Bar Council response to the Home Office consultation on the Investigatory Powers Act 2016: Codes of Practice

1. This is the response of the General Council of the Bar of England and Wales (the Bar Council) to the Investigatory Powers Act 2016: Codes of Practice consultation[1].

2. The Bar Council represents over 15,000 barristers in England and Wales. It promotes the Bar's high quality specialist advocacy and advisory services; fair access to justice for all; the highest standards of ethics, equality and diversity across the profession; and the development of business opportunities for barristers at home and abroad.

3. A strong and independent Bar exists to serve the public and is crucial to the administration of justice. As specialist, independent advocates, barristers enable people to uphold their legal rights and duties, often acting on behalf of the most vulnerable members of society. The Bar makes a vital contribution to the efficient operation of criminal and civil courts. It provides a pool of talented men and women from increasingly diverse backgrounds from which a significant proportion of the judiciary is drawn, on whose independence the Rule of Law and our democratic way of life depend. The Bar Council is the Approved Regulator for the Bar of England and Wales. It discharges its regulatory functions through the independent Bar Standards Board.

Overview

4. In this response we have focused, in particular, on the Code of Practice on Interception of Communications. The section on the Interception Code includes the Bar Council's major comments and concerns about the Act and the way it will be implemented. As there set out, the Bar Council's principal objection to the Act is the exclusion of material covered by legal professional privilege (LPP) from these powers of interception and examination by the state.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593725/IP_Act_codes_consultation_Feb2017_FINAL_WEB.pdf

5. We have also included comments on the Codes of Practice dealing with (a) bulk acquisition of communications data, (b) equipment interference, (c) retention and use of bulk personal datasets and (d) national security notices.

6. Each of the Codes includes at the end a short helpful section setting out the process by which an aggrieved person can make a complaint about powers exercised under the Act.

Background: Investigatory Powers Act 2016 and Legal Professional Privilege

7. The Investigatory Powers Act 2016 received Royal Assent on 29th November 2016. The long title to the Act reads –

> *An Act to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.*

Section 1(1) identifies the intent of the Act to allow interception of communications in accordance with law –

> *This Act sets out the extent to which certain investigatory powers may be used to interfere with privacy.*

8. Despite the statutory constraints on the use of intrusive powers by the state (which are both welcome and necessary), its effects are wide-reaching. The Act periodically uses the expression that actions authorised by the Act "shall be treated as lawful for all other purposes"[2]. This language was adopted from s.27 of the Regulation of Investigatory Powers Act 2000 which was interpreted by the House of Lords in *R v McE*[3] to enable the state to intercept communications between a lawyer and client which was subject to LPP. Previously such communications had been regarded as immune from eavesdropping by the state (or anyone else). The House of Lords decided that the wording of s.27 was sufficiently clear to overturn this historic constitutional protection from state intrusion. Lord Phillips, dissenting, described as "chilling" the effects of this decision on the conduct of litigation and the ability of lawyers to provided candid advice to clients[4].

---

[2] E.g. s.6(2)

[3] [2009] UKHL 15

[4] At paragraph [51]

9. The Act expressly authorises interception of and access to communications between lawyers and clients which are subject to LPP. The definition of LPP is set out in s.263(1) of the Act under "items subject to legal privilege", which states that term

> *(a) in relation to England and Wales, has the same meaning as in the Police and Criminal Evidence Act 1984 (see section 10 of that Act)*

S.27 contains a series of additional safeguards before an application for a warrant for intercepting items subject to LPP can be granted and authorised by a Judicial Commissioner. The rubric of s.27 is "Items subject to legal privilege". S.27 might have, but does not, contain a cross-reference to s.263(1) for the definition. You have to find it yourself by going to s.265 the index of defined expressions (which is not comprehensive).

10. No longer can a lawyer assure a client that what is said in conference or in written communication will remain confidential, even in circumstances where the client is not alleged to have engaged in any illegal conduct. It is for this reason that the Bar Council opposed those provisions of the Act which remove the protection of LPP and in so doing undermines the necessary trust which must exist between client and lawyer for citizens' rights to be effectively pursued and unlawful conduct effectively challenged.

