privilege has been resolved.

8. Any search of a Member's office or belongings will only proceed in the presence of the Serjeant at Arms, Speaker's Counsel or their deputies. The Speaker may attach conditions to such a search which require the police to describe to a senior parliamentary official the nature of any material being seized which may relate to a Member's parliamentary work and may therefore be covered by parliamentary privilege. In the latter case, the police shall be required to sign an undertaking to maintain the confidentiality of that material removed, until such time as any issue of privilege has been resolved.

9. If the police remove any document or equipment from a Member's office, they will be required to treat any data relating to individual constituents with the same degree of care as would apply in similar circumstances to removal of information about a client from a lawyer's office.

10. The execution of a warrant shall not constitute a waiver of privilege with respect to any parliamentary material which may be removed by the police.

11. In view of the concern shown by Members, I am circulating this document without delay, but I shall take into account any representations by Members for its revision and will issue a revised document, should this be necessary.

MICHAEL MARTIN
Speaker

ANNEX: UK House of Commons Braithwaite Review (1999)

<http://www.publications.parliament.uk/pa/cm199899/cmselect/cmhccom/745/intro.htm>

House of Commons Commission Review of Management and Services of the House of Commons by Michael Braithwaite, HC 745 of 1998–99 (extract)
--

ANNEX G Other models of governance
--

1. Before making our recommendations on governance, we considered whether there was a case for radical change. In doing so, we examined a number of other systems of governance to see whether they might be applicable or adaptable to the circumstances of the House.

The “local government” model

2. This is familiar to the substantial number of Members with local government experience. It was discussed in some of our interviews as a means of involving Members more closely in the administration of the House, but had no significant support.
3. In essence, this model would imply control of House administration by subject committees with executive powers, reporting to a general purposes committee. Officers would advise the committees, but would be subject to instructions from them.
4. We see problems of principle and practice in any version of this model. Members of local authorities are not only politically responsible to their electorate; they are legally responsible for their decisions. In certain circumstances, they may be surcharged. No similar responsibility is laid upon Members of Parliament; and primary legislation would be required to impose it.
5. We very much doubt whether there would be enthusiasm for such a change; but we are sure that it would be improper to confer executive responsibility without it. Accountability would be so diffuse as to be non-existent. There is no parallel with Ministers and Accounting Officers in Whitehall; the framework of statute and convention, together with collective Government responsibility, is entirely different.
6. In any event, the circumstances are not comparable. The main business of local authorities is the formulation and execution of policy in major areas such as education, housing, planning, transport and so on. One of the principal motives for Member involvement (and considerable commitment of time) is the pursuit of the policies, usually upon a party basis, on which they were elected.
7. The low level of interest in House administration among Members (except as consumers), the attendance levels in the domestic committees, and especially the high turnover in membership, suggest that this model of governance could not be sustained. It would risk lack of direction, or being in the unrepresentative control of a few individuals.
8. Subject committees in this model would in practice probably be “departmental” committees. This would emphasise the federal structure and its decision-making compartments; and (even with a general purposes committee) would make the necessary corporate governance harder, if not impossible, to achieve.
9. We do not think that there are features of the local government model which can be easily or usefully applied to the House.

The “Quaestor” model

10. This is a system in which individual Members, usually of some seniority, are given extensive executive powers over administration and services. These powers are often exercised in consultation with the presiding officer. This system is used in the French Parliament, for example.
11. The quaestor system has much to recommend it. The personal focus can make political responsibility clearer to fellow-Members; Officers can work closely with an individual rather than with committees, and get advice or authority quickly when required.
12. Very few Members are involved in formulating advice or making decisions, which may

have attractions from the point of view of achieving a simple system, but is open to criticisms of exclusivity.

13. Quaestors are found primarily in Parliamentary systems run by a bureau, in the Continental style: a committee of presiding officers and deputies, and leaders of party groups. A bureau will have wide powers over the organisation of business and a range of other Parliamentary matters. There is no Westminster equivalent; and without the overall control of such a body (some of whose Members act as representatives of their parties in the House) we doubt whether the quaestor system can easily be transplanted.

