Joint Committee on the Draft Investigatory Powers Bill – Information Commissioner's submission

Executive Summary:

- The draft bill is far-reaching with the potential to intrude into the private lives of individuals. The case justifying the measures, the necessity for them, their proportionality and the adequacy of compensatory safeguards, must be subject to detailed scrutiny.
- Parliament has a responsibility to scrutinise these provisions, not simply as they stand in the bill but in the wider context of surveillance generally.
- The law must be kept under ongoing review, with provision for effective post legislative scrutiny. A 'sunset clause' could ensure that this happens.
- The value of communications data to law enforcement is understood and is also vital to the Commissioner's own enforcement work.
- Little justification is advanced for the need to retain data for twelve months and the definition of any retention period needs to be evidence based.
- The Information Commissioner's role in auditing retained communications data needs strengthening with obligations on CSPs to cooperate combined with sanctions if they do not; greater clarity on access to CSPs' records; provision for retention notices; and a requirement for the Information Commissioner to be consulted on any codes of practice affecting the Commissioner's duties. Safeguards in relation to non-UK CSPs need clarifying.
- Internet connection records can be revealing and strong justifications for intrusion are required including the reassurance of post legislative scrutiny.
- Examples of the need for bulk personal data set warrants are not persuasive since equivalent provisions already exist in statute. The established approach could be used for data sets of concern. Consideration should be given to exempting certain data sets involving sensitive personal data, such as those, for example, relating to health data.
- Safeguards surrounding equipment interference and protecting privileged communications need reconciling and strengthening.

- Notices requiring the removal of electronic protection should not be permitted to lead to the removal or weakening of encryption. This technique is vital to help ensure the security of personal data generally.
- The simplification and strengthening of oversight arrangements is welcome, but should not be overstated, particularly the role of a Judicial Commissioner. The IPC role will be vital including in improving transparency. The role must be independent and inspire public confidence. Reports should include the value of data to law enforcement outcomes so that continued need and justification can be assessed. The process for notifying individuals of any errors should be strengthened.

Introduction

1. The Information Commissioner has responsibility in the United Kingdom for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations 2003, as amended (PECR). The Information Commissioner also has a more limited supervisory role under the Data Retention Regulations 2014 (DRR 2014) created under the Data Retention and Investigatory Powers Act 2014 (DRIPA).

2. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and taking appropriate action where the law is broken. His activities also include providing advice on policy and other initiatives that engage information rights concerns.

3. This evidence will focus on those aspects of the draft bill that fall within the Information Commissioner's direct regulatory remit. It also covers the other aspects of the draft bill that have an impact on the privacy of individuals.

4. The Information Commissioner recognises that there are significant and ever developing challenges that law enforcement and security bodies face in fulfilling their role. These challenges are not limited to the threats themselves but also involve the changing technological means that may be used. The Commissioner recognises that the provisions in the draft bill are aimed at helping law enforcement and security bodies respond to these evolving challenges. But it is not sufficient to give wide ranging powers without very careful consideration of the justification, the pressing needs they are meant to address, the proportionality of the measures themselves, and adequacy of any compensatory safeguards. To fail to make such a balanced assessment risks eroding the very freedoms those measures are intended to protect. Respect for an individual's private life is one of our cherished freedoms.

5. The draft bill is welcome to the extent that it brings together disparate existing measures into a single legislative context with the opportunity for proper parliamentary scrutiny of the whole package.

6. Parliament has a significant role to play not only in scrutinising the case justifying such measures, their proportionality, and the adequacy of safeguards. It has an important role in considering these measures in the wider context of the ever increasing general

surveillance of individuals. All of us leave digital footprints as we go about our everyday business, whether using a mobile phone, sending an email or text message, visiting a website, or checking social media. These digital footprints do not just show activities but can record our locations too. We feature increasingly on databases compiled in many different and specific contexts by both public and private sector organisations. There are significant features of the draft bill that touch on the lives of all citizens, not just those suspected of involvement in criminality.