11. This Act does not affect existing powers of non-intercept surveillance nor of covert human surveillance for which statutory authority is provided by other legislation.

Interception of Communications Code of Practice

12. The Bar Council considers that the draft Code which relates to powers conferred by Part 2 and Part 6 chapter 1 of the Act is well-written and generally clear. It expands on the language of the Act and gives the provisions context. The Act is complex and so the Code necessarily cannot avoid echoing that complexity.

13. When it comes to LPP, while the Code amplifies the reason for the sensitivity of LPP and how it falls into a special category, it gives little assistance to any who will be applying for a warrant in how to spot when LPP is likely to feature. Part 9 of the Code at paragraphs 9.36-9.37 and 9.43-9.67 set out the principles to be applied where LPP is involved. In particular paragraphs 9.45 and 9.46 refer to s.27 of the Act which creates the conditions which must be met before LPP material can be intercepted and accessed. Paragraph 5.33 includes cross-reference to part 9 in its section on targeted interception warrants. Paragraph 5.33(s) refers to s.51 of the Act when it should be to s.52. This will no doubt be corrected in the final version.

14. Paragraph 9.43 of the Code reiterates that the test for LPP is that set out in s.10 of the Police and Criminal Evidence Act 1984, and then in effect says "If in doubt, ask a lawyer". Paragraph 9.43 helpfully states that privilege is not lost where a professional legal adviser is advising a person who is suspected of having committed a criminal offence. Paragraph 9.45 then states –

> *Where there is doubt as to whether the communications are subject to legal privilege or over whether communications are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant intercepting agency.*

15. We consider that the Code should stipulate that legal advice must be sought whenever it is contemplated applying for a warrant which will or may access communication involving a lawyer. In addition, it should provide suggestions for how to recognise when a communication might involve LPP, such as reference to a database of lawyers' contact details – either published or covert. S.10 of the Police and Criminal Evidence Act 1984 is simple in its terms, but it leaves unsaid in what circumstances LPP arises during communications with a lawyer. It required a series of decisions in the *Three Rivers* cases[5] for the House of Lords to identify the parameters of LPP in cases involving, among other issues, communications with third parties. Inadequate understanding will lead to violations of LPP which will undermine confidence in the rule of law, one of the democratic cornerstones of the security of citizens. This risk is a real one given the power of the Secretary of State under s.24 to authorise interception warrants in urgent cases before receiving the approval of a Judicial Commissioner. Paragraph 9.37 states that "authorised persons" should receive on the safeguards regarding privileged information. This repeats similar requirements in paragraph 6.72 which calls for "regular mandatory training regarding the provisions of the Act and specifically the provisions of section 152 and the requirements of necessity and proportionality" to be provided to all "authorised persons" who examine material obtained under bulk interception warrants (Part 6 of the Act). Unfortunately paragraph 6.72 does not refer to the need for specific mandatory training on the provisions of section 153 which provides additional safeguards for items subject to LPP obtained under a bulk interception warrant. Nor does it include a draft of what such guidance. "Authorised persons" are defined in footnote 20 to paragraph 6.5

[5] *Three Rivers District Council and Others v Governor and Company of the Bank of England (No. 6)* [2005] 1 AC 610

Authorised persons is used in this Code[6] to mean an officer who has a suitable level of training and security clearance and who is permitted to select bulk data for examination.

16. The Bar Council recommended that the Code should provide that training to the lawyers involved and any other person within the agency who applied for a warrant should be specifically trained in LPP. To the extent that has been adopted in paragraph 9.37 we are grateful, but the persons included in that training must be extended. Even if our recommendation is accepted it will reduce but not eliminate what we see as an unjustified risk to the rule of law.

