This was my response to a review of the Investigatory Powers Act by Lord Anderson of Ipswich in 2023. The first few paragraphs explain the Review's remit and how I proposed to respond. After its formal closing date the Annual Report of the Investigatory Powers Commissioner for 2021 (IPCO 2021) was published with some interesting comments and statistics and David Anderson encouraged me to provide an addendum.

My pre-occupations are the lack of clarity in some critical definitions within IPA and the consequences of maintaining the position that intercept evidence should be inadmissible. The two concerns are linked. Many of the problems in the definitions arise from attempts at extending the scope of "communications" data. I also address, in an Appendix, the issue of whether there is any longer justification for treating intercept evidence as distinct from all other kinds of evidence, analogue and digital.

In the end Anderson felt he had to confine himself to the Home Office-ordered terms of reference. https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2

RESPONSE TO INDEPENDENT REVIEW OF THE INVESTIGATORY POWERS ACT 2016

PETER SOMMER

MARCH 2023

Scope of the Act, Scope of the Review

1. The scope of the Investigatory Powers Act (the Act) is set out in s 1:

> (1) This Act sets out the extent to which certain investigatory powers may be used to interfere with privacy.
>
> (2) This Part imposes certain duties in relation to privacy and contains other protections for privacy.

2. Under s 260 the Home Secretary must produce a report on the Act's operation and did so on 9 February 2023[1]. The Terms of Reference for the Independent Review[2] are limited to consider the priority areas for change to the Investigatory Powers Act 2016 identified as part of the cross-HMG internal strategic review to inform a potential legislative reform package to be brought forward as soon as parliamentary time allows.

3. But the Home Secretary's review does not cover the privacy aspects of the Act apart from the oversight regime. The purpose of the Act was to give the authorities powers to protect the public from criminal and other hostile activity but also from untoward surveillance by the authorities, The Acknowledgements list does not include any lawyers, experts or NGOs with knowledge of the practicalities of the use in the criminal justice system of the provisions and powers in the Act. As a result the review is skewed to the operational needs of law enforcement and the intelligence community at the expense of considering the practicalities. These include the problems of implementing the Act's definitions and acquiring reliable supporting evidence as well as addressing privacy aspects. Reliable evidence is essential to secure criminal convictions. It can therefore be asked whether the Home Secretary has fully met her s 260 obligations.

4. It is to be hoped that the Independent Reviewer can take a broader view than the Terms of Reference suggest.

5. The opening remarks of the Home Office review are a little misleading:

> The Investigatory Powers Act 2016 (the Act) was introduced to replace emergency legislation passed in July 2014 (the Data Retention and Investigatory Powers Act 2014 (DRIPA)) in response to the European Court of Justice striking down the Data Retention Directive of 2006. DRIPA was subject to a sunset clause providing for the legislation to be repealed on 31 December 2016. During the passage of DRIPA, the government committed to bringing forward new legislation which would provide the security and intelligence agencies, law enforcement and other public authorities with the investigatory powers necessary to address evolving threats within a changing communications environment.

6. The Act had older antecedents. During 2008 reports began to appear of an ‘Interception Modernisation Programme’ or IMP. According to the Home Office, the IMP was a 'cross-Government programme established to maintain our capability to obtain communications data and to support lawful interception, currently threatened by the advance of internet technologies and their increasing usage'. On 27 April 2009 the British Government released a consultation

[1] https://www.gov.uk/government/publications/report-on-the-operation-of-the-investigatory-powers-act-2016

[2] https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016/terms-of-reference-for-the-independent-review-of-the-investigatory-powers-act-2016

document outlining its plans for *Protecting the Public in a Changing Communications Environment*[3]. In her introduction to the document, the then Home Secretary, Jacqui Smith said: "I also know that the balance between privacy and security is a delicate one…. My intention is to find a model which […] strikes the right balance between maximising public protection and minimising intrusion into individuals' private lives."

7. It was only Part 4 of the Act, Retention of Communications Data, that was a direct and necessary response to the sunset clause in DRIPA and the requirement to have new legislation in place by December 2016. Parliament chose not to give itself more time to examine the complexities of the other aspects of the legislation. While the debates in the various Select Committees and on the floors of the Commons and Lords were able to look at many general principles including the introduction of new arrangements for oversight and safeguards for MPs and journalists, little time was spent looking at the detail of the practicalities. That involved linking legislative wording to the specifics of Internet and network technologies, essential if useful evidence was to be captured.

Scope of my response

8. I am limiting myself to the impact of the Act to the criminal justice system and will not be addressing those parts that relate to the activities of the intelligence community UKIC. My own relevant experience and knowledge is as an independent expert witness instructed on occasions by both prosecution and defence in criminal matters. During the passage of the Investigatory Powers legislation through Parliament in 2015-2016 I was one of two external special advisors to the Joint Select Committee that reviewed the draft law. A short CV appears as Appendix I.

Impact of the Inadmissibility of Intercept Evidence

9. At several points in the Act we can see the consequences of the attempts to maintain the inadmissibility of intercept in the face of changing information and communications technologies. Definitions in the legislation struggle when faced with the practicalities of locating and acquiring evidence to support specific sections and schedules – and showing that that evidence can be safely relied on to forensic science standards.

[3] http://www.homeoffice.gov.uk/documents/cons-2009-communications-data?view=Binary

10. The problem occurs around the concept of an Internet Connection Record where there are practical difficulties in separating "communications data" from "content".

11. The problem also occurs in the detailed definitions distinguishing data caught in the course of transmission and data captured from storage, particularly where concepts of ephemeral and temporary storage are introduced. There are also overlaps between "equipment interference" and digital forensics practice.

12. If we are to abandon the special status of the inadmissibility of intercept some thought must be given to what might replace it.

13. Thought must also be given to the routes available to law enforcement to overcome their disclosure obligations under CPIA 1996 when dealing with sensitive methods. A review of how Public Interest Immunity operates and the conditions under which it is granted may be needed.

