

IN THE MATTER OF
THE REGULATION OF INVESTIGATORY POWERS BILL
AND
IN THE MATTER OF
A HUMAN RIGHTS AUDIT FOR *JUSTICE* AND *FIPR*

ADVICE

1. In October 1999, Professor Jack Beatson Q.C. and I were instructed by *Justice* and the *Foundation for Information Policy Research* (“*FIPR*”) to consider the provisions of the Draft Electronic Communications Bill (Cm 4417), as published by the Department of Trade and Industry in July 1999. In our Joint Advice, dated 17 October 1999 we concluded that:

“there are serious concerns about the compliance of the draft Bill in its present form with the European Convention on Human Rights, in particular:

- a. The compliance of clauses 10 and 12 with the requirements of Article 6(1) ECHR (the right to a fair hearing) and Article 6(2) (presumption of innocence) (paragraphs 29 - 42 below); and
- b. The compliance of clauses 10 to 13 with the requirements of Article 8 (right to respect for one’s private life and correspondence) (paragraphs 13 - 28 below).

For the reasons given in paragraph 43 below, we also consider that the “secret” nature of some of the measures provided for by part III of the Act and the popularity of the internet and electronic commerce means that the category of potential “victims” under Article 34 of the Convention and section 7(7) of the Human Rights Act 1998 able to bring proceedings either in a domestic court or in the European Court of Human Rights (“the Strasbourg Court”) is potentially very wide indeed.” (para 3)

2. The Joint Advice was submitted to the Government and published *inter alia* on FIPR's website¹. Part III of the draft Electronic Communications Bill was subsequently withdrawn and is now, with some amendments, reintroduced as Part III of the Regulation of Investigatory Powers Bill ("RIP").
3. I am now instructed to re-consider the concerns expressed in our Joint Advice in relation to Part III of the RIP. Due to the time constraints imposed upon us, Professor Beatson Q.C. was unavailable to settle this advice.
4. I understand from those instructing me that there appears to be a perception in government circles that, due to the human rights sensitive nature of its content the Regulation of Investigatory Powers Act ought to be on the statute books before the Human Rights Act enters into force (2 October 2000): see e.g. the report in the *Financial Times* of 11 January 2000.
5. The amended provisions of Part III of the RIP show that a number of the concerns expressed in our initial Joint Advice have been taken on board and have now been accommodated. These include:
 - a) the Covert Investigations Commissioner's jurisdiction to review "the exercise and performance, **by any person** other than a judicial authority, of powers and duties conferred or imposed, otherwise than with the permission of such an authority, by or under Part III" (clause 53(3)(b), bold emphasis added);

1 Go to <http://www.fipr.org/ecomm99/econmaud.html>

b) the extension of the Tribunal's jurisdiction to any action brought under section 7(1)(a) of the Human Rights Act 1998 "relating to the taking place in challengeable circumstances of ... the giving of notice under section 46 or any disclosure or use of a key to protected information" (clause 56(2)(a) with clause 56(3) and (5)) and "to hear and determine any other such proceedings within subsection (3) as may be allocated to them ..." – see paragraph 26 of the Joint Advice;

6. Apart from these amendments, the serious concerns expressed in our Joint Advice remain and are, to some extent, aggravated by the amendments made.

Article 6 ECHR – presumption of innocence/privilege against self-incrimination

7. In dealing with the issue of the presumption of innocence, paragraphs 40 to 42 of the Joint Advice placed some reliance upon the judgment of the Divisional Court (Bingham LCJ, Laws LJ and Sullivan J) in R v DPP, ex parte Kebilene [1999] 3 WLR 175 and in particular on the *dicta* relating to the presumption of innocence. At the time of the Joint Advice this case was under appeal to the House of Lords.

8. In its judgment of 28 October 1999, the House of Lords allowed the appeal and reversed the decision (though not the relevant reasoning) of the Divisional Court. The House of Lords judgment is published at [1999] 3 WLR 972 and both judgments together are published at (1999) 28 EHRR CD1.