17. The Act distinguishes between communications content and communications data. The latter means details such as the date, time, telephone or electronic device used to make or receive the communication. During the Bill stage the Government insisted that the powers to access communications data could not impinge on LPP which they claimed was confined to content. The Bar Council disagreed, arguing that communications data alone could identify the parties communicating which would in some instances identify or at least indicate the nature and content of the communication. In paragraph 2.18 of this draft Code the Government accepts that data which is not "content" can convey meaning, e.g. a link between two persons. But such data does not count as "content" for the purposes of s.261 (the definition section) and "the fact that some meaning can be inferred from it does not make it content." Our concern is that warrants for access to communications data under Part 3 of the Act do not require authorisation by a Judicial Commissioner except in limited circumstances, namely when access is applied for by a local authority. In all other cases the state can gain a warrant to access communications data without a Judicial Commissioner having the opportunity to consider any LPP issues. Because the Act does not specify the need for authorisation by a Judicial Commissioner for Part 3 acquisition of communications data, the Bar Council cannot ask that such a process be included in the Codes of Practice. We can only lament the failure of Government and Parliament to provide even the limited protection which a Judicial Commissioner could provide were that process applicable for communications data.

18. We note that paragraphs 4.2 and 4.4 explain the provisions in ss.15(2)(b) & 136(2)(b) which allow interception warrants to authorise obtaining secondary data. Paragraph 4.4 states that under no circumstances may a UK intercepting agency ask an international partner to undertake interception on its behalf which would be a deliberate circumvention of the Act. We now know as a result of exceptional comments made by GCHQ, the FBI and the US National Security Agency (in response to assertions made by President Trump) that mutual respect for legality is regarded as essential. Paragraph 4.4 is an explicit example of this principle set out in an

[6] There is no definition of "Authorised person" in the Act

enforceable code. This and paragraphs 9.32 and 9.53 to 9.55 mean that the same (limited) safeguards apply to items subject to LPP whether the intercept is carried out by our security services or by an overseas state and whether the fruit of the intercept is intended for here or is a result of a mutual assistance request by a foreign state.

19. The conditions for granting an interception warrant include "Necessity and Proportionality". Paragraph 4.12 includes a cross-reference to Chapter 9 and the particular safeguards which are set out there, including for LPP. This is a helpful cross-reference in a complex process.

20. Section 27(6)(c) provides that where there are exceptional and compelling circumstances justifying intentional interception, or selection for examination, of items subject to LPP on the grounds that it is necessary for the purpose of detecting or preventing serious crime (*per* Section 20(2)(b)), the interception/selection must be "necessary for the purpose of preventing death or significant injury" – ie. detection is insufficient and serious crime for these purposes is in markedly different terms to the general definition in Section 263 (as relevant here: an offence carrying 3 years imprisonment or "conduct involving the use of violence"), which is expressly referred to in paragraph 4.10.

21. Paragraph 9.48 does not draw attention to the extent of the limitation on the justification for the interception/selection but rather adopts yet another definition of the applicable physical harm, namely a threat to "life and limb". Further the boxed example refers simply to "harm". It is suggested that in this regard the Code is confusing and misleading. It should not water down the statutory requirement and should draw attention to the revision of the definition of serious crime.

22. Paragraphs 9.22-9.24 and 9.60 (in respect of items subject to LPP) refer to the requirement for destruction of items other than in circumstances where its retention is necessary for authorised purposes, *per* Section 53. Paragraph 10.2 refers to the requirement to keep records of the arrangements in place for the destruction of material. It is suggested that there should be an obligation on the relevant authority to make and keep a record of the fact of destruction of individual items subject to LPP, save where the items are automatically deleted (see paragraph 9.23).

23. Paragraphs 10.15 to 10.31 concern what happens when LPP material has been intercepted or acquired and examined "in error". Paragraph 10.18 states that the Commissioner must be notified "as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred" and a full report submitted to her/him as soon as reasonably practicable. There is an argument that the Commissioner should

be notified immediately so that directions can be given to reduce the impact on the person(s) whose rights have potentially been violated. That would enable to Commissioner more speedily to determine whether the error is a "serious" error and one which requires the person concerned to be notified in accordance with s.231. However, there is the risk that the Commissioner's time could be taken up with what turn out to be unnecessary fears. When the matter is reported to the Commissioner, the report must identify when the error was first suspected (paragraph 10.19). We recommend that the Investigatory Powers Commissioner should investigate the reasons for any delay in reporting a relevant error and include in the annual report a recommendation as to whether immediate reporting of suspected errors is desirable. Where the error relates to the unauthorised dissemination of LPP material in the context of ongoing litigation (whether criminal or civil) between the state and the person, the public authority which made the error should inform the Judicial Commissioner of that fact as part of its submissions pursuant to Section 231(5). Whilst it should be inconceivable that the JC would not be informed, this ought to be an express requirement.