14. Operation Venetic, the UK response to a Dutch-French breach of the secure EncroChat smart phone system, provides a number of illustrations of some of the problems discussed here. Appendix II contains a brief description.

15. Appendix III comments on the arguments usually advanced in support of the continuance of the inadmissibility of intercept and shows how many of these have become obsolete and redundant in the light of digital evidence practice.

Internet Connection Records

16. The aim behind the concept of Internet Connection Record was to extend the definitions of "communications data".

17. In the Act there are two classes of communications data:

    - Entity Data - s 261(3) of the Act
    - Events Data – s 261(4) of the Act

18. Entity data is further explained in the Code of Practice[4] at paragraphs 2.23 ff – a person, device and the technical means by which they are able to communicate. One element is subscriber records – who owns what phone number, what ISP contract etc

19. Events data is described in paragraph 2.34 and 2.44-2.45 of the Code of Practice:

---

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

> events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

It can include call data records as supplied by telecommunications companies[5]

20. The definition if Internet Connection Record appears in s 62(7) of the Act and such records are regarded as events data:

> S 62 (7) In this Act "internet connection record" means communications data which—
>
> > (a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and
> >
> > (b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

21. During the passage of the Bill the Home Office produced a Factsheet[6] which said that ICRs are retained by communications service providers for one of three purposes: to identify the sender of a communication, to identify the communications services a person is using and to determine whether a person has been accessing or making illegal material online. It goes on to say: ICRs do not provide a full internet browsing history. The ICRs do not reveal every web page that a person visited or any action carried out on that web page." ICRs do not provide a full internet browsing history. The ICRs do not reveal every web page that a person visited or any action carried out on that web page."

> "What are ICRs?
>
> > • Internet connection records are records captured by the network access provider (e.g. the Internet Service Provider or Wi-Fi operator) of the internet services with which a uniquely identifiable device (e.g. a laptop or mobile phone) interacts.
> >
> > • It will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date.
> >
> > • **It could never contain a full web address as under the law these would be defined as content.** (emphasis added)

[5] I will not be covering any of the issues around definitions of "telecommunications companies"

[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf 30/10/2015

> • You may be able to see that a person has used, google.co.uk or facebook.com but you would not be able to see what searches have been made on google or whose profiles had been viewed on Facebook."

22. Further information is given in the Communications Data Code of Practice[7] at paragraphs 2.74-2.80. The general vagueness of the concept can be seen:

> 2.76 **There is no single set of data that constitutes an ICR, as it will depend on the service and service provider concerned**. (emphasis added) The core information that is likely to be included is: • a customer account reference – this may be an account number or an identifier of the customer's device or internet connection; • the source IP address and port; • the destination IP address and port – this is the address to which the person is routed on the internet and could be considered as equivalent to a dialled See paragraphs 2.80-2.83 for more information on third party data. telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc.) although ports are often reused for different purposes; and • the date/time of the start and end of the event or its duration.
>
> 2.77 In addition an ICR may also include, for example: • the volume of data transferred in either, or both, directions; • the name of the internet service or attributable server that has been connected to; and • those elements of a URL which constitute communications data – see paragraphs 2.59 to 2.66..

23. Chapter 9 of the Code of Practice – paragraphs 9.1-9.15 - covers the considerations before a warrant can be issued.

24. The definitions in "entity data" reflect data that would be created and collected by a telecommunications company in the ordinary course of its business – for the purposes of tariffing, engineering and maintaining quality of service. The same is true of most common forms of "event data" such as call data records[8]. But with Internet Connection Records, with its more *ad hoc* quality, telecommunications companies would have to craft acquisition tools for each occasion. This in turn places a particular burden on the Office of Communications Data Authorisations who will need specialist technical skills in order to see that each warrant does not exceed the "necessary and proportionate" test and that content is not inadvertently being captured.

25. A particular problem is highlighted in the Code of Practice – how to deal with web browsing – paragraphs 2.60-2.73. A full web address – Fully Qualified Domain

---

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

[8] These include date/time number called, number received, duration of call, and for mobile phones – identifiers for start and end cell masts. Full call data records may also carry further information

Name – FQDN – may easily point to the content of a web-page, which is excluded from "communications data". The FQDN may contain sufficient information about the web page simply from its naming convention but even if does not, simply clicking on it will cause the page to appear (if it is live or from the Wayback Machine at https://archive.org/web/. Although the Code of Practice describes the problem it does not appear to offer any solution, other than individual specific manual intervention. It observes:

> 2.67 An authorisation under Part 3 of the Act or retention notice under Part 4 of the Act may only authorise the acquisition or retention of communications data, and therefore can only cover those elements of a URL which constitute communications data.
>
> and
>
> 2.72 Section 87(4) of the Act ensures that a retention notice must not require the retention of third party data. Where the telecommunications operator needs the data for the functioning of a telecommunication system or where the data is retained or used for any other purpose, it is not third party data. For example, where data that would otherwise be third party data is processed and recalculated it is no longer third party data. Equally, where it is not reasonably practicable to separate the third party data from other data that is subject to the retention notice then that third party data can be retained. Determining what is third party data and whether it can be separated from other data is complex and will require careful consideration on a case by case basis as part of the consultation before a retention notice is given.14
>
> 2.73 A retention notice can never require a telecommunications operator or postal operator to retain the content of a communication.

26. The Internet Connection Record is a concept developed to meet declared law enforcement investigatory needs but which turns out to be extremely difficult to implement in practice. It will be interesting to see the results of the current experiments and trials.

Interception as defined in IPA 2016

27. Concepts of "interception" have had to become more complex as technology developed. In 2020 3648 targeted interception warrants were authorised and 158 targeted examination warrants

28. In the 2016 Act:

> **56 Exclusion of matters from legal proceedings etc.**

(1) No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)—

(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—

(i) any content of an intercepted communication, or

(ii) any secondary data obtained from a communication, or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

29. The underlying notion has not changed much since its first appearance in 1985:

9 Exclusion of evidence

(1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest—

(a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below ; or

(b) that a warrant has been or is to be issued to any of those persons.