14. However, to the extent that the concept can be used in the Westminster system, we have sought to reflect it in our recommendations on the role of the Chairman of the Finance and Services Committee. Those recommendations build on the function envisaged by Ibbs, which itself had some elements of the quaestor role.

The external chief executive

15. This was a suggestion more often made to us and in the JLA survey by Members (although still by very few). This would be an individual, probably from the private sector on a term appointment, brought in to supervise all the House's services, and responsible to the Finance and Services Committee or to the Commission.

16. This possibility was mentioned to us most frequently in the context of services such as accommodation and IT, and making sure that complaints were dealt with or did not arise. Although there is a theoretical argument for bringing in a chief executive (which we consider below) the expectations of such an individual seemed to relate more to a customer service manager than to a corporate chief executive planning and delivering the whole range of Parliamentary support, not only services to Members in their offices.

17. Service improvement is of course a real issue, and one which the JLA survey demonstrates is a continuing process. The Board of Management's action plan to address points arising from the survey will be a further stage. The substantial progress since the Ibbs report suggests that radical structural change is not required to maintain the process of improvement.

18. A chief executive with extensive outside experience of corporate governance, of driving costs down and achieving maximum value for money, could no doubt deliver "more for less" - although whether that would be substantially more than could be achieved through initiatives already under way and through the implementation of our recommendations would not be certain.

19. However, the implications of such an appointment, and perhaps its chimerical nature, need to be considered in rather more detail. The Clerk of the House is at Grade 1 level, equivalent to a Permanent Secretary. This reflects the importance of the Parliamentary and constitutional issues with which he deals, and will continue to do so. A chief executive would therefore be an additional Grade 1 appointment, and would no doubt have to be attracted at considerably more than Grade 1 salary — both of which elements would require to be justified.

20. Although an incoming chief executive would be familiar with the "transactional" type of business conducted in the Serjeant's Department or the Refreshment Department, and administrative and financial services, he or she would have no knowledge of the House and

its committees: what is required to support business, and how Parliament could develop and be more effective. The Clerk would remain the authority on such matters, and would be seen by staff of the House as being so. There would then be a situation where the chief executive ran administrative services, but was not seen as having authority in the core business; a perfect recipe for sidelining (or conflict). And if the chief executive were to override the Clerk's Parliamentary judgement, the effect on morale of those employed in the core business would be only one of the potential difficulties.

21. It is also worth bearing in mind that it is usual in the private sector for an incoming chief executive to import his or her own style and agenda. This may be desirable in a commercial environment, but might not be universally popular with Members. Conversely, many candidates might find the complex constraints of the House frustrating.

22. It should also be remembered that an incoming Chief Executive would have to become Accounting Officer for the Members' Salaries etc Vote, an area of particular sensitivity.

23. It was also suggested to us that the chief executive (either in this structure or in the "twin" model discussed below) should report to a management committee as a single authority. This suggests two possibilities:

- the management committee is the Commission. We think that this would grossly overburden the Commission, and would not be practical
- the management committee is not the Commission. In that case there would be little point in retaining the Commission; the House of Commons (Administration) Act 1978 would have to be amended, and the Commission's functions would have to be bestowed upon the management committee. If the Commission were retained, it would simply be a rubber stamp for the decisions of the management committee
- A committee which is not a single authority, but is subordinate to the Commission, is represented by the Ibbs model of the Finance and Services Committee, which is what we have sought to develop in our recommendations.

The Chief Executive and the Clerk as equals

24. It has been suggested to us that the need to maintain the Clerk's independence and distinct role could be accommodated in a system where the chief executive and the Clerk were of equal rank; the Clerk would deal with procedural matters and the chief executive would deal with everything else. This might reflect some aspects of models of governance used in health service structures, for example, where professional medical matters are the province of the health professionals, and chief executives deliver the support services.

25. There is some attraction in the principle of this model of governance; but we do not think that in this form it is easily or appropriately applied to the House.

