Regulation of Investigatory Powers Act Consultation: Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice

Response from the Information Commissioner

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

2. The Information Commissioner's response to this consultation is founded on his roles to help ensure compliance with the DPA and PECR. This includes his investigatory and enforcement functions which involve the acquisition and use of communications data under the Regulation of Investigatory Powers Act 2000. This response also addresses the measures necessary to enable him to perform additional functions required under the Data Retention Regulations 2014 (DRR).

3. The Information Commissioner is required under regulation 9 of the DRR to audit compliance with requirements and restrictions in relation to the 'integrity, security or destruction' of data retained by virtue of a notice under s.1 of the Data Retention and Investigatory Powers Act 2014 (DRIPA). He has the same duties under regulation 15(6) of the DRR in respect of communications data retained by virtue of the code of practice under s.102 of the Anti-terrorism, Crime and Security Act 2001 (ATCSA). Neither the DRR nor the primary legislation referred to provide the Information Commissioner with specific audit powers over Communication Service Providers (CSPs) who are retaining communications data under either the requirements of DRIPA or ATCSA. His powers to undertake audits of CSPs by virtue of his powers under regulation 5B of the PECR or more general assessment notice powers under the DPA are also insufficient to discharge his duties under the DRR.

4. The Commissioner's ability to undertake these audit functions depends largely upon requirements placed upon CSPs by retention notices issued under DRIPA and requirements in the DRR to follow the Retention of Communications Data Code of Practice (the retention code). This means that the provisions of the retention code itself and the notice (template at

Annex A to the code) are of crucial importance to delivering the intended safeguards and the Commissioner's role in ensuring these are applied in practice.

5. The Commissioner was consulted during the drafting of the retention code. This was welcome and has helped to ensure that it provides the necessary level of guidance to CSPs to help ensure that they have sufficient information to address their obligations surrounding security, integrity and destruction of data and to assist the Commissioner with his auditing of these aspects of their activities. The Commissioner also welcomed the positive discussions on the provision of adequate additional resources to discharge his functions under the DRR and looks forward to the necessary resources being provided before he commences this work.

6. Prolonged retention of data inevitably increases potential privacy risk. Ensuring that:
    - the retention code provides the guidance on the necessary safeguards around retention and this is followed by CSPs in practice,
    - the Commissioner has the necessary information made available to him by CSPs when undertaking audits and
    - the Commissioner has the necessary resources to provide the appropriate quality and frequency of audit to ensure that the safeguards are being followed in practice

    are all essential for providing reassurance to those whose communications data are retained for longer as a result of the DRIPA and the DRR.

7. The Commissioner has the following comments to make about specific provisions in the retention code where changes should be considered:

Retention code reference	Information Commissioner's comments
1.7	The Introduction draws attention to the Commissioner's duties to audit compliance. The introduction should make clear the CSPs obligations related to these duties as it is CSPs that must follow the code.
2.18	CSPs may also retain data under the voluntary code of practice under ATCSA. Although individual CSPs may also be subject to a retention notice, where the Information Commissioner receives notification of the issuing of a notice to ensure he can discharge his audit functions, there is no mechanism for making the Information Commissioner aware of where ATCSA voluntary retention arrangements are in place. It may become apparent during an audit that such arrangements are in place. Relying

	solely on this runs the risk that the need to audit this voluntarily retained data is not addressed in preparations for an audit. Similarly if communications data are voluntarily retained by a CSP not subject to a retention notice the Information Commissioner would be unaware. This may adversely affect the discharge of his duties under regulation 15(6) of the DRR. In order to avoid this potential problem the Secretary of State could notify the Information Commissioner where she is aware of such voluntary arrangements. If this will not identify all those CSPs where voluntary retention arrangements are in place and subject to audit then the code should include a requirement on CSPs to provide notification of their ATCSA voluntary retention to the Information Commissioner. This should include a duty to notify if voluntary retention subsequently ceases.
3.10	The provisions requiring prior consultation by the Secretary of State with CSPs before issuing a notice and the provision of advice and guidance in preparation should include the Information Commissioner's audit role and the CSPs' willingness and preparedness to assist with that. This would be a helpful reinforcing point made at the outset to help guard against confusion on their part over the Information Commissioner's powers to audit them.
3.15	The factors that the Secretary of State must take into account when deciding whether to issue a retention notice should also include the ability of the CSP to put in place the necessary safeguards around the security, integrity and destruction of retained data. The factors should also include the CSPs' commitment to the auditing of these measures by the Information Commissioner.
3.22	The requirement to send a copy of the retention notice and other relevant information to the Information Commissioner is essential to him being able to carry out his functions. This provision is particularly welcome. It could be made clearer that other relevant information may include where notices have been amended or withdrawn, referencing chapter 4.5, and where the Secretary of State is aware of voluntary retention under ATCSA. The reference to 'chapter 5' is incorrect. The Information Commissioner's duties are listed in chapter 7.
3.23	This section on the matters to be included in a notice should include the requirements on the CSP to permit audit of the security, integrity and destruction of the retained data by the Information Commissioner. The reference to including requirements in relation to security should be expanded to include