9. Paras. 40 to 42 of our initial Joint Advice state:

“Turning to the issue of the presumption of innocence, the offence under clause 12 resembles to some extent the offences considered by the Divisional Court in *R v DPP, ex parte Kebilene* [1999] 3 WLR 175, and the Supreme Court of Canada in *R v Whyte* (1988) 51 DLR 4th 481. In *ex parte Kebilene*, one of the offences charged was that of "without lawful authority or reasonable excuse [having] in his possession a quantity of books which contain information which is of such a nature as is likely to be useful to terrorists in planning or carrying out an act of terrorism". As Lord Bingham CJ held, this required the prosecution to prove the collection or possession of information, 'in itself innocent' (p. 190D), but the defendant had the burden of proving lawful authority or reasonable excuse. Lord Bingham CJ stated:

'A defendant who chooses not to give or call evidence may be convicted without *mens rea* of the offence being proved against him.

It seems to me that on their face both sections [under consideration] undermine, in a blatant and obvious way, the presumption of innocence.

Under section 16A a defendant could be convicted even if the jury entertained a reasonable doubt whether he knew that the items were in his premises and whether he had the items for a terrorist purpose. Under section 16B a defendant could be convicted even if the jury entertained a reasonable doubt whether the information had been collected or was possessed for any terrorist purpose. In both sections the presumption of innocence is violated.' (page 190F to H)

In *Reg v Whyte* (1988) 51 DLR (4th) 481, the Supreme Court of Canada considered a provision providing that where it is proved that a person charged with drunken driving occupied the seat ordinarily occupied by the driver he was to be deemed to have had the care or control of the vehicle unless he established that he did not enter the vehicle for the purpose of setting it in motion. It was held that this violated the presumption of innocence. Chief Justice Dickson, delivering the judgment of the court, stated:

'The real concern is not whether the accused must disprove an element or prove an excuse, but that an accused may be convicted while a reasonable doubt exists. When that possibility exists, there is a breach of the presumption of innocence. The exact characterisation of a factor as an essential element, a collateral factor, an excuse, or a defence should not affect the analysis of the presumption of innocence. It is the final effect of a provision on the verdict that is decisive. **If an accused is required to prove some fact on the balance of probabilities to avoid conviction, the provision violates the presumption of innocence because it permits a conviction in spite of a reasonable doubt in the mind of the trier of fact as to the guilt of the accused.**' (page 493, emphasis added)

This statement was approved by Lord Bingham CJ in *ex parte Kebilene*.

The reasoning in these statements applies *mutatis mutandis* to the offence established under clause 12 in respect of notices served under clause 10. Any addressee could be convicted of an offence under clause 12 while the jury had a reasonable doubt about whether, in fact, he had the key in the first place (or still had access to the key at the time disclosure was required). In *ex parte Kebilene* the DPP appealed to the House of Lords and the outcome of this appeal is awaited, but we consider the statements of principle by Lord Bingham and the Supreme Court of Canada to be strong indications that the provisions of clause 12 are likely to be held to violate the presumption of innocence in Article 6(2) of the Convention.”

10. In the House of Lords, Lord Steyn, giving the lead judgment with which Lord Slynn of Hadley agreed, stated that the Divisional Court’s conclusion that section 16A undermined the presumption of innocence was “overstated” ([1999] 3 WLR 972 at 984E). In doing so Lord Steyn, however, reiterated the “disfavour with which reverse legal burden provisions have been regarded by the Privy Council” but relied on the fact that the word “prove” in that section could be interpreted as placing only an evidential burden on the defendant. The appeal, however, was allowed on the basis that this particular decision of the Director of Public Prosecution was not amenable to judicial review. As a result, Lord Steyn expressly did not express a concluded view on the interpretation and compatibility of section 16A with Article 6(2) ECHR (see [1999] 3 WLR 972 at 985G to H).