26. In the first place, the chief executive would no doubt become Accounting Officer for all three Votes (two after the merging of the House Votes). This would make him or her Accounting Officer for the Members' Vote (see paragraph 22 above) and also for House expenditure. It would be difficult to separate the functions of Accounting Officer and Corporate Officer, so primary legislation would be needed to amend the Parliamentary Corporate Bodies Act 1992. But although the physical property and contractual part of the Corporate Officer's functions would be for the chief executive, the copyright and intellectual property functions would be appropriate to the Clerk. It would therefore be necessary to have two Corporate Officers, with some possibility of overlap.

27. The real problems would come in attempting a realistic separation between “administrative” and “procedural” services, and it is here that the difference from the health service model becomes apparent.

28. “Procedural” is too narrow a definition. The real split would have to be between “administrative” and “Parliamentary” functions, because the work of the House itself and its Committees would have to be a responsibility of the Clerk and not of the chief executive. The Parliamentary functions would involve

- The Clerk’s Department, which advises on procedure and business, but which also provides substantial select committee and other administration as an integral part of its work. It also has lead responsibility for printing and publishing, is the supplier of all House and official papers, and deals with inter-Parliamentary relations, including support of the House’s delegations to international assemblies
- The Library, which provides professional information and research services in close support of the Parliamentary duties of Members. It would be perverse to separate the specifically Parliamentary roles of the Library from its wider information responsibilities, so the Library as a whole would have to be on the “Parliamentary” side of the divide
- Core Serjeant functions of ceremonial, security and order in the Chamber and Committee Rooms, which are also directly related to proceedings, and would have to be provided by a small Department headed by the Serjeant at Arms, but without his works, communications and housekeeping responsibilities
- The Official Report, which operates entirely in the support of proceedings.

29. The “twin” model now starts to look rather less logical; the chief executive is responsible for finance, personnel, catering, works, housekeeping and IT, but nothing else. Moreover, the financial authority for the Parliamentary side rests not with the Clerk, who is in operational charge of it, but with someone of equal rank over whom he has no control, and to whom he will be a suppliant in seeking funds for support of the House’s core business.

30. The scope of the chief executive’s responsibilities now makes his or her Grade 1 level difficult to sustain. Rather more services are run at the moment by three Officers, none of whom is above Grade 3, and all of whom would be required in any new organisation.

31. There are other objections to this type of structure:

- it would encourage the development of two different cultures in two separate House services, exacerbating a problem which needs addressing in the current structure
- it would make much-needed House-wide corporate operation virtually impossible
- it would not provide greater clarity
- it would institutionalise the possibility of conflict between the House’s two most senior Officers.

32. We are aware that a few Parliaments (for example New Zealand and the French Assemblée Nationale) have a divided service; but in rather different circumstances:

- In New Zealand the Parliamentary Service is an administrative agency which provides support services, but includes responsibility for the equivalent of the Members’ Salaries etc Vote. The operation is also rather smaller; the Parliament of New Zealand is less than one-fifth the size of the House of Commons.

- In France's 577-member Assemblée Nationale, the Secrétaire Général de l'Assemblée et de la Présidence is responsible for the equivalents of all the services we listed in paragraph 26, while the Secrétaire Général de la Questure is responsible for finance, personnel, catering, security, works and transport. The two Secretaries-General are of equal rank. However, most of the senior staff in all Departments are fast-stream graduate entrants (equivalent to the Clerk entry in the House of Commons) and move freely between the two services, which are in fact more unified than the structure suggests.

33. We also note that the Swedish Riksdag is now exploring ways of merging services, and bringing the separate Administration and Finance Agency under the control of the Secretary-General of the Riksdag. The Canadian House of Commons experimented with a divided service, but the experience was not thought to be a success; some of the difficulties we have identified for this model were encountered. The Canadian House has now returned to a system in which the Clerk of the House is in overall charge of all Parliamentary and support services. This is by far the most widespread model in Parliaments of Commonwealth and EU countries.