30. Or in the 2000 Act:

17 Exclusion of matters from legal proceedings

(1)Subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner)—

(a)discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or

(b)tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.

31. Back in 1985 "content" consisted either of analogue voice calls or telex traffic. There was a clear technical distinction between those and communications data which consisted of date/time, number called and duration of call. The content was

obtained by placing a speaker/recorder [9]over the line, the communications data was captured by the telephone company for tariffing purposes.

32. By the time of the Regulation of Investigatory Powers Act (RIPA|) in 2000 there were the challenges of regular email, web browsing and webmail.

33. Regular email is the version where the user has on his/her own device a specialist program which enables emails to be originated, received and stored. In this situation it is relatively easy to separate communications data from content because of the way in which the underlying protocol works. This is the IETF's RFC 5321 and among other things it lists out various activities which are recorded and available for view (usually via a "view source" or similar command): the "from", "to", "subject", and "content" are all separate. "subject" and "content" are content of course. (There are many other items in the protocol which refer to, among others, the journey the email made, spam detection etc)

34. In web-based email the email sending, receiving and storage is via a website. The practical problem of separating communications data from comment is similar to that referred to in paragraph 25 above – the Fully Qualified Domain Name in this instance will be a "landing page" in which you can see who is sending and receiving emails but where the "subject" will be also clearly visible. They can only be separated by means of complex manual intervention. Each web-mail service will require slightly different measures. Every so often service providers change the appearance of their pages – and further manual intervention may then be required in response. The same problem exists with social media. General public postings will usually be admissible because the poster has given consent for them to be viewed. But where you have postings that are private to a group or a direct message (just to one person), the "communications data/content" problem arises.

35. In the RIPA 2000 regime the working assumption seems to have been that FQDN could not be used – all that was admissible was the name of the website up to the first backslash – Facebook.com/, Hotmail.com/. This denied investigators from capturing information about which participants were communicating with other participants.

36. In IPA 2016, as we have seen, the proposed solution was the Internet Connection Record, as with the practical problems of implementation already discussed.

37. But IPA 2016 also introduced further definitions presumably designed to assist investigators but which ran into clashes with notions of storage under Equipment Interference.

[9] Or an auxiliary telex machine for telex traffic

Equipment Interference and Interception

38. Equipment Interference (EI) appears in Part 5 of IPA. It enables, among other things, the capture from a remote computer of stored data and stored communications (ss 99-101). It was a substantial clarification and extension of powers which had existed before including the Police Act 1997 – Part III "authorisations to interfere with property etc". and Computer Misuse Act 1990 s 10 – ""Saving for certain law enforcement powers" which gave the police a means of otherwise unauthorised access to a computer powers of "inspection, search or seizure"

39. Unlike Interception, the product of such activity is fully admissible. In 2020 2951 TEI warrants were authorised, divided into 1915 for UKICs and 1036 for LEAs.

40. A particular feature of EI is lack of regular robust methods of execution to produce forensically reliable (and testable) evidence. Investigators have to operate covertly so as not to alert targets. Unlike the position with acquiring evidence from computers, mobile phones and storage devices, they have to operate remotely and without necessarily having full knowledge of the technical environment within which they are operating. Moreover they are having to capture data live while the system is still running[10]. As far as I know, despite the number of TEI warrants issued, the only circumstances in which product has been offered as evidence is in the Operation Venetic cases[11].

41. It was for this reason plus the likely need to keep EI precise methods secret so that they could be reused in future that at the time IPA was being discussed the assumption was that applications for public interest immunity would be frequent.

42. There are a variety of **ambiguities** in the detailed provisions, including the **overlap with interception:**

    S 99 says:

    > (2) A targeted equipment interference warrant is a warrant which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining—
    >
    > (a)communications (see section 135);
    >
    > (b)equipment data (see section 100);
    >
    > (c)any other information.
    >
    > (3) A targeted equipment interference warrant—

[10] https://doi.org/10.1016/j.fsidi.2022.301333

[11] See Appendix II

> (a)must also authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates;
>
> (b)may also authorise that person to secure the disclosure, in any manner described in the warrant, of anything obtained under the warrant by virtue of paragraph (a).

(4) The reference in subsections (2) and (3) to the obtaining of communications or other information includes doing so by—

> (a)monitoring, observing or listening to a person's communications or other activities;
>
> (b)recording anything which is monitored, observed or listened to.

But

> (6) A targeted equipment interference warrant may not, by virtue of subsection (3), authorise or require a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 3(1) (unlawful interception)

The Code of Practice has an interesting example:

> Example 2: An equipment interference authority wishes to conduct equipment interference to acquire private information from a computer and intercept an online video call in the course of its transmission. This activity constitutes both equipment interference and interception. The interception cannot be authorised as incidental conduct so a combined interception and equipment interference warrant, or separate authorisations must be obtained. A combined warrant may be issued by the Secretary of State and approved by a Judicial Commissioner.

43. But what then happens to the result of the activity – is it admissible as equipment interference or inadmissible as evidence – and how can one tell?

The Code of Practice recognises the problem but does not have an explicit solution:

> 5.113 The exclusion of matters from legal proceedings (section 56) continues to apply to an interception warrant that is part of a combined warrant. However, when an equipment interference warrant is combined with an interception warrant the material derived from equipment interference may still in principle be used in legal proceedings if required. If material derived from equipment interference authorised by a combined warrant reveals the existence of an interception warrant the material is excluded from use in legal proceedings according to section 56 of the Act.
>
> 5.114 Should the exclusion from legal proceedings mean that there may be difficulties in disclosing any material obtained under a combined warrant that

included an interception warrant, equipment interference authorities may wish to consider the possibility of seeking individual warrants instead.