7. There are also other forms of surveillance by public bodies. Examples include widespread automatic number plate recognition systems (ANPR) which results in an average of around 30 million records of the routine use of vehicles being collected every single day. These records are not linked to any suspicion of criminal activity, but they are nevertheless retained in a central database for a number of years. Similarly, access to airline passenger name records for those who fly in or out of the UK can be extensive and largely unseen. Ally to this the extensive network of CCTV cameras and this technology's developing capabilities and there is an increasing danger that we are living in a society where few aspects of our daily private lives are beyond the reach of the state. This poses a real and increasing risk that the relationship between the citizen and the state is changed irreversibly and for the worse[1].

8. Parliament has a vital role in considering the draft bill not only on its own merits but also in the broader context of all these wider developments, many of which have evolved with little, if any, statutory underpinning - but always in the name of improving public security and the capabilities of those who are there to protect us.

9. Measures in the draft bill which require more extensive information to be retained, make that information available to others in different contexts than for which it was originally collected, and store it for prolonged periods, engage concerns about core data protection and PECR safeguards. These protections include appropriate transparency, individual control, purpose limitation, data minimisation and ensuring effective security measures. These protections are aimed at minimising information risk (such as unwarranted intrusion or the consequences of a security breach) and providing individuals with confidence that their information will be respected and safeguarded.

[1] see Information Commissioner's 2010 report to Parliament on the state of surveillance https://ico.org.uk/media/1042386/surveillance-report-for-home-select-committee.pdf

10. These protections are underpinned by Article 8 of the European Convention on Human Rights (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter). Article 8 of the Charter provides a specific right to data protection, emphasising its importance to citizens in the modern world. None of these provisions are absolute rights and all recognise the need to accommodate other important societal needs. Our own DPA has its provisions limited where there are statutory requirements, national security may be affected, or law enforcement purposes likely to be prejudiced[2].

11. Judgements of the courts now clearly reflect the importance of these protections, both at domestic[3] and European[4] level. These cases point to the importance of properly assessing and weighing the impact on the fundamental right to privacy and data protection. The new General Data Protection Regulation, recently agreed, will come into force in 2018 and will increase the potential of jurisprudence from the Court of Justice of the European Union (CJEU) impacting on data protection and the relationship with fundamental rights. From the existing case law it is clear that the following guarantees should be in place when personal data is being processed by national security bodies:

- Processing based on clear, precise and accessible rules
- Necessity and proportionality with regard to the objectives pursued
- Existence of an independent oversight mechanism
- Effective remedies for the individual

12. Parliamentary scrutiny is an essential component not only when the legislative measures are considered initially, but also through regular detailed post legislative scrutiny and review. The Information Commissioner has previously recommended the inclusion of 'sunset clauses' to ensure that the threats the legislation is intended to address still exist, the measures are effective in addressing these, and the right balances are struck in practice. The draft bill is far reaching and has the power to affect the lives of all citizens to differing degrees. For these reasons, the bill should include a sunset clause or other provisions requiring effective post legislative scrutiny. This would ensure that measures of this magnitude remain necessary, are targeted on the right

[2] See, for example, exemptions provided under DPA sections 28, 29 and 31.
[3] Secretary of State for the Home Department -v- David Davis MP and others [2015] EWCA Civ 1185
[4] Digital Rights Ireland (Advocate General's opinion) [2013] EUECJ C-293/12 (12 December 2013); also Maximilian Schrems v Data Protection Commissioner case (C-362-14)

areas, and are effective in practice. To fail to make this provision risks undermining public trust and confidence. It will also enable the legislation to be considered in the light of the latest jurisprudence from the CJEU and European Court of Human Rights (ECHR)

13. The Information Commissioner's view on the key aspects of the draft bill that engage his statutory functions are set out below, followed by his comments on other provisions of the draft bill.