11. Lord Cooke of Thorndon, agreeing with Lord Steyn, further explained:

“My Lords, **I see great force in the Divisional Court's view that on the natural and ordinary interpretation there is repugnancy.** To introduce concepts of reasonable limits, balance or flexibility, as to none of which article 6.2 says anything, may be seen as undermining or marginalising the philosophy embodied in the straightforward provision that everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. On its face section 16A of the Act of 1989 enables a person to be found guilty of a very serious offence merely on reasonable grounds of suspicion.

...

When the whole Act comes into force, the new canon of interpretation will be that, so far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights. This is a strong adjuration. It seems distinctly possible that it may require section 16A of the Act of 1989 to be interpreted as imposing on the defendant an evidential, but not a persuasive (or ultimate), burden of proof. I agree that such is not the natural and ordinary meaning of section 16A(3). Yet for evidence that it is a possible meaning one could hardly ask for more than the opinion of Professor Glanville Williams in *The Logic of "Exceptions"* [1988] C.L.J. 261, 265 that "unless the contrary is proved" can be taken, in relation to a defence, to mean "unless sufficient evidence is given to the contrary;" and that the statute may then be satisfied by "evidence that, if believed and on the most favourable view, could be taken by a reasonable jury to support the defence."

I must not conceal that in New Zealand the Glanville Williams approach was not allowed to prevail in *R. v. Phillips* [1991] 3 N.Z.L.R. 175. But, quite apart from the fact that the decision is of course not authoritative in England, section 6 of the New Zealand Bill of Rights Act 1990 is in terms different from section 3(1) of the Human Rights Act 1998. The United Kingdom subsection, read as a whole, conveys, I think, a rather more powerful message.

As this case has reached this House, there would appear to be something to be said for a resolution by your Lordships now of the question whether, when section 3(1) and the rest of the Human Rights Act is in force, it will be possible for provisions such as section 16A of the Act of 1989 to be read and given effect in a way which is compatible with the Convention rights. But the possibility of such a resolution had apparently not been foreseen by counsel; the argument on section 3(1) was by no means as full as is desirable if the effect of so major a new canon of interpretation is to be settled; and I accept that it would be premature to embark on the question. It should be left to be dealt with in this case, as far as may be found just or expedient, by the trial judge and on any subsequent appeals." ([1999] 3 WLR 972 at 986G to 987H, bold emphasis added)

12. As a result, their Lordships, though accepting that there was a possible interpretation of section 16A that could make that section compatible with Article 6(2) ECHR, left this issue to be argued before and decided by the trial court (and, on appeal, the Court of Appeal and, possibly, the House of Lords). They expressly

accepted that any such argument and decision would have to be based upon section 3(1) the Human Rights Act 1998 which provides that:

“So far as is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights.”

13. For the reasons we set out in our Joint Advice, the natural and ordinary meaning of wording of the provisions of the draft Electronic Communications Bill as considered by us were equally “repugnant” as those in section 16A, considered by Lord Cook. It appears that the Government has sought to answer this criticism (and the comments made by the House of Lords in Kebilene) by replacing the word “appears” with the words “believes on reasonable grounds” in clause 46(2) RIP, thereby reverting to language commonly used in the context of the issue of warrants, and by adding a second element to the offence under clause 49(1), namely that the accused “is a person who has or has had possession of the key”. This, however, fails to take into account two things:

