

The implications and possible legal consequences of the UK Government's failure to correctly implement s5(1) of the Directive on Privacy and Electronic Communications into S1(1) of the Regulation of Investigatory Powers Act 2000 with regard to phone hacking offences

Author: Claire Bradley BA, MSc, ILEX, MA (European Law)

Abstract: This paper examines the implications of an EU Member State failing to correctly transpose an EU Directive into national law and the principles that might subsequently affect the application of national law in the light of the conflicting directive. In particular, it looks at the example of how the failure of the UK Government to transpose Directive 2002/58/EC (The Directive on Privacy and Electronic Communications) into UK law might impact upon claims made regarding the unlawful interception of communications under s1(1) and s1(2) of The Regulation of Investigatory Powers Act 2000 (RIPA). It looks at the regulatory framework established by RIPA and compares this to the provisions contained in Directive 2002/58/EC, and the Data Protection Directive, and explores how the principles of harmonious interpretation of national law in the light of the wording and purpose of a directive, is likely to change the effect of that regulatory framework in both criminal and civil cases.

Disclaimer: "The information and theoretical arguments expressed in this academic paper should not be construed as formal legal advice. The author accepts no liability for any reliance made on the statements therein, and any person looking for advice or seeking to issue formal proceedings in connection with the unlawful interception of communications should seek specific legal advice from the law firm representing them as to the legal principles that are likely to apply to their individual case, under both national law and European law."

Introduction

According to Keir Starmer QC¹, the principal offences that are likely to be considered in the context of a possible prosecution of a journalist for phone hacking offences are²:

- Offences contrary to the Official Secrets Act 1989
- Misconduct in a public office
- Offences contrary to the Regulation of Investigatory Powers Act 2000
- Offences contrary to the Computer Misuse Act 1990
- Bribery, Corruption, and perverting the course of justice
- Data Protection Act 1998 offences³

The Regulation of Investigatory Powers Act 2000 (hereafter “RIPA”) is therefore one of the two key pieces of legislation in the interception of communications claims against various UK newspaper companies, the other being Directive 2002/58/EC, commonly known as the Directive on Privacy and Electronic Communications⁴.

However, it would appear that the Directive on Privacy and Electronic Communications⁵ was incorrectly transposed from EU law to national law. The aim of this paper is to examine the

¹ Keir Starmer QC ‘Statement made on behalf of: The Crown Prosecution Service Witness: Keir Starmer QC, Director of Public Prosecutions Statement No:1 Statement made 7th February 2012, p16 <http://www.levesoninquiry.org.uk/wp-content/uploads/2012/02/Witness-Statement-of-Keir-Starmer-QC.pdf>

² Keir Starmer QC ‘Statement made on behalf of: The Crown Prosecution Service Witness: Keir Starmer QC, Director of Public Prosecutions Statement No:1 Statement made 7th February 2012, p16

³ Keir Starmer QC ‘Statement made on behalf of: The Crown Prosecution Service Witness: KEIR STARMER QC, Director of Public Prosecutions Statement No:1 Statement made 7th February 2012, p16

⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)

⁵ Directive on privacy and electronic communications art 5(1)

legal implications of this failure to correctly transpose the provisions of the Directive on Privacy and Electronic Communications⁶ into UK law. In particular, the paper will be examining in what ways this is likely to affect the legal framework applicable to breaches of s 1(1) and s 1(2) of the Regulation of Investigatory Powers Act 2000.

We will start by reviewing these two main pieces of legislation in more detail.

The Regulation of Investigatory Powers Act 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000 was introduced to:

make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed.⁷

In relation to the interception of communications, the Regulation of Investigatory Powers Act 2000 is comprised of two elements; s 1(1)⁸ creates a criminal liability and s 1(2)⁹ details when a person commits the offence of intentionally and unlawfully intercepting a communication by means of a private telecommunication system. However, if one of the exemptions found in s1(6)¹⁰ are met, then this will exempt the person of criminal liability and will instead create a civil liability.