Communications Data

14. The amalgamation of a number of separate provisions relating to the retention of communications data within the one legal instrument is welcome, particularly some of the detailed provisions which previously existed in the Data Retention Regulations 2014 (DRR 2014) rather than in the primary legislation. There is still a reliance on codes of practice to provide additional details and safeguards. It is important that the likely content of these codes is available for scrutiny during the passage of the bill so that the whole regulatory framework including any limitations is clear.

15. The Information Commissioner does understand the value of communications data for investigatory purposes. He has first-hand experience of its evidential value in relation to his own enforcement and prosecution powers and it is important that he is specified in Schedule 4 as a relevant public authority. In particular the power to acquire communications data is essential to his work in prosecuting the unlawful obtaining and disclosure of personal data and tackling nuisance telephone calls and texts. The lack of this data would impair his ability to take action in areas of increasing public concern.

16. The concept of Communication Service Providers (CSPs) retaining data for longer than needed for their own business purposes and then making this available to specified bodies on request is carried forward from existing legislation. This approach is preferable to the creation of a central data centre where data could, in theory, be transferred and held under state control. The period for retention remains at twelve months though there is little evidence provided explaining why this is the appropriate period. The justification for this period should be made clear, especially as it should be possible to provide evidence of the number of such requests and their law enforcement outcomes based on current arrangements.

17. The Information Commissioner has built up his own experience of exercising his current audit functions under DRR 2014 in respect of retained data and has identified areas where the provisions surrounding this can be improved.

18. The Information Commissioner will be required under clause 182 to audit the integrity, security and destruction of retained data. This aligns with his current role under the DRR 2014. As currently drafted, the draft bill does not require CSPs to cooperate with the Information Commissioner's audits on the integrity, security or destruction of data held under a relevant notice from the Secretary of State. The existing position under the DRR 2014 facilitates this through the retention notices given to CSPs and their compliance with the Retention Code of Practice. Putting a duty on the Information Commissioner to undertake an important oversight role without the accompanying powers in primary legislation to fulfil this duty is a deficiency that needs remedying. For example, under section 40A of the DPA, the Information Commissioner has the power to serve an assessment notice on a government department or NHS body in order to undertake a compulsory audit.

19. Whilst this has not prevented the Commissioner from complying with his obligations to date there have been challenges from CSPs around the extent of the Commissioner's powers. Putting a duty on CSPs to cooperate could also make clear it covers all 'retained' data covered by a retention notice including data retained in CSPs' disclosure systems, another area of query. It is our experience, from our wider audit role under the DPA, that organisations cooperate more readily where we have a clear statutory power of audit. Such provisions could also include sanctions for failing to cooperate. The draft bill could also clarify that the offence provisions at section 59 of the DPA which cover the confidentiality of information provided to the Information Commissioner also extend to the performance of his duties under clause 182.

20. The draft bill should also provide for the Information Commissioner to be directly notified about retention notices being issued, varied and revoked. Given that the Information Commissioner's powers of audit relate to the Secretary of State's retention notices there should be a proactive duty on the Secretary of State to inform the Information Commissioner.

21. Schedule 6 of the draft bill sets out the ability of the Secretary of State to issue relevant codes of practice. The current Retention Code sets much of the practical details surrounding the retention of data by CSPs and the Information Commissioner's role in

supervising aspects of their activities. Given the Commissioner's interest in this code he should be added to the list of bodies with whom the Secretary of State must in particular consult when producing a code[5] .

22. The importance of the arrangements that are set out in the Retention Code are illustrated by current provisions in the DRR 2014 detailing the way in which communications data are to be retained by CSPs.

23. Retaining more data for longer inevitably engages concerns about the security of the retained data. Regulation 7 of the DRR 2014 currently requires CSPs to hold data securely and specific security arrangements for the retention of data by CSPs are set out in chapter 6 of the Retention Code. This also provides for the Home Office to include specific security requirements in data retention notices and to provide security advice and guidance to all CSPs who are retaining data. The Retention Code envisages retained data being kept in a dedicated retention and disclosure system which is securely separated from a CSP's business system. However the Retention Code does provide for an alternative, and data may be retained in business or shared systems subject to specific security safeguards being agreed with the Home Office.