- a) that section 16A of the Prevention of Terrorism (Temporary Provisions) Act 1989, the natural and ordinary interpretation of which Lord Cooke found “repugnant”, also refers to the concept of “reasonable suspicion”; and
- b) the unique technical difficulties arising in this context (see paras. 4 to 11 of our initial Joint Advice). In this context no protection is derived from the provision that the prosecution must prove beyond reasonable doubt that the accused “has or has had” possession of the key. In the vast majority of cases the accused may well be happy to accept that he “has had” the key (thereby verifying the “reasonable belief”) but, for the reasons set out in the Joint Advice, that does

not lead to the conclusion that he still “has” the key or access to it. As a matter of good practice, encryption keys are periodically changed and replaced and some systems even use a new key with every exchange of messages, destroying old keys continually (“Perfect Forward Secrecy”). Previous (and current) keys and/or the passwords that protect them are (a) easily forgotten and (b) may be lost e.g. through technical defects, such as faults in back-up procedures, premature or unintended deletion or operator error in reconfiguring complex systems options. In fact, it is understood that a computer which “hangs” during the process of encrypting the entire disk may destroy all or part of the data stored. If, as a result, the accused cannot remember the password to the private key stored on his computer or is otherwise unable to get access to it, nobody will be able to get access to it. However, under clause 49, as currently drafted, he would be guilty of an offence because he failed to comply with the section 46 notice. None of the defences set out in clauses 49(2) and (3) would avail the accused as they require disclosure of “all such information in his possession as was required by that person to enable possession of the key to be obtained” or of “sufficient information to enable possession of the key to be obtained”. As the key is “lost” no amount of information given will be “sufficient” to enable possession of the key to be obtained². However, if the accused accepts that (at one time) he had a key, he would still have to prove a negative virtually incapable of objective or corroborative evidence, i.e. that he cannot remember the password (or otherwise get access to the key), and a jury

2 This defence could only operate where e.g. a copy of the key is stored with a Trusted Third Party.

could/would still have to convict despite being in doubt about an essential element of the offence.

14. Added to the technical difficulties set out in the Joint Advice, those instructing us have drawn our attention to two further areas of concern

- a) The availability of technical means which would enable any computer user not only to encrypt files and make access to them subject to the need for a key but also to hide the files themselves and make access to them subject to knowledge of the required object name (“steganographic file systems”). Any individual who does not have both the object name and the password/key could not access those files and, more importantly, anybody who does not have the object name could not even ascertain whether files of the description sought are present on the computer³;
- b) The fact that there is a significant potential for conflict between the safeguards that would be necessary in order to ensure an ability to comply with a clause 46 notice and the requirements under principle 7 of the Data Protection Act 1998.

As the Data Protection Registrar stated, in her submissions to the Select Committee on Trade and Industry on the Draft Electronic Communications Bill:

“The security of information collected electronically is also an issue and Principle 8 of the 1984 Act and Principle 7 of the Data Protection Act 1998 require that those processing personal data take adequate security measures to protect it. This has implications for those collecting personal data over the Internet, especially where that data is of a sensitive or financial nature. **The Registrar expects to see organisations collecting information over the Internet putting**

³ I am instructed that analogous techniques are available in order to transmit data in a way that it becomes impossible to prove the existence of the communication via interception.

appropriate technical safeguards in place to prevent unauthorised access to the information they hold. Techniques such as encryption should also be used as part of that process where appropriate.”⁴

This puts those providing ecommerce opportunities and others charged with the management and/or custody of personal data with a very real dilemma.

Where they use effective and strong encryption protected by sophisticated passwords, with periodic changes to both the keys used and the passwords used, the likelihood that a password is lost or forgotten are significantly increased. However, failure to use such available technology to secure the data could effectively render them in breach of the Data Protection legislation.

15. Application of available technology, such as steganographic file systems, would make it impossible for prosecuting authorities to show (let alone prove) that there is “protected information” on the computer in question, which would authorise the issuing of a section 46 notice. This is of particular difficulty as it has recently been held in the context of the Police and Criminal Evidence Act 1984 that it was not permissible to seize material in order to sift through it to determine whether it fell within the scope of the warrant issued: R v Chesterfield Justices ex parte Bramley [2000] 2 WLR 409 (QBD).