June 1999

ANNEX: UK House of Commons Tebbit Review (2007)

<http://www.publications.parliament.uk/pa/cm200607/cmselect/cmcomm/685/685.pdf>

<http://www.publications.parliament.uk/pa/cm200607/cmselect/cmcomm/685/68502.htm>

House of Commons Commission Review of Management and Services of the House of Commons by Sir Kevin Tebbit KCB, HC 685 of 2006–07 (extract)

CLERK OF THE HOUSE/CHIEF EXECUTIVE

84. In our view, the main focus of change should be at the level of the Board of Management. It has been suggested to us that the single most beneficial reform — and salutary shock to the system — would be to appoint a Chief Executive from outside to run the House Service as a whole in a more business-like manner. It is argued that the person who becomes Clerk of the House, by virtue of that individual's qualities, experience and expertise as a procedural/legal specialist, is not best placed to take on the broader management and leadership role that a Chief Executive is required to perform.

85. While this proposition has a certain force, it was not accepted by Ibbs or Braithwaite. We have come to the same conclusion as they did, for the reasons set out below.

86. The role of the Chief Executive, in business or government, is to be responsible for the delivery of the front line outputs of the organisation, as well as for the enabling services which underpin them. Much of the front line output of the House of Commons Service lies in the Chamber of the House and its Committees — the domain where the Clerk of the House is the pre-eminent expert. It is highly unlikely that any external candidate could be found with sufficient procedural and parliamentary expertise to perform this function, as well as having

the normal Chief Executive competences.

87. A separate Chief Executive would, as a consequence, be responsible mainly for support services and facilities management. This would divide the leadership roles between Clerk of the House and Chief Executive in an organisation which is, arguably, already over-compartmentalised and in need of greater corporate unity and direction.

88. The political environment of the Commons, within which the Chief Executive would need to fit, would also impose constraints. Since the Speaker combines the two roles of presiding over the Chamber and over management and services, the two intertwined, he would, inescapably tend to rely for advice on both aspects from the official with whom he has most to deal on a daily basis — and that is the Clerk of the House. Moreover, the self-governing nature of the Commons, where so much is also political, would constrain a Chief Executive, brought in from outside, from exercising the degree of control that such an individual would expect to have in order to deliver objectives. It would not be an attractive position to take. **We therefore recommend that the Clerk of the House should continue to perform the dual role of Clerk of the House and Chief Executive/Accounting Officer.**

June 2007

ANNEX: UK House of Commons: The Wilson doctrine

TELEPHONE TAPPING

17 November 1966 House of Commons Debates vol 736 columns 634-41

§The following Questions stood upon the Order Paper:

§Q13.Mr. RUSSELL KERR: To ask the Prime Minister on how many occasions warrants have been issued for the tapping of hon. Members' private telephones; and if he will give an assurance that no such warrants will be issued.

§Q14.Mr. DONNELLY: To ask the Prime Minister whether he will state the criteria upon which he has issued his warrant for the tapping of hon. Members' telephones.

§Q15.Mr. PETER M. JACKSON: To ask the Prime Minister if he will bring up to date the statistics of warrants authorising telephone-tapping given to the Committee of Privy Councillors; and whether he will issue an annual return, showing the number of permissions that have been given, the number that have been withdrawn, and the number outstanding at the date of making the return.

§Q16.Sir T. BEAMISH: To ask the Prime Minister whether he will give an assurance that the issue of warrants giving authority to tap telephone conversations remains under the Home Secretary's sole authority; and in what respects the criteria governing the issue of such warrants have been changed since October, 1964.

§The Prime Minister (Mr. Harold Wilson): With permission, I will now answer Questions Nos. Q13, Q14, Q15 and Q16.

The House will know that, since the publication of the Report of the "Committee of Privy Councillors appointed to Inquire into the Interception of Communications" in October, 1957, it has been the established practice not to give information on this subject.

Nevertheless, on this one occasion, and exceptionally because these Questions on the Order Paper may be thought to touch the rights and privileges of this House, I feel it right to inform the House that there is no tapping of the telephones of hon. Members, nor has there been since this Government came into office.

The House will, I know, understand that the fact that I have felt it right to answer these Questions today in no way detracts from the normal practice whereby my right hon. Friend the Home Secretary and myself are unable to answer Questions relating to these matters.