44. But s 56 seems to prevent any querying in open court how this might be achieved.

45. There are further some puzzles within IPA, for example: **when does "transmission" start and end?** We need to consider two situations:

- Store and Forward Systems
- Encryption systems

46. Store and Forward Systems Many widely used messaging systems use "store and forward". This is to overcome the problem when an intended recipient is not immediately online, perhaps when a device is powered off or temporarily not connected to a network. It is overcome by providing an intermediate resource which holds a message until the intended recipient is back online. In conventional email the resource is called a Mail Transport Agent (MTA) – all ISPs offering email have one. There are usually facilities for emails to be deleted after a set time. With web-based email and social media the data is retained on storage systems linked to web sites. What js the status of this stored data,and what legal means are available to acquire the data and present it in court? Or withhold from evidence?

47. One possibility points to the definition s 4 (b) " any time when the communication is stored in or by the system (whether before or after its transmission)." In addition ss 56 (a) (ii) and (b) which cover, respectively, secondary data and interception-related conduct. On that basis the temporarily stored data can't be referred to in legal proceedings.

48. But if the MTA is seized or subject to a production order and data is extracted from it then the data would appear to be from storage and thus admissible

49. The same would apply if the data was acquired remotely from the MTA via an equipment interference warrant.

50. S 56, though, would appear to impose a ban on any "question asked, assertion on disclosure made…."

51. Encryption systems. In true end-to-end encryption encrypting and decrypting only occurs at the end points, typically these days on a smartphone. If the sent and received messages are stored for later retrieval on the device then they are admissible if the device is seized (and not strongly password-protected) or if captured remotely via equipment interference.

52. But suppose there is no storage for later retrieval – that in the encrypting stage the message is very briefly in the clear before being decrypted on the handset and then sent onwards in encrypted form? In the decrypting stage an encrypted message is

received, decrypted on the handset, and briefly shown in decrypted form to the handset owner but not stored. Is all this traffic inadmissible? Are the circumstances different if you have a technical means of capturing the ephemeral decrypted data? Is the data still in the course of transmission, or is it" stored", if only for a few microseconds? There are twin problems – interpreting the legislation and establishing forensically if and how ephemeral data is being captured.

53. **IPCO Comment on warranting problems** It is instructive to look at the comments in the *IPCO Report 2020*[12]:

> 14.50 TEI applications have the potential to be complex, describing technically complicated and potentially novel actions. This poses a challenge to the authorities applying for warrants because they are required accurately, yet succinctly, to describe the planned operation, as well as providing an appropriate assessment as to the extent of risk for any collateral intrusion.
>
> 14.51 It is also challenging at times to define the boundaries between TEI, targeted interception (TI) of live-time communications and the field of digital forensics. This can arise, for example, where LEAs seek to retrieve evidence from cloud-based storage, following an arrest and the seizure of a telephone or computer during reactive investigations. Because of a lack of clarity and guidance on how existing statutory powers can be exercised to obtain this material, we have seen an increase in applications for TEI to conduct forensic examinations of communication devices to retrieve data held remotely on the internet, such as email or social media accounts….

54. To this can be added the problems of producing testable evidence to forensic standards.

Possible New Warranting Structures

55. If a decision is made to abandon s 56 of the Act then thought must be given to what might replace it.

56. Plainly there seems to be every reason to maintain the existing warranting arrangements for entity and simple event data – ss 261(3) and (4) – in so far as they correspond to data already routinely collected by telecommunications companies for existing business purposes.

[12] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

57. But for "content" one obvious place to look for examples is in the arrangements for covert surveillance in the Covert Surveillance and Property Interference Code of Practice [13]

> 3.1 Surveillance is **directed surveillance** if the following are all true:
>
> • it is covert, but not intrusive surveillance ;
>
> • it is conducted for the purposes of a specific investigation or operation;
>
> • it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
>
> • it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought
>
> 3.19 **Intrusive surveillance** is covert surveillance that is:
>
> • carried out in relation to anything taking place on residential premises, or
>
> • in any private vehicle, and
>
> • involves the presence of an individual on the premises or in the vehicle, or
>
> • is carried out by a means of a surveillance device.
>
> 3.21 The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained, as it is assumed that intrusive surveillance will always be likely to result in the obtaining of private information. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of private information.

58. As can be seen the criterion is not based on a direct assessment of breach of privacy and not on one form of technology as opposed to others. That would suggest that for the current purpose the criterion for enhanced surveillance of telephone and internet traffic should be whether the material amounts to "content". As for the distinctions between directed and intrusive surveillance higher standards for requirements for a "content" warrant.

59. We could end up with a tri-level warranting scheme:

---

13 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

- Entity data
- Events data
- Content

60. Since content would be admissible the question for applicants and granters of appropriate warrants would be relatively simple: if in doubt a warrant would need to be sought at the higher level.

61. The Code of Practice contains some useful guidance about the assessment of online covert activity (sections 3.10-3.17). There are also some considerations of how far "covert surveillance" overlaps with "content" (3.10—3.11)[14]

Review of PII considerations,

62. S 56 of the Act and indeed all its predecessors contains a *quid pro quo.* Intercept can't be referred to but neither can it be used in evidence, only for intelligence in order to acquire evidence that is admissible. It is not clear that the same doctrine always holds good for arrangements under public interest immunity.

63. Under the right to a fair trial. disclosure is determined by a statutory test whereby any material that might reasonably be considered capable of undermining the prosecution case or assisting the case for the defence should be disclosed. S 3 CPIA 1996. The right to disclosure of this material is limited by the doctrine of public interest immunity (PII), which allows the court to withhold relevant information from the defence where it decides it is in the public interest to do so. The court must apply a balancing exercise to determine the interests of the defendant in receiving all the information relevant to their defence with the interest of the state in protecting sensitive information.

64. It seems very likely that there will be persuasive arguments for the concealment of the precise methodology of data acquisition both via equipment interference and, if it is allowed, via intercept. Concealment of methodology is far less necessary where data is obtained from storage "at rest"; indeed it is a fundamental of digital forensics that methods of acquisition, preservation and subsequent analysis are entirely open and carried out using validated methods and accompanied by an audit trail of investigative activities[15].