	integrity and destruction. Ensuring coverage of all three aspects may be particularly important if the audit activities of the Information Commissioner show areas of concern and subsequent notices could reflect these as additional requirements.
3.24	The terms of the retention notice given to CSPs are important in ensuring there is no doubt about a CSP's duties to cooperate with the Information Commissioner when undertaking an audit of the security, integrity and destruction of their retained data. This would include having access to relevant premises, people, systems, retained data and records. The current notice template should be amended addressing the detailed comments shown in relation to 'Annex A' set out below.
4.13	Variations to integrity and destruction requirements should also be included in the final bullet point. Concentrating on security stops short of the requirements at regulation 7 of the DRR.
6.	This section is headed 'Security of retained data' but addresses the elements required by regulation 7 of the DRR relating to security, integrity and destruction of data. The heading should be changed to 'Security, integrity and destruction of retained data' to ensure proper prominence is given to the other two essential requirements.
6.13	This paragraph refers to there being no 'inaccuracies' introduced as a requirement of regulation 7 (1) (a). The regulation makes no specific reference to inaccuracy and the contents of data could still be factually accurate even if incomplete. It may be a better reflection of this provision to make clear that it is ensuring that it is of the same integrity with no variations from the relevant business data that is the concern rather than just referring to inaccuracy.
6.19	This section helpfully refers to complying with instructions or recommendations by the Information Commissioner and mentions his 'published' guidance on security as an example. This is followed by a caveat saying that this and the further requirements made by the Home Office are unlikely to be publicly available. The last sentence should be amended to make clear that 'most' of these further requirements are unlikely to be available for the reasons listed to avoid any contradiction.
7.7	Reference is made to the possible publication of reports to demonstrate '…the oversight of the security of data…' Any such reports would also include oversight of the arrangements for integrity and destruction of data so this reference should be expanded to make this clearer.

9.3	The title of this section could make clear that this covers data integrity and destruction as well as security.
Annex A Schedule 2-B)	The comments on 3.24 above are relevant here. The notice given to the CSP has a crucial role in ensuring their cooperation with the Information Commissioner when undertaking his oversight role required in the DRR. His experience of undertaking audit activities of CSPs under existing more limited powers is that they require a full justification of the legal basis of these activities. It cannot be assumed that the goodwill of the CSPs will ensure that the Information Commissioner is given access to all he needs to discharge his duties. The requirements on the oversight of retained data at B) need strengthening to ensure there is no ambiguity leading to lengthy dialogues with CSPs over powers and the opportunity for less than full cooperation. The first bullet point of paragraph B) refers only to 'security'. This is in contrast to other references which refer to the three matters the Information Commissioner must oversee namely security, integrity and destruction. Paragraph A) directly above this section is an example. Any record keeping required by this bullet point must be capable of covering records relating to integrity and destruction too. The second bullet point under paragraph B) provides for such information being provided to the Information Commissioner on request. This can be read very narrowly as merely providing the Information Commissioner with a copy record of whether and how security requirements have been met. This on its own is unlikely to provide the necessary level of requirement on CSPs to enable the Information Commissioner to discharge his duties. This section should make clear that this include having access to relevant premises, people, systems, retained data and records.

8. The Acquisition and Disclosure of Communications Data Code of Practice (the acquisition code) engages the Information Commissioner's wider statutory remit. This includes his investigatory and enforcement functions which involve the acquisition and use of communications data under the Regulation of Investigatory Powers Act 2000.

9. The Commissioner has the following comments to make about specific provisions in the acquisition code where changes should be considered:

Acquisition code reference	Information Commissioner's comments
5.31-5.37	These sections deal with malicious and nuisance communications under 'the Privacy Regulations'. Although reference is made to Privacy and Electronic Communications (EC Directive) Regulations 2003 at 5.26 there is no reference to these being thereinafter being referred to as 'the Privacy Regulations'. Either 5.26 needs amending to make this clear or the full title should also be used in later provisions. Although footnote 96 refers to regulation 15 which deals with tracing such calls, this is not very clear and some readers may assume that this reference to 'nuisance calls' relates to unsolicited calls referred to at regulation 21. There is a very different mechanism for regulating those. Improving the clarity of the references may avoid any confusion.
6.21	This section reflects the duties placed on CSPs under Chapter II of Part I of RIPA to report communications data errors to IOCCO within five working days of the error being discovered. However, some communications data errors will also amount to personal data breaches under PECR. CSPs are required under regulation 5A of PECR to notify the Information Commissioner of a personal data breach without undue delay. In such cases, CSPs are therefore under two separate statutory obligations to notify both IOCCO and the Information Commissioner. The Information Commissioner is aware that there is some confusion amongst CSPs about the reporting requirements under RIPA / PECR with some believing that reporting communications data errors to IOCCO will be sufficient to meet their statutory obligations under regulation 5A of PECR. In order to avoid this confusion the acquisition code should make it clear that its requirements do not affect a CSP's statutory duty under regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 to notify the Information Commissioner of a personal data breach.
7.4	The Information Commissioner has produced a Subject Access Code of Practice to assist organisations adopt good practice when handling subject access requests. This section could make reference to this with a footnote to this guidance which is available at: https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf

7.5	Section 28 of the DPA does provide a substantial exemption from subject access where this is required for the purposes of safeguarding national security. Section 28(2) makes clear that a certificate from a Minister of the Crown is conclusive evidence of that fact, though this can be challenged through appeal to a Tribunal. The availability of such a certificate may be an important consideration when a person is considering whether to rely on this exemption and this aspect of the exemption should also be referenced.
7.10	This section could usefully refer to the fact that under section 42 of the DPA an individual may request the Information Commissioner to assess whether a subject access request has been handled in compliance with the DPA.
7.18	This section could usefully reference the guidance the Information Commissioner has produced on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle. A footnote could link to this guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/
7.20	Reference is made to the European Commission adequacy finding for Canada. This relates to transfers to organisations regulated by Canadian data protection legislation affecting the private sector. Whilst the Information Commissioner has no concerns about the level of protection that may be provided by Canadian public sector bodies this is not an appropriate example to use as it unlikely that communications data will be transferred to private sector bodies in Canada.
7.21	As mentioned in the comments on section 7.18 the Commissioner has published guidance to help organisations discharge their responsibilities. It would be helpful to point to this publication first rather than just referring readers to the Information Commissioner for guidance.

Information Commissioner

January 2015