The Information Commissioner's response to the Home Office consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data

Introduction

1. The Information Commissioner (the '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). These powers and duties in relation to retained communications data have been carried forward under the Investigatory Powers Act 2016 (the IPA).

2. The Commissioner 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. Her duties include providing advice on policy and other initiatives that engage information rights concerns. The Commissioner is responsible for regulating the aforementioned legislation and will continue that role as regulator for upcoming changes to data protection legislation: the General Data Protection Regulations (GDPR) and Data Protection Bill which are due to come into effect in May 2018. She also has powers of audit in respect of communications data retention systems under the IPA.

The Commissioner's interest

3. The Commissioner has two separate interests in this matter. Firstly, as a regulator in the arena of privacy and data protection, she recognises the critical importance of striking an appropriate balance between the rights of individuals and the need to ensure effective

law enforcement and she continues to take a close interest in how this balance is struck by the Investigatory Powers Act. It is of fundamental importance that the rights and freedoms of individuals are not eroded without justification, in the interests of security and law enforcement.

4. Secondly, the Commissioner also has powers to obtain and make use of communications data in the course of her regulatory enforcement activities. There are elements of her duties which cannot be effectively pursued without such powers. For example, in her role as regulator of PECR, the acquisition of communications data is essential in determining when a person has misused electronic communications channels, for example in sending mass marketing emails or telephone calls to recipients who have not opted-in to receiving them.

5. Historically, such offences under PECR (and associated offences under the DPA, including the harvesting and brokerage of personal contact details in order to undertake such marketing) have not been classified as 'serious crime' and have not been subject to custodial sentences in order to meet defined thresholds of 'serious crime'. The Commissioner has previously argued that the extent of such activity (even in purely numeric terms), and the potential effect on individuals, merits such a classification.

6. The Commissioner welcomes the amendments proposed, in the classification[1] of any offence committed:

    - by a person who is not an individual [ie, a body corporate]; or
    - which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy

    as 'serious crime' for the acquisition of events data. This would permit her to continue to obtain communications data as evidence where companies, and individuals, are committing offences affecting an individual's privacy under PECR and the DPA.

7. The Commissioner is nevertheless concerned that a body corporate may commit offences of a minor or largely technical nature, and ought not to be subject to the retention or acquisition of communications data in circumstances where this is unwarranted. Consideration should be given to putting an appropriate threshold in place for the retention and acquisition of such data.

[1] See proposed amendments to the IPA, sections 86(2A)(b) and 87(10B)(b)

8. The Commissioner notes the remarks on page 16 of the consultation, that *'communications data may be of particular use at an early stage in an investigation, at which point the seriousness of the offence concerned may not be fully known'*. This is undoubtedly true in many instances, however this should not be used as justification for the acquisition of communications data on a speculative basis, or where there are no reasonable grounds for suspicion that a genuinely serious offence may have been committed. It should not simply be sufficient for an offence to meet the criteria at sections 86(2A)(b) or 87(10B)(b), there should be reasonable grounds to conclude that any offence is of a sufficiently serious nature.

Communications data and telecommunications operators

9. The Commissioner recognises the view expressed, that the definition of communications data has been left intentionally broad within the IPA, in order to maintain flexibility in the reach of the legislation for future technological developments. Similarly, the definition of telecommunications operator and/or communications service provider (CSP) are very broad and might, on a literal reading, give rise to unexpected consequences such as the potential inclusion of domestic WiFi systems. She is therefore of the view that the definitions could be usefully clarified within the Code of Practice in order to exclude elements where there is clearly no intention to apply the IPA, as the Code may be more easily amended as necessary in light of future technological developments.

The specific requirements of the judgment

10. The judgment anticipates that limits may be set to the collection of communications data by way of geographical restrictions, and the Government response acknowledges that a retention notice may make provision for geographic, and other, restrictions where appropriate. The response also notes the requirement on the Secretary of State to take various factors into account when making a decision to require the retention of communications data under the IPA.

11. The DPA, the GDPR and associated Law Enforcement Directive and the Data Protection Bill currently before Parliament all require that no more personal data is processed than is necessary for the purpose. It is important, therefore, that these restrictions (whether geographic or otherwise) are employed wherever possible and do

not merely exist as possibilities which are not actually used in practice because it may be difficult to determine in advance what data may prove useful to an investigation. To that end, the Commissioner acknowledges the proposed changes to section 88 of the IPA, in respect of the factors to be taken into account by the Secretary of State when preparing a data retention notice. As drafted, these factors are very broad, namely:

> […] the appropriateness of limiting the data to be retained by reference to -
>
> i. location, or
> ii. descriptions of persons to whom telecommunications services are provided

12. The Commissioner believes that in order to be consistent with data protection legislation the Secretary of State will need to interpret such provisions restrictively, so that the presumption is that any notice will be drafted narrowly by default, rather than simply requiring consideration (however cursory) of the 'appropriateness' of limiting the data. This could be reflected in the Communications Data Code of Practice, for example, at section 17.17 where the factors to be taken into account by the Secretary of State could include a requirement to construct the notice as restrictively as is reasonably possible, by default.