6 Directive on privacy and electronic communications
7 Long title of the Regulation of Investigatory Powers Act 2000
8 The Regulation of Investigatory Powers Act 2000 s1(1)
9 The Regulation of Investigatory Powers Act 2000 s1(2)
10 The Regulation of Investigatory Powers Act 2000 s1(6)

S1(1) of RIPA¹¹ – Criminal liability

The circumstances in which interception of a communication being transmitted by a public postal service or public telecommunication system is a criminal offence are covered in s 1(1) of RIPA¹². There is an exception for conduct with “lawful authority,” which is detailed in s 1(5)¹³.

S1(2) of RIPA¹⁴ – Civil liability

Section 1(2) of RIPA¹⁵ provides that it is an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system. However, a person is excluded from criminal liability under section 1(2) if either he is a person with a right to control the operation or the use of the system; or he has the express or implied consent of such a person to make the interception. Provided one of these exemptions are met, a breach of s1(2) of RIPA will only give rise to a civil liability.

Directive 2002/58/EC¹⁶ – The Directive on Privacy and Electronic Communications

Section 1(1) of RIPA¹⁷ was presumed to implement Article 5(1) of Directive 2002/58/EC (hereafter “the Directive on Privacy and Electronic Communications”)¹⁸. Article 5(1) of the Directive on Privacy and Electronic Communications¹⁹ states that:

11 The Regulation of Investigatory Powers Act 2000 s1(1)

12 The Regulation of Investigatory Powers Act 2000 s1(1)

13 The Regulation of Investigatory Powers Act 2000 s1(5)

14 The Regulation of Investigatory Powers Act 2000 s1(2)

15 The Regulation of Investigatory Powers Act 2000 s1(2)

16 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF>

17 The Regulation of Investigatory Powers Act 2000 s1(1)

Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services...

In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)²⁰.

A Comparison Between The Regulation of Investigatory Powers Act 2000 and the Directive on Privacy and Electronic Communications²¹

The Regulation of Investigatory Powers Act 2000 is made up of two elements; s 1(1) that creates a criminal liability and s 1 (2) which creates a civil liability (as outlined above).

According to the provisions of s 1(1) of RIPA:²²

It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—

(a) a public postal service; or

(b) a public telecommunication system.”

18 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF>

19 Directive on privacy and electronic communications

20 Directive on privacy and electronic communications art 5(1)

21 Directive on privacy and electronic communications

22 The Regulation of Investigatory Powers Act 2000 s1(1)

http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

According to the Home Office²³ Section 1(1) of RIPA²⁴ was supposed to implement Article 5(1) of the Directive on Privacy and Electronic Communications²⁵.

The key difference between RIPA²⁶ and the Directive on Privacy and Electronic Communications²⁷ is that in claims under Section 1(1) of RIPA²⁸ it has to be shown that the offence was committed intentionally, whereas under s5(1) of the Directive on Privacy and Electronic Communications²⁹ it does not – it is a strict liability offence. This means one does not have to show what the person intended, but rather just prove that they committed the offence.

Furthermore, Section 3(1) of RIPA³⁰ authorises interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has ‘reasonable grounds for believing’³¹ that consent to do so has been given. This conflicts with Article 2(h) of the Data Protection Directive³², which defines consent as “freely given, specific and informed”.

Therefore, the oft-raised argument by certain elements of the tabloid press that individuals were using the press and had therefore effectively consented to any interceptions would

23 Home Office Consultation paper: Regulation of Investigatory Powers Act 2000: Proposed amendments affecting lawful interception 2010: A consultation
<http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-amend-effect-lawful-incep?view=Binary>

24 The Regulation of Investigatory Powers Act 2000 s1(1)

25 Directive on privacy and electronic communications art 5(1)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF>

26 The Regulation of Investigatory Powers Act 2000 s1(1)

27 Directive on privacy and electronic communications art 5(1)

28 The Regulation of Investigatory Powers Act 2000 s1(1)

29 Directive on privacy and electronic communications art 5(1)

30 Regulation of Investigatory Powers Act 2000 s 3(1)

31 Regulation of Investigatory Powers Act 2000 s 3(1)

32 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

appear to be legally unsustainable under the provisions of the Directive on Privacy and Electronic Communications and the Data Protection Directive.³³

Also, Section 1(1) of RIPA³⁴ creates a criminal offence of intercepting any communication in the course of its transmission by means of a public postal service or a public telecommunication system.