24. Paragraph 11.9 provides for the obligations on the holder of retained intercepted content or secondary data if it "comes to his attention" that there is a prosecution (the term is "at the prosecution stage", the meaning of which is unclear – presumably it refers to post charge). Consideration should be given to whether, when relevant material is retained, there should be an obligation on the holder proactively to ascertain whether there is a prosecution. As the code is currently drafted it appears to be a matter of chance whether it comes to his "attention" or not.

Bulk Acquisition of Communications Data

25. Paragraph 11.8 contains a reminder of the duty on prosecutors to review all content and secondary data to "make sure that the prosecution is not proceeding unfairly". Paragraph 11.9 provides that if it comes to the attention of a holder of retained intercepted content or secondary data that there is a prosecution (the term is "at the prosecution stage", the meaning of which is unclear – presumably it refers to post-charge) then the prosecutor should be informed that a warrant has been issued under s.15 and that content or secondary data possibly relevant to the case has been intercepted. This Code deals with powers under chapter 2 of Part 6 of the Act, i.e. acquisition of bulk communications data from a telecommunications operator (s.158(6)) in respect of communications data relating to the acts or intentions of persons outside the British Islands (s.158(3)). This is to be distinguished from chapter 1 of Part 6 which empowers the Home Secretary to issue a warrant on the application of the head of an intelligence service for bulk interception of communications to or from a person overseas relating to the acts or intentions of a person outside the British Isles (s.138(1)(a) and (3)).

26. Paragraph 3.7 states that chapter 1 does not allow bulk obtaining and examination of communications in relation to individuals in the UK whereas chapter 2 does provide for obtaining and selection for examination of communications data "in relation to individuals within the UK". It is not clear that the Act does impose this restriction. Chapter 1 of Part 6 is confined to applications by the security services "relating to the acts or intentions of a person outside the British Islands" but would include communications with such a person received via an overseas telecommunications operator from a lawyer in the UK.

27. A distinction is made by s.261 (the section containing "telecommunications" definitions) between "communications data" (s.261(5)) and "content of a communication" (s.261(6)). Communications data is defined for the purposes of the Act by s.261(5) as -

> *in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data … but does not include any content of a communication*

The general definition section, s.263, defines "data" as

> *"data" includes data which is not electronic data and any information (whether or not electronic)*

As both these definitions are specifically applied to chapter 2 of Part 6 by s.175(2) it is to be hoped that the exclusion in s.261(5) of content prevails over "any information" in s.263.

28. This is but one example of the complexities of this Act, and the difficulties of navigating its provisions so as to be sure of the extent of any power conferred by it and any statutory restriction on that power. It demonstrates the need for the Judicial Commissioners who must approve these warrants to be properly assisted by lawyers. There is at present no provision for the Judicial Commissioners to be able to receive representations from an advocate on behalf of the target of the warrant or the person or entity on whom the warrant will be served. It is understandable that those persons should not be given notice of an application for a warrant given the conditions which must be satisfied before warrants can be authorised, but it does mean that legitimate arguments about interpretation and the balance between the powers of the state and the duties to protect individuals' interests will depend on the Judicial Commissioners adopting inquisitorial role for themselves, which is not necessarily encompassed within their duty to apply the test of judicial review to the approval of decisions to

issue, amend and renew warrants.[7] Interpretation of the Act and the Codes will then be subject to the judgments of the Investigatory Powers Tribunal and the Court of Appeal (ss.232, 242 and 243) which are likely to be delivered substantially after the decisions under review have taken effect and may only be published in exceptional cases due to security concerns. Consideration should be given to appointing special advocates as *amici* where the Judicial Commissioner thinks necessary to have adversarial argument. This process should ensure compliance with the decision of the Grand Chamber of the CJEU in *Secretary of State for Home Department v Watson*[8].