24. Whilst it may be possible to ensure that normal business systems holding retained data have the appropriate security safeguards in place such systems are, by their nature, aimed at facilitating wider business use with greater levels of access. This may pose more of a challenge not only for CSPs to ensure appropriate security but also for the Information Commissioner to audit. Ensuring there is a requirement, either on the face of the legislation or in a subsidiary code of practice that requires the data to be retained separately from normal business systems may help reduce security risks. This is all the more important given retention of internet connection records (ICRs).

25. Clause 182 requires the Commissioner to audit CSPs who are complying with retention notices under Part 4 of the draft bill. Clause 79 makes clear that persons outside the UK can receive such notices and must have regard to these. It is not clear whether this would also include complying with the safeguards in clause 182 and, if so, how this would be achieved in practice with a CSP in another jurisdiction. This needs clarifying as, otherwise, important compensatory safeguards may not be available in practice.

[5] See schedule 6 section 5(2)

26. One potentially welcome feature of the draft bill is the filtering mechanism proposed at clause 51. If this mechanism is effective this could reduce privacy intrusion such as when trying to resolve IP addresses. However how this would work in practice would require some attention and close review by the Investigatory Powers Commissioner (IPC) to ensure that it is achieving its aims and not being used in inappropriate ways.

Internet Connection Records

27. One new feature in the draft bill surrounds the requirement on CSPs to retain Internet Connection Records (ICRs). Although these are portrayed as conveying limited information about an individual they can, in reality, go much further and can reveal a great deal about the behaviours and activities of an individual. Such records would show particular services that are connected to and this could be a particular website visited although not the pages within them. This could lead to a detailed and intrusive picture of an individual's interest or concerns being retained and then disclosed. There is also increased risk to all individuals if such retained data are subject to a security breach and that detailed picture of their interests and activities becomes available to third parties. This could lead to unintended consequences and again reinforces the need for specified security requirements for CSPs to safeguard against this risk.

28. Retaining ICRs is an area where there needs to be strong justification and if this is made on the basis of an assertion of need in advance of a power being given then there needs to be effective post legislative scrutiny to judge the magnitude and nature of the records retained and the use that was made of these in practice including law enforcement outcomes.

29. There are challenges in resolving IP addresses down to particular identifiable individuals which may make such data of less value in practice. It is understood that in 2014 Denmark repealed its provisions that are similar to the draft bill as they were unable to achieve their objectives in practice. It is not sufficient for the IPC to report on the working of the arrangements; it is the use of the information and its value that is the indicator of whether such intrusion is necessary and proportionate. This information would need to be provided as part of any post legislative scrutiny.

30. The requirement to retain ICRs also adds another dimension to the Information Commissioner's role extending the records that must be supervised. At present the Commissioner receives specific grant in aid from the Home Office to undertake his functions under

the DRR 2014. That is based upon a predicted number of audits and a dedicated audit team has been created for this purpose. If the nature or number of records retained increases this will require appropriate funding for this additional work to ensure the audit controls remain an effective safeguard. This will also be true if there are requirements to audit CSPs providing services from outside the UK.

Bulk personal dataset warrants

31. The provisions in the draft bill around the acquisition of bulk personal data sets require particular scrutiny. These provisions are limited to the security and intelligence services. The examples given in the Guide to Powers and Safeguards refer to telephone directories and the electoral roll. These datasets are already available to various agencies often under specific statutory provisions. For example, Schedule 1 of the Counter-Terrorism Act 2008 amends the Representation of the People (England and Wales) Regulations 2001 to require the supply of the full electoral register to the security services. The relevant specific legislation can be amended if there are issues around any limitation affecting availability to the security and intelligence services as this amendment demonstrates. The examples in the Guide seem particularly inappropriate given the existing availability of these datasets and others, including vehicle keeper and driver data, to conventional law enforcement bodies.