[14] In the version of the Code I have the reference is to RIPA; in an updated version presumably this would be to IPA

[15] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912389/107_FSR-C-107_Digital_forensics_2.0.pdf

65. The grounds for methodology concealment will be that knowledge could be used in the future to circumvent or frustrate later investigations. The problems will be at their height in relation to Equipment Interference. The *IPCO 2020 Report* says that in the related year 1036 TEI warrants were issued for Law Enforcement Agencies. As far as I know none of these resulted in TEI evidence being presented in open court it seems a reasonable assumption that their existence was the subject of PII applications.

66. Little judicial guidance as to how to manage the situation. Part 15of the Criminal Procedure Rules describes how an application is made and the possibilities of appeal[16].There is also guidance for prosecutors in the CPS Disclosure Manual at chapter 13[17].

67. The main case is R v H, R v C [2004} UKHL 3 which sets out a series of s questions. Having established that the concealment of disclosure meets a test of real risk of serious prejudice to an important public interest and that there is the minimum derogation necessary the judge has to ask whether any limited disclosure may render the trial process, viewed as a whole, unfair to the defendant:

> 37 Throughout his or her consideration of any disclosure issue the trial judge must bear constantly in mind the overriding principles referred to in this opinion. In applying them, the judge should involve the defence to the maximum extent possible without disclosing that which the general interest requires to be protected but taking full account of the specific defence which is relied on. There will be very few cases indeed in which some measure of disclosure to the defence will not be possible, even if this is confined to the fact that an ex parte application is to be made. If even that information is withheld and if the material to be withheld is of significant help to the defendant, there must be a very serious question whether the prosecution should proceed, since special counsel, even if appointed, cannot then receive any instructions from the defence at all.

68. The trouble is that this guidance does not seem to be very helpful when what is desired is to withhold details of a technical means of evidence acquisition. One route might be a replication of the *quid pro quo* in the current arrangements in s 56 IPA. If the defence is not allowed to know the precise means by which a stream of evidence was obtained then there seems a very good case for insisting that any such evidence should be wholly excluded, The police would still be able to use the information obtained as intelligence but any charges would need to be based on evidence which could be fully tested.

[16] https://www.legislation.gov.uk/uksi/2020/759/part/15/made, especially rules 15.3 and 15.6

[17] https://www.cps.gov.uk/legal-guidance/disclosure-manual-chapter-13-making-pii-application

Appendix I: CV

Peter Sommer combines academic and public policy work with commercial cyber security consultancy, with a strong bias towards legal issues. He has acted as an expert in many important criminal and civil court proceedings in the UK and international courts usually where digital evidence has been an issue including Official Secrets, terrorism, state corruption, global hacking, murder, narcotics trafficking, corporate fraud, privacy, defamation, breach of contract, professional regulatory proceedings, harassment, allegations against the UK military in Iraq and child sexual abuse. He gave evidence to the Investigatory Powers Tribunal in PI & others v GCHQ, Particular themes of his instructions have been situations where technologies need to be interpreted in legal terms and assessments of quantum and extent of damage. He is on the list of experts maintained by the NCA to assist law enforcement in major investigations.

His first degree is in law, from Oxford University. Until 2020 he was professor of digital evidence at Birmingham City University where he is now a visiting professor. Until 2011 he was a visiting professor in the Department of Management at the London School of Economics. He is also currently a visiting professor at De Montfort University and lectures and examines at other universities. He has consulted for OECD, UN, European Commission, UK Cabinet Office Scientific Advisory Panel on Emergency Response (the predecessor of SAGE), UK National Audit Office, Audit Commission, and the Home Office. The OECD work, written with Ian Brown, addressed the cyber aspects of Future Global Threats He has given evidence to the Home Affairs and Science & Technology Select Committees, the Joint Committee on the Communications Data Bill and to the Intelligence and Security Committee. He was a Parliamentary Specialist Advisor on Secure E-Commerce legislation to the old Trade & Industry Select Committee and also a Parliamentary Specialist Advisor to the Joint Select Committee on the Draft Investigatory Powers Bill.

He is the author, pseudonymously, of The Hacker's Handbook, DataTheft and The Industrial Espionage Handbook, and under his own name, Digital Evidence, Digital Investigations and E-Disclosure (IAAC) now in its 4th edition

During its existence he was the joint lead assessor for the digital speciality at the Home Office-sponsored Council for the Registration of Forensic Practitioners and has advised the UK Forensic Science Regulator and the Home Office on communications data.

He is a Fellow of the British Computer Society and also a Fellow of the Royal Society of Arts.

Appendix II: Operation Venetic

1. NCA Operation Venetic is the UK response to the extensive breach of a highly encrypted smart phone service called EncroChat. It had been very popular with

top level serious organised criminals. At the height of its popularity across Europe there may have been over 60,000 users, 10,000 of them in the UK. EncroPhones started appearing in 2016. The service was closed down in June 2020. Trials based on evidence collected during Operation Venetic are ongoing.

2. Some of the issues arising in the related series of trials and in proceedings before the Investigatory Powers Tribunal provide useful illustrations of some of the problems with IPA 2016.

3. EncroPhones, heavily modified Android smartphones, were found to be highly resistant to the usual acquisition and recovery techniques deployed by law enforcement. When such phones were, prior to Operation Venetic, located and seized technical evidence was limited to describing their known functions but data stored on them could not be accessed unless law enforcement had been able to obtain relevant passwords.

4. The Encro service featured:

    - Secure text messaging
    - Transmission of photographs
    - Automatic deleting of traffic after a specified time, typically 7 days.
    - Voice calls
    - Secure Notes

5. Actual facilities changed over the life of the service; one feature was the ability to update programs and facilities remotely.

6. The Encro handsets communicated with each other via one or more mediating computer servers. The main server was based in Lille, France.

7. All communications between the handsets were encrypted. The handsets could not make regular phone calls or make use of regular Internet facilities. Encro was a "closed" system. The encryption deployed was claimed to be end-to-end. If properly implemented this means that encryption and decryption only takes place on the Encro handsets and not on any other device, server or link that might form the chain of connection.