29. In paragraph 2.18 of the draft Code on Interception of Communications the Government accepts that data which is not "content" can convey meaning. This blurs the distinction between data and content. As was said by the CJEU in *Watson* at paragraph [55]

> *Even though that data does not include the content of a communication, it could be highly intrusive into the privacy of users of communications services.*

30. There is no equivalent concession in this Code and no reference to the Interception of Communications Code which would make the point. Paragraph 2.9 of this Code asserts –

> *It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.*

31. There is a footnote to *inferred meaning* referring to s.261(6)(a) which concerns "events data". There is no definition in the Act of "inferred meaning". Why the discrepancy? Is the potential for content seeping into data not equally relevant to the application of chapter 2 of Part 6 as it is to Part 2? Is this a consequence of different teams drafting each code? Although data can convey content, the Act expressly disregards that fact when it comes to the safeguards for the interception of content. This a fundamental problem with the Act and is a concern that we raised in our response to the Communications data codes of practice: acquisition, disclosure and retention consultation in 2015[9].

32. Chapter 1 of Part 6 (dealing with content of communications) includes in s.153 additional safeguards for items subject to legal privilege. No such provision appears in chapter 2. This Code in paragraphs 6.20 to 6.23 contains the process for dealing with

---

[7] See s.23(2) for Part 2; ss.89(2) and 91(2) for Part 4; s.108(2) for Part 5; ss.140(2), 146(2), 159(2), 165(2), 179(2) and 187(2) for Part 6; ss.208(2), 216(2), 219(4), 228(8) and 225(8) for Part 7; and ss.254(3) and 258(3) for Part 9.

[8] Judgment of 21. 12. 2016 — Joined Cases C-203/15 And C-698/15 – see paragraphs [109]-[111] and [119]-[120]

[9] http://www.barcouncil.org.uk/media/336369/bar_council_response_to_the_communications_data_codes_of_practice.pdf

communications data relating to MPs, doctors, journalists and lawyers. Paragraph 6.20 states

> *It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.*

33. The reference in paragraph 6.21 to s.2 of the Act[10] gives inadequate emphasis to the significance of the potential breach of LPP by the fact of access to communications data as well as the capacity to examine its detail. It fails to explain why LPP is sensitive or how it is to be assessed. It is to be hoped that those applying for warrants as well as those issuing them and the Judicial Commissioners authorising them will be familiar with intricate detail of the Act as well as all the codes of practice; but it should not be assumes that this will be the case, particularly for a busy Secretary of State who was not responsible for the Act.

34. It remains doubtful whether these provisions for bulk access will satisfy the conditions set out by the Grand Chamber of the CJEU in *Watson*. The focus in the Act on the gravity of conduct which must be the subject of warrants will probably be compatible. The duration of the warrants, the ability to amend and renew may not survive challenge. It remains to be seen whether the examination of the facts in individual cases will be sufficiently robust to satisfy that judgment, including how the test of judicial review is applied – will it be simply procedural or a full merits review which *Watson* indicates is necessary[11]?

Equipment Interference

35. This Code deals with targeted interference under Part 5 and bulk interference under Part 6 chapter 3. The purpose of these powers is to enable the powers of interception and acquisition of communications and data to be effective (paragraphs 3.10-3.13). It includes authorisation of intrusive or non-intrusive surveillance in order to identify and locate the equipment (paragraphs 3.17-3.21) but does not authorise interception of a communication unless otherwise authorised (paragraph 3.22).

36. Chapter 9 of the Code sets out details of the safeguards before such warrants can be issued and executed and the steps to be taken when dealing with items subject to legal privilege are set out in paragraphs 9.39 to 9.63.