32. There are also limitations on the applicability of the DPA where this may affect national security (s.28) with a Minister of the Crown being able to provide a conclusive certificate to that effect only challengeable by way of judicial review. This can mean that data sets are already disclosed, such as, for example, congestion charging data held by Transport for London to the Metropolitan Police. It is not clear why existing provisions are considered insufficient. A clearer justification needs to be made of the types of data that are not currently available under existing provisions and why warrant provisions are necessary. These warrant powers should not be available in addition to existing statutory access arrangements.

33. Given the increasing amounts of personal data generated and held in data sets this could be a particularly far reaching and intrusive provision. Whilst the safeguards surrounding authorisation are welcome, there may be some data sets that should be exempted. An obvious example is health data where there are other substantial public policy reasons why such data should not be available in bulk. There is increasing centralisation of records such

as with the Care.data programme and other efforts to create significant national level collections of health related information.

34. There are no arrangements for auditing the acquired data and this omission should be rectified. This could include ensuring that only information of value is retained, with measures implemented to delete personal data that is not of interest.

Equipment Interference

35. Equipment interference has the potential to be intrusive and it could also damage the very systems subject to interference with unforeseen consequences. It is not clear why a differential approach to the warrant authorisation process has been adopted, with the Secretary of State having a role in certain cases but chief law enforcement officers in others. The same is true of with modifications where a Judicial Commissioner reviews law enforcement bodies but not intelligence agencies. There should be a consistent and appropriately robust approach adopted.

36. There are also differences in the way safeguards are applied. Clause 85 sets out specific safeguards for Members of Parliament but these are not extended to others who are involved in privileged communications protected elsewhere in the draft bill. There should be consistency of approach.

Maintenance of Technical Capability-Removal of Electronic Protection

37. Clause 189 permits the Secretary of State to impose obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data. This could be a far reaching measure with detrimental consequences to the security of data and safeguards which are essential to the public's continued confidence in the handling and use of their personal information.

38. If the possible obligations surround the weakening or circumvention of encryption then this is matter of real concern. The Information Commissioner has stressed the importance of encryption to guard against the compromise of personal information. Weakening encryption can have significant consequences for individuals. The constant stream of security breaches only serves to highlight how important encryption is towards safeguarding personal information. Weakened encryption safeguards could be exploited by hackers and nation states intent on harming the UK's interests. This evidence has already pointed to

potential concerns, at paragraphs 23-24, about retained communications data being held on normal business systems and the increased challenges of ensuring appropriate security. These concerns would increase still further if necessary electronic protections were weakened or removed.

39. The practical application of such requirement in the draft is unclear in the draft bill and the accompanying Guide to Powers and Safeguards does not provide specific details to enable the full extent of the provision to be assessed.

40. Sub-clause 190 (8) requires that the existence of any such a requirement is not disclosed so there is no transparency around the existence of measures that could affect encryption of an individual's information. This clause and Clause 191 do provide for an operator to ask the Secretary of State to review the requirement and the IPC and Technical Advisory Board need to be consulted. However, the Secretary of State can still proceed with the requirement irrespective of any contrary view expressed by either body. This seems a significantly weaker position than other aspects of the draft bill that requires an actual approval.

Oversight Arrangements

41. Central to the proposed oversight arrangements is the creation of the IPC bringing together existing functions. The Information Commissioner welcomes this as the existing landscape is complex. He took the initiative in producing a 'surveillance roadmap' to set out the various functions to try to explain the different powers and responsibilities of the various commissioners. The proposals in the draft bill are a welcome simplification. It is important that the IPC receives the necessary funding to provide the high level of public reassurance this role is meant to provide. It is also important that the IPC is independent.