§Mr. Russell Kerr: May I thank my right hon. Friend for his reply? However, is he aware that many hon. Members on both sides of the House believe, rightly or wrongly, that their telephones have been tapped? While the whole House would acquit my right hon. Friend of any knowledge or complicity in such a perversion of the nation's security arrangements, will he consult with my right hon. Friends the Home Secretary and the Paymaster-General—*[Laughter.]*—to make sure that some of our security people are not undertaking free enterprise of a rather smelly kind on this issue?

§The Prime Minister: On the issue of the belief of certain hon. Members that their telephones are being tapped, I would point out that my postbag and those of many other right hon. and hon. Members suggest that a very high proportion of the electorate generally are under the delusion that their telephones are being tapped. This delusion spreads to hon. Members and I should say that I used to suffer from it myself at one time.

As for the general position, I hope that my statement will be an answer to some of the scurrilous comment in the Press during the last three or four days about the attitude of the Government to this question and will also answer, I hope, some questions put by hon. Members on Monday and the usual Pavlovian titter which occurred when the name of my right hon. Friend the Paymaster-General was mentioned—not least because the only connection that he has had with this question was when I sought his advice on reviewing the practice about tapping Members' telephones when we came into office. He therefore shares such responsibility as I can take for the present arrangements.

§Mr. Donnelly: Is my right hon. Friend aware that this is an extremely serious matter and that three questions arise? The first is the criteria on which any telephones belonging to anyone are ever tapped. Will my right hon. Friend make it clear that there has been absolutely no change in the circumstances listed in the Report of the Privy Councillors?

The second point concerns who is entitled to authorise such tappings. Will my right hon. Friend make it clear that these people are known and identifiable, because it is a very important matter?

Thirdly, when the matter goes outside national security and the whole question of detection of crime, will my right hon. Friend give instructions that any extraneous information which may be discovered as a result of tapping will not go beyond the security authorities to anyone who is not a member of the security services?

§The Prime Minister: My answer referred to the tapping of telephones of hon. Members. As regards any other person or group of persons, the position is exactly as stated by the then Prime Minister to the House after the publication of the Privy Councillors' Report and I have nothing to add to or subtract from what was said then. Authority for tapping rests with my right hon. Friend the Home Secretary, as the Report made clear.

So far as the special case of Members of Parliament is concerned, as I have said, following the discussion I had, shortly after we took office, with the then Home Secretary, the policy has been laid down in the terms which I have again stated today.

§Mr. Jackson: Is my right hon. Friend aware that many hon. Members believe that both authorised and unauthorised tapping is increasing? Is he further aware that paragraph 130 of the Report of the Privy Councillors stated that '... there can be no certainty that the unauthorised tapping of telephones does not occur and it might even be done without the commission of a trespass on private or Crown property.'?" and that paragraph 131 states—

§Mr. Speaker: Order. Questions even on telephone tapping must be concise.

§The Prime Minister: The position regarding unauthorised tapping—and this also relates to the question put by my hon. Friend the Member for Feltham (Mr. Russell Kerr)—is as follows: any tapping that, in accordance with the rules of the Report, becomes necessary by any Crown servant concerned with the things covered in that Report, can only be done with the individual authority of my right hon. Friend the Home Secretary under very strict conditions.

If the question put by my hon. Friend the Member for The High Peak (Mr. Peter M. Jackson) relates to a practice which one understands has developed in other countries, and is causing concern here—tapping by private persons to steal industrial secrets, for example—that is a separate matter and does not come within the remit of Question and Answer in this House.

§Mr. Speaker: The hon. Member for The High Peak (Mr. Peter M. Jackson) did not get his question over. Would he like to put it now?

§Mr. Jackson: Is my right hon. Friend aware that paragraph 131 of the Report states that Parliament might consider whether legislation should be passed to make unauthorised telephone tapping illegal?

§The Prime Minister: That is an entirely different matter from the subject raised in the Questions on the Order Paper today. It has, however, been raised at Question Time with the Postmaster-General on past occasions.