8. The breakthrough came as a result of a Dutch-French Joint Investigation Team (JIT). They appear to have acquired some EncroChat handsets and subscriptions. Having obtained the appropriate warrants from the French courts they created a copy of the Encro server in order to understand its facilities. They designed what they describe as a "tool" and the UK authorities as an "implant" which was sent to each connected EncroChat handset via the "update" facility. The aim was to weaken the Encro security facilities such that the French authorities were able to exfiltrate and capture EncroChat traffic. The implant was activated and the acquired data was sent to facilities owned by French law enforcement – the French took the operational lead. Once there it could be processed and passed on to local

investigators but also, under agreement, via Europol to international law enforcement partners such as the UK's NCA.

9. The French Operation was called Emma, the Dutch Lemont [18]and the subsequent exploitation within the UK is called Operation Venetic.

10. The messages and images collected by Operation Emma fell into two categories. The first category consists of messages that were already held on the phone. Because of the automatic delete facility these usually were only for the 7 previous days. This is known as Phase 1 or Type 1 messages. The second category was messages and images collected "live" as they were being created or received by the smartphone. These are Phase 2 or Type 2 messages and images.

11. The French authorities have refused to provide the National Crime Agency and anyone else in the United Kingdom with the detail of how their tool worked and the processing they carried out prior to deliver material to the National Crime Agency. They claimed national security defence secrecy. Nevertheless the NCA felt able to accept what was delivered to them.

12. The NCA and UK prosecuting authorities needed to be able to show that the messages and other traffic such as photos had been captured from storage. Many of the messages reveal, explicitly, trafficking in narcotics and some also refer to firearms. If they had been caught in the course of transmission they would be regarded as intercept and be excluded by virtue of s 56 IPA. In the early part of 2020 before Operation Emma was initiated but also afterwards there were extensive discussions between NCA and the French authorities and also between NCA and CPS to attempt to arrive at a conclusion.

13. The only information we have about French activities comes from the hearsay evidence of a French investigator. In a judgement delivered on 4 January 2021 in a case referred to as R. v A, B, D, C,, the presiding judge decided that the hearsay evidence could be admitted on the basis of s 116 CJA 2003. The Court of Appeal upheld this position - R. v A, B, D, C, [2021) EWCA Crim 128 – 5 February 2021.

14. In the original hearing the judge was also asked to rule whether the tendered messages had been acquired from storage or via intercept,. The position on the Phase 1 messages was quite clear as they had plainly been stored on the handset. Matters were far less clear for those Phase 2 messages that appear to have been captured either at the point of origination or point of reception but had not been sent to permanent storage[19]. There was a defence expert report but none from the prosecution. Based on the information before him the judge determined that the

[18] For convenience I will refer to the activities as Operation Emma as in this instance French law enforcement investigators appear to have taken the lead

[19] EncroChat phones had an automatic facility which deleted messages after (by default) 7 days. The stored messages were held in an identifiable database called *realm.*

Phase 2 messages were also acquired from storage. His reasoning was that since end-to-end encryption was being used, the only point at which unencrypted traffic could exist was in some form of storage, however ephemeral, on the handset.

15. There is plausible contrary view, that one of the effects of the French tool/implant was to weaken the end-to-end encryption such that knowledge of the encrypting keys was available at the mediating server, which was under the control of the French authorities. If this view is correct then the Phase 2 traffic was collected in the course of transmission – and would be inadmissible.

16. We cannot exhaustively arbitrate between these two views because the French method remains opaque and, so far at least, it has not been possible to reverse engineer the tool/implant and the related activities on computer resources controlled by the French.

17. The point for the purpose of this Appendix is not to attempt to resolve the storage/intercept in the Venetic cases but to identify the extreme challenges of doing so.

18. It should also be said that there are a number of other legal issues around the Venetic investigations including the circumstances of warranting but these are not of direct relevance to a consideration of the workings of the Investigatory Powers Act. There are also questions about the reliability and completeness of the material apparently captured by the tool/implant and, assuming it is admissible, being tendered as evidence.

Appendix III: Arguments about Retaining Inadmissibility of Intercept

1. **The arguments against allowing interception evidence to be admitted.** The arguments against allowing interception evidence to be admitted are said to be[20]:

    - that knowledge of the technical means used would assist wrong-doers and make the task of law enforcement and intelligence more difficult

    - that employees of law enforcement would be placed at significant risk

[20] Based ton the Report of the Interceptions Commissioner for 2005-2006, paragraph 46. http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf , the Report of the Chilcot Committee, http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf and a 1999 Home Office document produced prior to RIPA and which is no longer on the Home Office website.

- that the process of disclosure would force law enforcement agencies to reveal more than was safe about their methods
- that the expense to the intercepting agency of storing the material would be considerable
- that compliance with disclosure requirements would involve the transcribing of large quantities of conversational material which in turn would be very costly
- that it would be difficult to prove who was talking to whom
- that innocent third parties who had had contact with an accused might find their privacy compromised

Nearly all of these are based on mis-conceptions either of technology or of the application of the criminal justice system.

2. **Knowledge of the existence and reach of interception** The existence of interception facilities in the UK is not a secret; the power to carry out interceptions is enshrined in statute and each year the IPCO states the number of warrants in force.[21] For 2020, the latest year for which statistics are available there were 3648 TI authorisations covering UKIC, MoD and law enforcement. [22]

3. **The Technology of Telephone Interception** There is nothing complicated or secret in the principles of how interception of landline and cellular phones take place or how to capture Internet-related (IP – Internet Protocol) traffic. For conventional, voice-based telephony two elements are required: the voice component (by placing simple circuitry across the line or by capturing digitally) and the "traffic" component - who called whom, when and for how long – which is part of the regular record of the telecommunications company for revenue collection and quality of service purposes and already admissible.

   Under s 253 of the Act the Secretary of State can issue a Technical Capability Notice to "relevant operators" to provide facilities to support any authorisation, which includes the collection of intercept material.

   There are two linked elements to the technology: the handover interface between the telecommunications or communications company; and the means to record what is handed over.