37. Paragraph 3.9 identifies the source of the definition of LPP as s.98 of the Police and Criminal Evidence Act 1984. That should be a reference to s.10 of that Act.

38. The Code recommends that equipment interference agencies should provide internal guidance to their staff to assist them to determine whether a lawyer who is a

---

[11] E.g. at paragraph [120]

target is acting in a professional capacity (paragraph 9.52). Any such internal guidance provided by any agency or authority which is empowered by this Act to apply for or execute warrants or examine material obtained under the Act should be published.

39. Paragraph 9.41 states that where there is doubt as to whether the items are subject to LPP or whether the crime exception applies then the advice should be sought from a legal adviser within the relevant equipment interference agency. To avoid inconsistent advice from within different agencies and government agencies we strongly suggest that a dedicated section within the government legal service be set up to deal with issues of LPP. This will become an important issue in several applications under the Act. This is the first time that a statute has expressly authorised access to and interference with privileged communications between lawyer and client.[12]

40. When it is discovered that LPP material which has been obtained inadvertently, paragraph 9.56 prescribes

> *an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes set out in section 129(3). If not, the material should not be retained, other than for the purpose of its destruction.*

41. This direction ignores the special sensitivity of LPP material. S.129 does not address items subject to LPP. The extra safeguards provided for LPP material elsewhere must be applied in these cases, and so a requirements to apply the provisions of s.131 (which imposes additional safeguards for items subject to LPP) should be added.

42. Where items which are subject to LPP have been acquired or selected for examination the Investigatory Powers Commissioner must be informed "as soon as reasonably practicable" (paragraph 9.58). There is no reason why that should not be done <u>immediately</u> it is realised that LPP material has been acquired or selected, especially since paragraph 9.58 envisages that Commissioner being asked for advice and guidance whet here is doubt whether material is subject to LPP.

43. As in the case of the Bulk Acquisition of Communications Data Code, there is a question whether the provisions for thematic warrants under Part 5 (paragraph 5.12) and bulk interference warrants (chapter 6 of the Code) are sufficiently focused to satisfy the *Watson* judgment.

44. Sections 106(1)(a) and (3)(a) provide that a law enforcement chief can issue a targeted equipment interference warrant if such is necessary, *inter alia*, "for the

[12] In *R v McE* [2009] UKHL 15 the House of Lords interpreted the Regulation of Investigatory Powers Act 2000 as enacting a power to intercept privileged lawyer/client communications, even though there was no express provision to that effect in the Act.

purpose of preventing or detecting serious crime"[13]. Section 112(6)(c) states that where there are exceptional and compelling circumstances justifying interference with equipment for the purpose of obtaining, or selecting for examination, items subject to LPP, such must be "necessary for the purpose of preventing death or significant injury". Paragraph 9.44 of this Code repeats the terms of Section 112(6)(c) in contrast to paragraph 9.48 of the Interception Code which restates them as a "threat to life and limb". This inconsistency again suggests that different teams have drafted the Codes and it should be corrected. The boxed example again simply refers to "harm".

Retention and Use of Bulk Personal Datasets

45. Bulk Personal Datasets can be acquired by a security and intelligence agency for intelligence purposes under Part 7 of the Act. The information obtained will relate to groups of individuals, many of who it is known will not be involved in any activity which is the subject of the Act (paragraph 2.2).

46. The expression "bulk personal datasets" is not defined in the Act or the Code other than in paragraph 2.2 –

> *For the purposes of the Act and this code, a set of data that has been obtained by a Security and Intelligence Agency comprises a BPD where it includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.*

47. The Code recognises that the fact that a person is a lawyer is not sensitive, nor are the kind of professional details which are likely to appear on a CV or website (paragraph 4.14).

48. There is a helpful reminder at paragraphs 7.12 and 7.13 of the need for sensitivity when dealing with material which is subject to LPP, including the possibility of unintended consequences. It is a shame a similar paragraph to 7.13 does not appear in each of the other codes.