16. However, the amendments to the “offence” under clause 49 further exacerbates the concerns expressed in paragraphs 29 to 39 about the possible infringements of the

4 Memorandum of 3 March 1999, para. 15, bold emphasis added; see <http://www.publications.parliament.uk/cgi-bin/htahl?WORDS=encrypt+data+protect+techniqu&STYLE=s&COLOR=Red&STEMMER=stem&URL=/pa/cm199899/cmselect/cmtrdind/187/9030902.htm>

privilege against self-incrimination. Under clause 49 it is for the prosecution to show that:

- a) a notice was served;
- b) the accused did not comply with the notice; and
- c) he has or has had possession of the key.

In the scenario outlined above, it would be impossible to prove by technical means that the accused “has” possession of the key. Even to prove that he “has had” the key could only be done through his admission. As none of the defences in sub-clause (2) or (3) could avail the accused his only “defence” would be to remain silent on the issue of “possession”.

17. The above would suggest that for anyone using encryption, in order to avoid unjustified suspicion and possible wrongful conviction, it would have to be good practice to

- a) Use steganographic file systems or equivalent technology; and
- b) Not to admit to ever having had a key rather than be helpful and co-operative.

For the vast majority of individuals this is counter-intuitive and for society in general counter-productive.

18. This clearly falls within the protection from self-incrimination as set out *inter alia* in the European Court of Human Right’s judgment in Saunders (as set out *inter alia* in our Joint Advice) and as most recently restated by the Scottish High Court of Justiciary in its judgment of 4 February 2000 in Brown v Procurator Fiscal, Dunfermline (Appeal No 1652/99). In that case, the High Court of Justiciary

reached its conclusion on the issue after a comprehensive review of the jurisprudence of the Court and Commission of Human Rights as well as Scottish, English, American, Canadian and South African case law. The consequences of this are further aggravated by the fact that under English law, unlike Scots law, convictions can be founded upon admission alone without any corroboration.

Article 8 – right to respect for private life

19. Part III of the RIP, as amended from the Draft Electronic Communications Bill, still does not sufficiently address the requirements of Article 8 ECHR as set out in paragraphs 15 to 25 of the Joint Advice. RIP still leaves the assessment of the necessity for the disclosure requirement and its proportionality as well as e.g. the existence of legal professional privilege to the person giving notice or “such other person” as notified in the notice, both of whom are members of the executive, without “supervision” by an independent judge: this type of procedure was expressly criticised by the Court of Human Rights in Kopp v Switzerland, which in turn was recently reconfirmed in Amann v Switzerland, judgment of 16 February 2000.

20. In paragraph 22 of the Joint Advice, a quotation from the recent judgment in Valenzuela Contreras v Spain, sets out the minimum safeguards required in order to avoid an abuse of power. These include:

- a) definition of the category of persons liable to interception – in RIP, this definition appears to be everyone who uses a computer and encryption/decryption software or any browser of digital television to access a

website with a password: this includes virtually everyone who participates in ECommerce;

- b) a judicial order for interception;
- c) the nature of the offences which may give rise to such an order – this is of particular importance in cases, such as those likely to arise under the RIP, where the interference with the individual’s correspondence and private life is of such a substantial nature. As the European Court of Human Rights has repeatedly stated, the more substantial the interference with a Convention right, the stricter the test of “necessary in a democratic society” and, therefore, proportionality will be applied. However, the RIP does not set out the offences in relation to which a notice may be given and disclosure required. The way clause 46 is currently drafted it could be applied in the context of any (low-level) data gathering exercise relating e.g. to minor offences and clause 46(3) would impose a requirement, in this context, to assess the proportionality of the interference. It is also noteworthy that clause 46(2)(b)(ii) extends the power to demand the key beyond the investigation of crime or the need to protect national security to cases where it is “likely to be of value for purposes connected with the exercise or performance **by any public authority of any statutory power or statutory duty**” (emphasis added). In light of the severity of the interference this is clearly insufficient to comply with the requirements laid down by the European Court of Human Rights. In order to fulfil these requirements clause 46 should expressly identify those serious offences to which it applies to set the appropriate framework for the individual officer’s assessment of proportionality.