   Information about the handover interfaces for the various types of telecommunications services is published on the website of the the European

[21] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

[22] In the same year there were 239,086 authorisations for access to communications data granted to law enforcement agencies

Telecommunications Standards Institute (ETSI) – http://portal.etsi.org/li/Summary.asp. The actual standards are also published at http://www.gliif.org/, the Global Lawful Intercept Forum. The US equivalents, designed to work under CALEA, Communications Assistance for Law Enforcement Act, are published by the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS). The ATIS website sells the current specification documents: https://www.atis.org/docstore/. Details of the application to cable-based systems can be found at http://www.cablelabs.com/specifications/archives/PKT-SP-ESP-I03-040113.pdf

The main features are conversion between technical protocols and the ability to guarantee and preserve the reliability of the intercepted material. The voice and the traffic components (referred to in the literature as the IRI, Intercept-Related Information) are designed to be crytographically inextricably linked as a control against tampering and editing – the voice file and information about the call including the various terminating phone numbers, time and duration of call, are all held together as a single item when handed over to the Lawful Intercept authority, whoever that is.

Significant detail is published by vendors of law intercept equipment such as ss8 – www.ss8.com., Squire Technologies https://www.squire-technologies.co.uk/solutions/solutions-for-lawful-interception, and Utimaco, https://utimaco.com/products/categories/lawful-interception

Most of the data captured today is already in digital form - content of emails, web-browsing, social media - so that there are no **transcription costs**. The computer-aided transcription of analogue voice traffic is now of a high order of accuracy. Nuance's Dragon Naturally Speaking does this locally on a PC and the same is true on Apple Silicon where the facility is a basic part of MacOS. I can hold my Android phone up to the loudspeaker of a tv during a news bulletin and can see the text conversion, though in that instance the conversion will have been done remotely on facilities owned by Google.

Once data is collected digitally, the cost of storage and back-up is minimal. The problem of volume of storage is not particular to intercepted data but is routinely dealt with following seizure of devices with storage – PCs, laptops, tablets, smartphones, USB sticks, external hard-disks, data held in the cloud. A desktop 5 GB hard drive, sufficient for most criminal cases, costs around £100. Mass storage systems would be cheaper. The problem of data storage is not limited to criminal matters – businesses would be expected to retain data for at least 7 years.

4. **Disclosure Obligations and Costs Regime** The applicable law is Criminal Procedures and Investigations Act, 1996 (as amended, particularly by the Criminal Justice Act 2003[23]). Practical detail appears conveniently in the

[23] Part 5

CPS *Disclosure Manual.* The practicalities of disclosure for intercept material would be very similar to those for stored data and communications data – reasonable lines of enquiry[24]. The prosecutor would apply the basic tests of the obligation to disclose to the accused any prosecution material which had not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused. '(s 3 CPIA) and the guidance in the Attorney-General's Guidelines[25]. Detail on digital material appears in Appendix A including general principles of handling[26] sifting and examination of large data volumes, the production of a Disclosure Management Document and involvement with defence interests.

There appears to be nothing unique in this respect in intercepted data as opposed to data captured from storage. Similar arguments may arise when the defence say that the selection of tendered material is subject to investigator cognitive bias and over proof of provenance.

Disclosure costs would be low – delivery of stored data is now via hard disk or USB drive. Agreement could be sought on a counsel-to-counsel basis which elements would be printed out for a jury bundle.

Defence lawyers and experts are already adept at using search tools to review disclosed material. At a practical level it may be useful for one or more pre-trial expert-to-expert meetings and joint reports under CrimPR 19.6.

5. **Sensitivity of Interception Methods** The above descriptions apply to the vast majority of intercepts, which are carried out with the full co-operation of the communications service providers. Different considerations may apply where the co-operation is not available and where technicians may, for example, eavesdrop on radio, satellite and microwave transmissions or break into a cable. Passive collection is also possible[27]. But this must refer to a tiny minority of instances and those are presumably concentrated on overseas activities and for intelligence purposes. For these situations the route would be presumably be via Public Interest Immunity.

   In practice there are much more likely to be sensitivities over methods of equipment interference.

6. **Impact on Interception Staff** If one thinks about what is involved in accepting a lawful intercept from a co-operating communications service

[24] https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/Disclosure-reasonable-lines-of-enquiry-and-communications-evidence.pdf

[25] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923774/Attorney_General_s_Guidelines_on_Disclosure_2020_NOT_YET_IN_FORCE.pdf

[26] Lifted from the *ACPO Good Practice Guide for Digital Evidence*

[27] https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf, paras 3.15-3.17

provider, this has to be one of the least dangerous activities carried out by an agency. The operator stays in their office and uses a keyboard, a telephone, a screen, and possibly a loudspeaker. The installer of a voice probe or device of equipment interference, the products of which are admissible under "property interference" or Part 5 IPA 2026 , must covertly visit hostile territory. More widely; the agent handler, physical surveillance operator and under-cover personnel must all go out into the "field".

7. **Rights of Innocent Third Parties** The rights of third parties who had innocent connections with an accused and who conversations with them might have been intercepted will be dealt within the same way as innocent people who have email contact with suspects and whose emails are found in storage on smartphones, PCs, tablets, laptops, on mainframes and in cloud services. There the collateral intrusion problem exists already and is in fact much greater. Data captured via interception is only caught during the duration of the interception exercise; data captured from storage, including that acquired via equipment interference will almost always have a very strong historic quality – several years' worth. The innocent conversations will only be seen/heard by lawyers and experts and will not be used in open court. Abuse of such data would be a contempt of court. Guidance is provided by the case of Carl Bater-James and Sultan Mohammed v the Queen [2020] EWCA Crim 790 which covers four Principles, of which the first three are relevant. There is also a draft Code of Practice issued under the Police, Crime, Sentencing and Courts Act, 2022[28]

8. **Use by Defence** The normal use of intercept evidence would be to show planning, intent, or "bad character"[29]. The usual stances of the defence will include: that the material has not been collected in a reliable manner, that authorisations have not been correctly obtained, that the prosecution have misidentified the speakers/participants; that the selected passages are being misinterpreted as to significance and meaning; that by also referring to other conversations in the unused material, a different light is shed on the motivations of an accused. But all these are within the normal scope of court activity and in any event applies to material obtained by property interference and from computer data storage[30] which are currently admissible. Defence lawyers are bound, inter alia, by the law enforcement processing requirements of DPA 2018 Part 3 and ss17-18 CPIA 1996 – Confidentiality of disclosed information. Presumably these also apply to their sub-contractors, including experts.