49. Procedures dealing with LPP material and the special need for sensitivity are set out in more detail in paragraphs 7.20 to 7.36. Unfortunately paragraph 7.30 contains similar guidance about the decision whether to retain LPP material which has been obtained inadvertently as that set out in the Equipment Interference Code (see paragraph 17 above). Whenever such a situation occurs, the Code should

[13] The need for a separate and less stringent test for a different law enforcement chief pursuant to Section 106(3)a) is not obvious.

emphasise that the full safeguards for LPP material as set out in e.g. ss.27, 131 and 194 must be applied.

50. Paragraph 7.34 contains a direction that when LPP material is disseminated to an outside body it must be accompanied by a clear warning that it is subject to LPP, and paragraph 7.35 points out the potential abuse of process when any such dissemination takes place. This creates the interesting conundrum of whether LPP is lost when disseminated to a third party; or whether LPP remains intact for all other purposes even though ineffective against state intrusion for the purposes of the Act. Again the question is raised – why is a similar warning not included in all the other Codes?

51. As in the case of the Bulk Acquisition of Communications Data Code, there is a question whether the provisions for Bulk Personal Datasets under Part 7 are sufficiently focused to satisfy the *Watson* judgment.

52. Section 204(3)(a)(ii) (Class BPD) warrants and Section 205(6)(a)(ii) (Specific BPD) warrants can be issued where it is necessary "for the purpose of preventing or detecting serious crime". Where the purpose is to identify items subject to LPP, or such identification is likely, there must be compelling and exceptional circumstances which necessitate the issue of the warrant, *inter alia*, for "preventing death or significant injury" (Sections 222(1)(a), (5)(b) and (7(c)). Paragraph 7.27 restates this criterion as a "threat to life and limb", as in the Interception Code but in contrast to the Property Interference Code. In this regard the current conflicting language within the Act, between the Act and the individual Codes and between the Codes is confusing. Where, exceptionally, authorisation is being granted for the intentional surveillance of LPP material it is imperative that those who are operating within the new statutory regime are given the clearest possible guidance.

National Security Notices

53. Sections 252 to 258 in Part 9 of the Act empowers the Secretary of State to issue a notice to a telecommunications operator in the UK to take specified action. This is not a warrant and, unlike them, is not subject to an application process. The action stipulated in the notice must be something for which a warrant would not be necessary.

54. The subject of LPP material is dealt with peremptorily in paragraph 3.8

> *Paragraph 2 of Schedule 7 of the Investigatory Powers Act provides that a code issued under the Act must contain particular provision designed to protect the public interest in the confidentiality of journalistic information and any data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information. Where a notice requires the taking of a step that involves an*

interference with privacy, and a warrant or other authorisation has been obtained to authorise that conduct, the Code of Practice relevant to that authorisation will contain provisions required by Paragraph 2 of Schedule 7 of the Act. Where a warrant or authorisation is not available to authorise an interference with privacy, it will never be appropriate to obtain journalistic information or any data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information via a national security notice. As such, it is not necessary to include more detailed safeguards in respect of such information in this code as they are not relevant.

55. This paragraph seems to assume that LPP material is only to be found in lawyers' possession. The process under Part 9 does not in itself result in the state gaining access to any communications or data, it enables the Secretary of State to ensure that the material is accessible should it become necessary for a warrant in respect of any of that material. However, Part 9 does not specify or restrict the actions which the notice can require; s.252(2) enables the notice to require the operator

to take such specified steps as the Secretary of State considers necessary in the interests of national security.

56. The disparate nature of this power is likely to affect material subject to LPP, whether in the hands of a lawyer or the client or a third party in whose hands it remains privileged. If, for example, the notice included a requirement to destroy or remove material which is subject to LPP, that could have the kind of unintended consequences which were sensibly included in paragraphs 7.13 1nd 7.35 of the Code on Retention and Use of Bulk Personal Datasets.

Bar Council
Tuesday 4 April 2017

For further information please contact
Natalie Darby, Senior Policy Analyst
The General Council of the Bar of England and Wales
289-293 High Holborn, London WC1V 7HZ
Email: NDarby@BarCouncil.org.uk