- d) limit on the duration or effect of the interference – this is of particular importance where, as here, the disclosure of a key compromises the totality of an individual’s security of communication and a notice may be subject to a requirement to keep the existence of the notice secret under clause 50;
- e) provisions for maintaining the integrity of the records and a proper audit trail for possible inspection by a judge (here possibly the Commissioner or the Tribunal) and/or the defence – this requirement is clearly not fulfilled by clause 51, entitled “safeguards”. It would be crucial for the effectiveness of these minimum standards of protection against abuse and for the (judicial) supervision offered by the Commissioner that there be a requirement that all notices are copied to the Commissioner (similar to the requirement to copy all interception warrants to the Interception Commissioner). This is not currently provided for.

21. Even if, despite these concerns, there is a possibility, however strained, of interpreting the provisions of Part III RIP in a Convention compatible manner, it seems highly inappropriate for the Government to legislate in the full knowledge that the chosen wording of a provisions would require a “departure from the natural and ordinary meaning” of its words so as to avoid a breach of Article 6 ECHR. Section 3 of the Human Rights Act was clearly envisaged to allow especially prior “repugnant” legislative provisions to be read in a Convention compliant manner and not to dissolve the Government and Parliament from legislating in a Convention compatible manner (unless the contrary intention is

expressed, e.g. through not making a section 19 statement) without the use of “repugnant” language. This is so *inter alia* because otherwise there would be:-

- a) unnecessary legal uncertainty for the individual seeking to direct his conduct in line with the law. The case of R v DPP, ex parte Kebilene is a prime example of the uncertainty created: here a strong three member Divisional Court, including the Lord Chief Justice, held that Article 6(2) had been breached but the House of Lords, accepting the “repugnancy” on its face, was able, as a result of the strength of the interpretative direction in section 3 of the Human Rights Act and by departing from the ordinary and natural meaning of the statutory words, to contemplate a “possible” interpretation which avoided a conflict with the Convention.
- b) unnecessary litigation at great expense to the public purse in that prosecutions will be brought and fought where they should not be and lengthy arguments will have to be made and heard by the courts as to the compatibility of the prosecution’s case with the requirements of Article 6(2) ECHR applying the “possible” (though strained) meaning of the words in the relevant provisions. This will inevitably expose defendants to an unnecessary risk of a violation of Article 6(2) ECHR being committed and will therefore lead to further unnecessary appeals to the Court of Appeal, the House of Lords and, possibly to the European Court of Human Rights.

Furthermore, there are limits to what is possible under section 3. The analogy of legislation which is potentially incompatible with European Community is instructive. In *Clarke v Kato* [1998] 1 WLR 1647 the House of Lords had to decide whether a car park qualified as a “road” within section 192 of the Road Traffic Act 1988, an

issue which involved consideration of three European Directives on the approximation of the laws of member states relating to insurance against civil liability in respect of the use of motor vehicles. Lord Clyde accepted that it might be “perfectly proper to adopt even a strained construction to enable the object and purpose of legislation to be fulfilled”. He continued, however, (p. 1655) that “it cannot be taken to the length of applying unnatural meanings to familiar words or of so stretching the language that its former shape is transformed into something which is not only significantly different but has a name of its own.” He considered that this “must be particularly so where the [statutory] language has no ambiguity or uncertainty about it”.

22. In its White Paper “Rights Brought Home: The Human Rights Bill”⁵, the Government, in principle, appeared to accept this need to legislate so as to ensure that the natural and ordinary meaning of future legislation is Convention compatible. In para. 3.2., having described the new procedure of a statement of compatibility made by the Minister, the White Paper goes on to set out the reasons for not making such a statement:

“There may be occasions where such a statement cannot be provided, for example because it is essential to legislate on a particular issue but the policy in question requires **a risk to be taken in relation to the Convention**, or because the arguments in relation to the Convention issues raised are not clear-cut. In such cases, the Minister will indicate that he or she cannot provide a positive statement but that the Government nevertheless wishes Parliament to proceed to consider the Bill. Parliament would expect the Minister to explain his or her reasons during the normal course of the proceedings on the Bill. This will ensure that the human rights implications are debated at the earliest opportunity.” (bold emphasis added)