§Sir T. Beamish: May I press the right hon. Gentleman on this point? Since the tapping and taping of private telephone conversations without the knowledge of the Post Office and without authority is much easier than many people imagine—and I assure the right hon. Gentleman that I am not suffering from delusions and would gladly give him confidential evidence—will the Prime Minister consider the question in paragraph 131 that the unauthorised tapping of private telephone conversations might be made an offence?

§The Prime Minister: I would be glad to consider any evidence the hon. and gallant Gentleman sends me. I know that my right hon. Friend the Postmaster-General would also want to consider it to see whether there was a case fully made out for dealing with "private

enterprise" telephone tapping of the kind that the hon. and gallant Gentleman has in mind. I hope, however, that the answer I have given to his and other questions will put into perspective some of the monstrous accusations made in certain newspapers over the past four days about the Government's attitude towards tapping of Members' telephones.

§Mr. Lubbock: Is the Prime Minister aware that one of the reasons for the widespread delusion which he has mentioned is the grossly unsatisfactory state of the telephone system as a whole? To give one example, when I tried to telephone someone yesterday, I burst in on another private conversation between two individuals on three consecutive occasions. Will the Prime Minister therefore ask his right hon. Friend the Postmaster-General to get a move on with improving the telephone system so that these allegations are not made?

§The Prime Minister: That is a separate question, which has been raised many times with the Postmaster-General. I notice that the level of the supplementary questions now is very different from the dramatic build-up given to this subject by some of the Conservative Press over the past three days.

§Mr. Dribberg: Is my right hon. Friend aware that at least two of his answers have implied quite clearly that there was tapping of hon. Members' telephones before the present Government came to power in 1964? Would he say anything more about that?

§The Prime Minister: I hold no responsibility for what was done in this matter before the present Government came to power, but it is fair to point out that the Privy Councillors' Report itself said that Members of Parliament should not be treated differently from members of the public. It is always a difficult problem. As Mr. Macmillan once said, there can only be complete security with a police State, and perhaps not even then, and there is always a difficult balance between the requirements of democracy in a free society and the requirements of security.

With my right hon. Friends, I reviewed the practice when we came to office and decided on balance—and the arguments were very fine—that the balance should be tipped the other way and that I should give this instruction that there was to be no tapping of the telephones of Members of Parliament. That was our decision and that is our policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it. I am aware of all the considerations which I had to take into account and I felt that it was right to lay down the policy of no tapping of the telephones of Members of Parliament.

§Mr. Frederic Harris: Can the Prime Minister tell me why any Labour Members should imagine that their conversations on the telephone are interesting enough for them to be tapped?

§The Prime Minister: I do not think that this matter, which raises very deep concern about the privileges and rights of hon. Members, is in any sense a party question. My decision that hon. Members' telephones should not be tapped was, of course, unrelated to the tapping of telephones of hon. Members of any particular party; and I am sure that the attitude of the previous Government was also completely unrelated to the party affiliations of any hon. Members concerned.

§Mr. Gordon Walker: I am very glad to hear the Prime Minister's decision that no hon. Members' telephones should be tapped, but would he agree that, in principle, there is a distinction between the privilege of a Member concerned in some proceedings in Parliament and the similarity of all Members with ordinary citizens in all other respects, and that it is important that this principle should be maintained and asserted?

§The Prime Minister: I certainly agree about that and I do not myself believe that this involves a question of privilege, as we understand it in the narrow sense in this House. My original Answer was drafted to make that clear. Someone has to take the decision one side or the other of this very, very difficult balance. With my concept of responsibilities to the House, I feel that, although the arguments are finely argued in the Report of the Privy Councillors, it has been right to alter the practice and to say that there should be no tapping whatsoever.

§Sir Ian Orr-Ewing: Is the Prime Minister aware that during the nine years which have elapsed since the Privy Councillors' Report was published, unauthorised tapping of telephones has become both much easier and much more ingenious and that, therefore, the recommendation of the Privy Councillors in paragraph 131 has now become urgent? As it is easy to make an unauthorised tapping of a telephone cable, will the Government give serious consideration to making it illegal?