42. It is important that commissioners with a corresponding interest in issues do cooperate and we have experience of setting out more formal arrangements such as working with Interception of Communications Commissioner to develop a memorandum of understanding over the reporting of security breaches by CSPs. There will be further scope for sensible cooperation, given the supervisory role of the IPC, to ensure that matters that also affect data protection compliance concerns or the duties under clause 182 are referred to the Information Commissioner.

43. Ensuring individuals have effective rights of redress where powers are used incorrectly must be an essential component of the regulatory framework. The draft bill includes provisions that should help improve on the existing position such as the IPC examining errors and the impact of these on individuals. These are then referred to the Investigatory Powers Tribunal to consider whether an individual affected should be contacted. This still leaves a significant discretion in the hands of these two bodies. Making individuals aware of errors unless there are significant reasons not to do so, such as prejudicing an ongoing or planned operation/investigation, should be the norm.

44. Another significant difference from the current landscape is the inclusion of Judicial Commissioners as part of the IPC arrangements. They represent what has been described as a 'double lock'. Clarity is important when describing this arrangement. The Judicial Commissioners review a decision, primarily one made by the Secretary of State, through applying judicial review principles to that decision such as the reasonableness of the action. This is not quite the same as approving an application on their own initiative and from first principles. Whilst this is a useful additional oversight role, it is not the same as a direct application to a judge for a warrant. A decision refusing to approve a warrant may also be subject to review on application to the IPC by the Secretary of State who may then overrule that decision. To refer to this process as a 'double lock' may be overstating this safeguard as it is essentially a more limited review process and even then subject to appeal.

45. It is important that there is appropriate separation of roles within the IPC to ensure that its oversight mechanisms are not perceived as being compromised by its authorising role, or the Judicial Commissioners falling within that framework. There must be no impression of 'marking their own work'. The IPC must provide annual reports but the mandatory content of that report, specified at clause 174, does not include anything around the value of that data to the bodies who gain access to data in terms of results achieved thereby. This is essential to judging whether measures are necessary and strengthens the need for effective post legislative scrutiny. Transparency would also be aided by information revealing the extent of the use of powers under the legislation. This may need to stop short of revealing the organisations who have received warrants or notices but information could be provided on the number of warrants and notices that have been served or are active at any one time. Expanding the breadth of the IPC's reports will also be a welcome step towards further increased transparency, a prerequisite for helping maintain public trust and confidence.

Conclusions

46. The draft bill provides an important opportunity for full consideration of the range of investigatory powers provided to public bodies and the overall effects on citizens. Ensuring that these powers are put on a clear and predictable legal basis is essential. The inclusion of mechanisms to ensure that proper processes are followed with appropriate review is vital. The draft bill includes some welcome features. But all these need to be weighed against a clearly articulated pressing need and rationale showing how and why the measures are necessary to achieve these. More needs to be done such as around retention periods for communications data, the need for all internet connection records, and range of personal data sets available under warrant.

47. It is also essential that there is appropriate transparency in the operation of arrangements and the reports of the IPC will have an important role to play. But there also needs to be more formal post legislative scrutiny of the need for measures with evidence provided of the actual outcomes resulting from the measures. Only then can the continued need and proportionality be judged. Including a sunset clause should ensure this happens.

48. Safeguards also need further attention including strengthening the Information Commissioner's powers where these act as compensatory safeguards placing specific duties on CSPs to cooperate with him and prescribing sanctions for those who do not. There are also important additional safeguards that could be introduced to reduce the risk of security breaches in relation to retained data. Similarly powers to require the removal of electronic protection must not extend to removing or weakening encryption which plays an essential role in helping ensure the security of personal information.

49. The oversight provisions including review by a Judicial Commissioner are a positive step, but fall short of full judicial approval of measures. There can also be a strengthening of the circumstances where individuals are made aware of errors that have affected them giving them the opportunity to take their own action and hold authorities to account. Expanding the range of matters that the IPC must report on to include a review of the overall operation of the regime would also be a welcome step towards improved transparency.

Christopher Graham
Information Commissioner
18 December 2015