---

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1076098/PCSC_Extraction_Consultation_Final_.pdf

[29] Possible, subject to certain judicial safeguards, under ss 98 ff Criminal Justice Act 2003.

[30] A frequent issue with personal computers used by several people is "whose fingers on the keyboard at the relevant time?

RESPONSE TO INDEPENDENT REVIEW OF THE INVESTIGATORY POWERS ACT 2016:

SUPPLEMENTAL NOTE

PETER SOMMER

22 MARCH 2023

The Annual Report of the Investigatory Powers Commissioner for 2021 (IPCO 2021) was published after the deadline for responses to the Independent Review but I wish to draw attention to one aspect which reinforces my own observations.

In paragraphs 2.10 ff of IPCO 2021 the following appears:

> 2.10 In early 2021, we conducted a review of the definition of CD and identified many areas of ambiguity arising largely from the Government's decision to adopt a technology neutral drafting style in the IPA. The benefit of this approach is that it aims to ensure that the legislation has longevity by being able to accommodate developments in technology. The trade-off, however, is that the definition has to adopt a degree of ambiguity in order to accommodate those changes in technology. CD is a particularly complex area. It includes data that goes to the heart of how technology systems operate. Determining what constitutes CD under the current definition has found us needing to spend significant time and resources discussing a particular system or service with the Technology Advisory Panel (TAP), sometimes even down to the packet level; such discussions also often generate multiple legal views.
>
> 2.11 The outcome of our review was that the IPC is concerned that the current definition of CD is not fit for purpose. He feels that both operational professionals and the public should be able to understand with relative ease what data is CD and what data is not. It cannot be right that only a combination of systems engineers and legal experts poring over the legislation and Code of Practice can reach a tentative conclusion on what is the most widely used investigative power.
>
> 2.12 In an attempt to address this, throughout 2021 joint discussions were held between OCDA, IPCO and the Home Office Investigatory Powers Unit to develop additional guidance as to the definition of CD and TO. The guidance explained the IPC's and Home Office's agreed view that the definition of TO is broad, covering many companies which do more than just provide a telecommunications service and which might not be aware that they are a TO within the meaning of the IPA. We consider that the definition is not limited to telephony and internet service providers but is broad enough to include any website owner or operator. This means that social media platforms, online marketplaces, streaming platforms, online dating sites, food delivery services, banks, cloud providers and taxi services booked online are all TOs.

2.13 It is important to note, however, that unlike internet service providers which may be exclusively a TO, most of these types of companies will only be a partial TO in respect of certain services. For example, a business which simply provides a telecommunications service is likely to hold all users' account data as CD. With partial TOs, it is, therefore,necessary to determine what data a company holds as a TO rather than for the purposes of other parts of the business as, in general, a CD authorisation will only be available in relation to the data it holds as a TO. For example, the guidance describes how a payment method used for a subscription to an online streaming service would be CD. However, if that company also operates an online marketplace then the payment method used for a transaction would not be CD, as a payment for goods does not relate to the provision or use of the telecommunication service, i.e., the operation of the website.

2.14 The challenges for operational practitioners, OCDA and TOs to identify what data is CD and what is not are self-evident, especially if the public authority and OCDA are not familiar with how that business operates. The guidance was formally "launched" by the IPC and the Home Office in November 2021 and will be implemented after a programme of training across public authorities during 2022. We will report on progress on the interpretation and impact on the level of compliance in our 2022 Annual Report. It is the IPC's expectation that the guidance will ultimately be included in the next update of the Code of Practice.

2.15 To illustrate one issue with the definition of CD, under old section 21(4)(c) of RIPA, the definition of CD included:
"any information not falling within [the preceding paragraphs] that is held or obtained,
in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service".

2.16 The definition therefore clearly covered what is often called "subscriber" or "account" data (i.e. "entity data" under the IPA). This is vital for law enforcement as it enables them to identify who is using a particular system or service. It is of note that paragraph (c) of the RIPA definition, in contrast with the preceding paragraphs, did not carve out the content (i.e. the meaning/substance) of a communication. It therefore did not previously matter how a TO held data, i.e., whether it obtained or held data as content. Paragraph (c) could, however, on its face, include content such as the body of an email. In enacting the IPA, Parliament decided expressly to carve out content from *all* limbs of the definition of CD (see section 261(5) of the IPA). On one view, a large proportion of what is traditionally considered to be subscriber or account data comes from content; for example, your name may be included in an electronic web form when you open an online account and when you click "submit" it is sent to that company's servers. The "content" or "the meaning" of that communication is the information you have entered in the form. If that is the only record ofthe subscriber or account data held by the TO then, if that analysis is correct, it places such data beyond the ambit of a CD authorisation. This may therefore pose significant difficulties for law enforcement and other public authorities who rely on this vital information to protect the public. For this reason alone, the IPC considers the case for legislative clarification to be strong.

The analysis of the problems of separating communications data (CD) from content is very similar to the observations I made in my Response at paragraphs 9, 21-25 and 32-36.

However I strongly suspect that the case for "legislative clarification" will need to include removing s 56 IPA and allowing "content" to be admitted. At paragraphs 55-60 I show that introducing a tri-level warranting scheme would be relatively simple but would also remove many of the problems IPCO 2021 identifies.

I note that IPCO 2021 also refers to the problems of defining what is meant by a "telecommunications operator"; although I understand the issues I decided to limit my Response to those areas where I have had immediate professional experience.

At paragraph 65 I quote the IPC 2020 statistics for the issue of law enforcement TEI warrants. The IPCO 2021 figure is 1139 (up from 1036) but my underlying argument remains unaltered.

9.