13. The consultation addresses the security of data retained outside the EU. The proposal is that this should amount to an adequate level of protection required by EU laws. Adopting an approach of ensuring adequate levels of protection is welcome. The United Kingdom's withdrawal from the EU will mean that, over time, levels of protection set out in EU legal instruments will no longer have legal effect in the UK. It is not clear whether the intention is to maintain that link with EU law levels of protection or to root this back to the standards that will be required by UK law once it leaves the EU. Whilst in practice both may have equivalently high standards it should not be the case that the requirement to have an adequate level of protection as required by EU law falls away to no level of protection once EU laws no longer apply in the UK.

14. The consultation considers the perceived difficulties around the general notification to individuals that their data has been accessed. The proposal is that no notification is provided as this may adversely affect law enforcement interests. This seems an over generalisation and a more case by case approach should be considered. The example of the use of communications data for locating a missing person illustrates this. It presumes that a missing

person has no knowledge of the technique of locating a mobile phone to trace its user's whereabouts. Given that the consultation document itself is quite open about this technique and the use of location based services on mobile phones is commonplace, it is less likely that revelation of the use of data will result in changes in future behaviour. Indeed it may well be the case that a 'missing person' is not actively seeking to avoid being found, or is at risk of harm.

15. The Commissioner notes the Government view as to the non-applicability of the CJEU judgment to the retention or acquisition of communications data for national security purposes. For the reasons set out in the consultation document, she concurs with this view, however she notes the provisions in part 4 of the Data Protection Bill, which relate to processing of personal data by the Intelligence Services and notes that the exemption at current clause 108 of the Bill still retains a requirement that any processing be lawful, and conform to a condition set out at Schedules 9 or 10 (as appropriate). The requirement to process data lawfully will require conformity with the relevant provisions of the IPA, but also the Human Rights Act 1998, and consideration as to the necessity and proportionality of any interference with those rights.

Draft Code of Practice

16. As a designated statutory consultee for the draft Code of Practice, the Commissioner has provided detailed comments on previous draft versions. This consultation response will therefore not examine the draft in detail, as the Home Office is already aware of the Commissioner's specific views. However she would like to highlight key thematic areas which may benefit from further consideration by the Home Office.

17. The Commissioner acknowledges the unique role she has to play in the provisions under the IPA in relation to the powers to audit the retention of communications data under this Act. In the Code of Practice, there is reference to the need for discussion and review between the Commissioner and the Home Office on cases which might arise. The Commissioner welcomes engagement with the Home Office, but reminds all parties that the powers and duties conferred on her under the IPA are without prejudice to the powers conferred on the Commissioner under data protection legislation. Under the imminent changes to this legislation, the Commissioner's audit powers will be strengthened and she will have the capacity to undertake compulsory data protection audits, not just on

government departments but on all data controllers. The Commissioner is also able to take further independent enforcement action, if necessary.

18. The draft Code of Practice makes clearer the various systems and processes subject to the Commissioner's oversight activities. The draft code reflects the Home Office view that the Commissioner's audit powers under this legislation do not extend to communications data retained in separate stores such as for the purposes of disclosure. Whilst the draft code makes clear that this does not preclude this data from the Commissioner's general powers under data protection legislation, this does result in a different level of supervision for essentially the same retained data that merits the additional specific supervisory safeguards in other contexts.

19. The Commissioner welcomes the recognition in the draft code that data retention notices could place obligations on CSPs to submit to her security audits. Whilst the IPA sets out a statutory responsibility for the Commissioner to provide oversight of the security of retained data, there is no reciprocal obligation placed on CSPs to comply with audit requests. Although the Commissioner would prefer her power of audit to be on the face of the legislation, inclusion of the power within binding data retention notices is to be preferred to inclusion solely within the Code of Practice.

20. The Commissioner is also mindful that there should be no scope for confusion about who is responsible for funding any necessary security remediations. We have raised this issue with the Home Office directly so action can be taken to resolve this uncertainty.

21. The Commissioner recognises the further clarity provided in the current draft on the usage of a request filter and the data controllership of the data processed, particularly as this service is likely to be provided through third parties under contract. There is no indication about what happens to data that is not disclosed after a search through a request filter, and what the retention period for information processed in the filter is, ie within the filter itself. Might there be circumstances, for example, where data is retained within the request filter after it has been deleted from a CSP's systems under the statutory retention period set out in the IPA? These are matters which may usefully be addressed in this Code.

22. More broadly, users of the Code may benefit from greater clarity on which party will be the data controller, and which a data

processor, or whether parties may be joint data controllers, through the different stages of data retention and filtering. For example, if a CSP may not access retained data (which it does not hold for its own business purposes), without the consent of the Home Office, the CSP is clearly not in a position to determine the manner and purpose of the processing of that data for itself, and will not be a data controller for it. Responsibility for data security rests primarily with the data controller, which should instruct its data processors accordingly, however under new DP legislation, both data controllers and processors can be liable for enforcement action in the event of data breaches.

23. The Commissioner has expressed concern about the requirement for the removal of encryption in the transferring of retained data, as encryption forms an essential safeguard. While there is a recognised need for information retained to be presented in an intelligible form, there should be assurance that encryption is not removed, to ensure that data communication remains secure.

24. Finally, one of the key principles of data protection is the retention of personal data only for as long as it is necessary. The Commissioner would welcome requirements in the Code about the need to review retention periods of communications data within the maximum period of 12 months. It should not be assumed that just because a statutory 'long-stop' retention period is specified, that all data should be retained for this length of time. The Code of Practice could serve as a useful prompt for due consideration of how long data should actually be retained.

Information Commissioner
18 January 2018