§The Prime Minister: I agree about the seriousness, particularly if tapping comes to be developed in this country on the scale on which it has developed in other countries for use by one industrial company against another industrial company. This matter has been raised in the House before and it will be further considered. My answers have related not to unauthorised, but to authorised tapping, and I have stated the practice which we are following.

§Mr. Fitt: Would the Prime Minister agree to extend the assurances which he has given to the House to cover Members of Parliament in Northern Ireland? Is he aware that it is very well known that the Government of Northern Ireland indulge in telephone tapping for party political purposes?

§The Prime Minister: If my hon. Friend wants to send me any evidence which he has on that subject—

§Mr. Fitt: Will my right hon. Friend ask Captain O'Neill next time he sees him?

§The Prime Minister: —it will be studied with very great care. I can assure him that the answers which I have given this afternoon have related to all questions and practices connected with authorised tapping under the coverage of the White Paper and for which my right hon. Friend and I are responsible.

§Mr. Chichester-Clark: Is the Prime Minister aware that the question of the hon. Member for Belfast, West (Mr. Fitt) was the gross terminological inexactitude which he knows it to be and which he has never been able to substantiate in this House and which should not have been made?

§The Prime Minister: I asked for evidence, but this afternoon I was dealing with areas within the jurisdiction of my right hon. Friend.

§Mr. Fitt: On a point of order. Is my right hon. Friend aware that telephone tapping was admitted in the Northern Ireland Parliament?

§Mr. Speaker: The hon. Member must know that that was not a point of order.

ANNEX: Erskine May's Parliamentary Practice (2011) page 264 (extract) on the Wilson doctrine

In 1966 the then Prime Minister said that he had given instructions that there was to be no official tapping of telephones of Members of the House of Commons (known as the Wilson Doctrine). In exceptional circumstances the House would be informed.¹¹² The doctrine has been several times restated by the Prime Minister and most recently, in a case involving a Member, by the Home Secretary.¹¹³ The Committee on Standards and Privileges has concluded that in certain circumstances 'phone hacking', which it defined as 'gaining of unauthorised direct access to a remotely stored mobile telephone communication', in respect of Members' mobile phones could potentially constitute a contempt.¹¹⁴

¹¹² HC Deb (1966–67) 736, c 639; ibid (2001–02) 377, c 367W (and, for the House of Lords, HL Deb 1999–2000) 616, cc WA137–8).

¹¹³ HC Deb (2007–08) 472 cc 538–39. For examples of restatements by the Prime Minister, see HC (Deb) (2005–06) 444, cc 95–96WS; HC Deb (2006–07) 463, 2103W.

¹¹⁴ Fourteenth Report, HC 628 (2010–12).

ANNEX: UK Parliament recent Ministerial Answers to Parliamentary Questions on the Wilson doctrine

24 January 2011 House of Commons Debates, column 35W

Jonathan Edwards: To ask the Prime Minister whether there have been any changes to the Wilson doctrine since May 2010. [35701]

The Prime Minister: No.

3 July 2013 House of Lords Debates, column WA238

Lord Strasburger: To ask Her Majesty's Government whether the Wilson Doctrine on the interception of MPs' telephone calls still applies; whether it covers internet-based communications; and whether it applies to members of the House of Lords.[HL1217]

Lord Wallace of Saltaire: Though it has been the longstanding practice for successive Governments not to comment on surveillance or interception operations. I can confirm that the Wilson Doctrine still applies, and applies to both Houses I refer the noble Lord to the then Prime Minister Tony Blair's written answer to Norman Baker MP on the terms of the Wilson Doctrine on 19 December 2001, Official Report, column 367W and his subsequent confirmation that it continues to apply on 30 March 2006, Official Report columns 95 and 96WS. His earlier written reply to a question by Norman Baker on 4 December 1997, Official Report, column 321W, made it clear that the Wilson Doctrine applied to telephone interception and to the use of electronic surveillance by any of the three security and intelligence agencies. This is still the position.