R (LIBERTY) v SSHD & SSFCA

Note from the Secretaries of State on 'systems data' and 'identifying data'

1. Mr Justice Holgate asked during argument on Thursday 20 June about the different definitional approaches to 'systems data' and 'identifying data' in the Act (these being components of the definition of 'secondary data' in s137 in the bulk interception context[1]).

2. The starting point is that there are various items of information that can form part of any given communication, and the Act carefully winnows out the different constituent parts for the purposes of applying different sets of safeguards to them.

3. 'Content' is defined expansively in s261(6) – "**any** element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication…" (emphasis added), excluding any meaning to be inferred from the fact of the communication or its transmission, and subject to a deeming provision providing that anything that is systems data is not content: s261(6)(b).

4. 'Systems data' is then defined in s261(4) – broadly speaking, it is data that enables / facilitates the functioning of a system.

5. Very often systems data will consist of technical information that sheds no light on the meaning of a communication. However, there will be (limited) instances of overlap between information that constitutes 'systems data' and information that reveals something of the meaning of a communication. For example, the Secretaries of State agree with the Claimant that text entered into Google would constitute systems data, since it enables the functioning of the search engine, and yet it might also (depending on the text entered) reveal the meaning of a communication. That explains the need for the deeming provision in s.261(6)(b).

6. Parliament has also identified a further component of a communication, 'identifying data', which is data which may be used to identify, or assist in identifying, any person, apparatus (etc.): see s261(3).

7. Given that definition, identifying data will often – and certainly more often than systems data - also be content because it will reveal aspects of what might reasonably be considered to be the meaning of a communication.

8. It is no doubt for this reason (i.e. the extent of the overlap) that rather than having a provision deeming that identifying data cannot be content (as with systems data), the definition of secondary data in s137 specifically covers identifying data

[1] As well as being components of the equivalent definitions of 'equipment data' (s100) and 'protected data' (s203), which are the equivalents of secondary data in the bulk EI context and the BPD context respectively. For simplicity, this note refers to secondary data only.

only where it is logically separable and, if so separated, would not reveal anything of what might reasonably be considered to be the meaning

9. In this way, the most sensitive aspects of identifying data are carved out of the definition of secondary data, and will be subject to the same safeguards as content itself – including the BI safeguard.

10. For that reason, at least one of the examples in the Claimant's tables is misplaced. Entry 9 in the table concerns the voices of callers on telephone calls. The Secretaries of State agree that this constitutes identifying data as defined in s261(3), but it is hard to see how such information could be separated, or how this could be done without revealing the meaning of the communication. Thus such information would not count as secondary data under s137, and would be subject to the BI safeguard if an analyst wished to select them for examination.

11. Identifying data that can be logically separated (etc.), plus systems data, do fall within the definition of secondary data in s137 in the bulk interception context (and the equivalent definitions in relation to the other bulk powers), reflecting Parliament's decision that such data should be subject to a different set of safeguards from 'pure' content, which does not include the BI safeguard, but does include JC approval, operational purposes, IPC oversight, and so on.

12. It would not be helpful to deal with the Claimant's tables line by line, because: (i) the Defendants accept that secondary data is designedly broader than RCD, and includes material that can (in particular cases) be relatively sensitive, as shown in the examples from the Codes, albeit not as sensitive as the most sensitive content; and (ii) in respect of some of the examples, the question of whether the information in the examples would amount to 'identifying data' within the scope of 'secondary data' (i.e. whether it is logically separable and, if so separated, would not reveal anything of what might reasonably be considered to be the meaning of the communication) is likely to be fact-specific.