23. The current scenario appears to fall within the category of cases envisaged by the above passage: there is a serious risk in relation to the Convention compliance of

these provisions and, arguably, the Convention issues raised are not clear-cut (as the case of R v DPP, ex parte Kebilene showed). Nevertheless, the Minister promoting the RIP felt able to make a statement of compatibility to both Houses of Parliament (as had been the case with the Electronic Commerce Bill) despite having been made aware of the serious concerns about the way Part III of the Bill had been drafted, *inter alia* by Justice and FIPR. This makes it the more surprising that, in its response to the recommendations of the House of Commons Select Committee on Trade and Industry, the Government appears to imply that no specific deficiencies or areas of concern to the clauses in Part III of the Draft Electronic Communications Bill had been identified⁶.

24. In line with the Government's policy as set out in the White Paper it would have been more appropriate for the Minister NOT to make such a statement and to explain the concerns (and the Minister's reply to those concerns) at the earliest opportunity in order to enable the fullest possible debate in Parliament. Section 19, requiring the making of such a statement of compatibility, has been in force since 24 November 1998 and is therefore not affected by the 2 October 2000 date.

25. In light of the fact that a section 19 declaration has been made and the specific and serious concerns raised *inter alia* in this advice, it would now appear most appropriate, and in conformity with the spirit of the Human Rights Act, for the Government to explain its thinking on compatibility and its reasons for departing from the White Paper standard on section 19 declarations. As the current Attorney

5 Presented by the Secretary of State for the Home Department, October 1997, Cm 3782

General stated in Parliament:

“Her Majesty's Government believes that a debate in Parliament provides the best forum in which the person responsible can explain his or her thinking on the compatibility of the provisions of a Bill with the Convention rights. Reasons can then be given in the context of particular concerns about particular provisions.”⁷.

Conclusion

26. For the reasons set out above, and following the experience of the Electronic Commerce Bill, and the late withdrawal of Part III from the Bill as presented to Parliament, it is disappointing that the Government has failed to address the serious concerns identified in the context of Part III of the Electronic Commerce Bill, before they introduced Part III of the RIP. As a result, it would be appropriate and desirable that the Minister explain his reasoning on compatibility to Parliament and to allow the matter to be debated, rather than merely assert that the provisions of the Bill as currently drafted comply with Convention rights (this would also be in line with the final recommendation of the Trade and Industry Select Committee). Because (a) that Part of the Human Rights Act that requires the making of a statement of compatibility (section 19) has been in force since 24 November 1998 and (b) the duty to read legislation, as far as possible, in a Convention compatible way (section 3(1)) applies to legislation “whenever enacted” (section 3(2)), it is difficult to see why there should be any benefit in human rights terms in the Regulation of Investigatory Powers Bill reaching the Statute Book before 2 October 2000. On the contrary, in light of the conclusions reached in our initial

6 [Third Special Report](#), HC 199 ,ISBN 0 10 209000 9

7 House of Lords Hansard, Written Answers, 19 May 1999, col. 35; see also House of Lords WA 10 December 1998, col 116, House of Lords WA 17 December 1998, col. 186, House of Lords WA 30 June 1999, cols 41 to 42 and the Home Office “The Human Rights Act 1998, Guidance to Departments” at para. 37

Joint Advice and above, it would appear that the provisions in this Bill would benefit from substantial reconsideration and redrafting, free from unnecessary time pressures. The significance of the interference with the rights of the individual would also suggest that these provisions warrant substantial consideration and debate by both Houses of Parliament before they reach the Statute Book.

20 March 2000

Tim Eicke
Essex Court Chambers
24 Lincoln's Inn Fields
London WC2A 3ED