By contrast, the Directive on Privacy and Electronic Communications³⁵ creates a general prohibition of *listening, tapping, storage or other kinds of interception or surveillance of communications, by means of a public communications network and publicly available electronic communications services*³⁶.

Therefore, since 31 October 2003, which was when the provisions of the Directive on Privacy and Electronic Communications³⁷ were due to be transposed into national law, UK national law on privacy of communications has conflicted with EU law.

Infringement proceedings against the UK regarding confidentiality of communications

The European Commission launched legal action against the UK on the 14th April 2009³⁸ following complaints about how the UK authorities had dealt with internet users concerns about the use of behavioural advertising (Phorm) by internet service providers.

33 Directive on privacy and electronic communications art 5(1) and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

34 Regulation of Investigatory Powers Act 2000 s 1(1)

35 Directive on privacy and electronic communications art 5(1)

36 Directive on privacy and electronic communications art 5(1)

37 Directive on privacy and electronic communications

38 European Commission press release IP/09/570: *Telecoms: Commission launches case against UK over privacy and personal data protection*, © European Union, 1995-2012

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&quiLanguage=en> Date accessed 10/11/2011

On the 30th September 2010 the European Commission referred the UK Government to the European Court of Justice³⁹, for incorrectly applying EU rules on confidentiality of communications.

Specifically, in these infringement proceedings the European Commission identified⁴⁰ three gaps in the existing UK rules governing the confidentiality of electronic communications:

▲ *There is no independent national authority to supervise interception of communications. The establishment of such an authority is required under the E-Privacy and Data Protection Directives, in particular to hear complaints regarding interception of communications*⁴¹.

▲ *The current UK law – the Regulation of Investigatory Powers Act 2000 – authorises interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has ‘reasonable grounds for believing’ that consent to do so has been given. These UK law provisions do not comply with Article 2(h) of the Data Protection Directive⁴² which defines consent as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”⁴³.*

39 European Commission document: Electronic Communications - 2002 Regulatory Framework Infringement procedures opened for incorrect implementation p20
http://ec.europa.eu/information_society/policy/ecomms/doc/implementation_enforcement/infringements/inf_proc_incorr_impl_111111.pdf Date accessed 10/11/2011

40 European Commission press release IP/09/1626: *Telecoms: Commission steps up UK legal action over privacy and personal data protection*, © European Union, 1995-2012
<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626> Date accessed 10/11/2011

41 European Commission press release IP/09/1626: *Telecoms: Commission steps up UK legal action over privacy and personal data protection*, © European Union, 1995-2012

42 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

43 European Commission press release IP/09/1626: *Telecoms: Commission steps up UK legal action over privacy and personal data protection*, © European Union, 1995-2012

^ *The Regulation of Investigatory Powers Act 2000 provisions prohibiting and providing sanctions in case of unlawful interception are limited to 'intentional' interception only, whereas EU law requires Members States to prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.*⁴⁴

On the 19 May 2011, the European Commission suspended the UK's referral to the European Court of Justice⁴⁵, following the UK Government's passing of the Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011.⁴⁶

The Explanatory Memorandum attached to this statutory instrument⁴⁷ confirms that RIPA⁴⁸ did not correctly implement both Article 5(1) of the Directive on Privacy and Electronic Communications⁴⁹ and Article 2(h) of the Data Protection Directive⁵⁰ and that the aim of this Statutory Instrument is to correct these errors in drafting.

44 European Commission press release IP/09/1626: *Telecoms: Commission steps up UK legal action over privacy and personal data protection*, © European Union, 1995-2012

45 European Commission document: Electronic Communications - 2002 Regulatory Framework Infringement procedures opened for incorrect implementation p20
http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/infringements/inf_proc_incorr_impl_111111.pdf Date accessed 10/11/2011

46 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340
<http://www.legislation.gov.uk/ukxi/2011/1340/made>

47 Home Department, Explanatory Memorandum to the Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011, 2011 No. [XXXX]

48 The Regulation of Investigatory Powers Act 2000

49 Directive on privacy and electronic communications art 5(1)

50 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

So how did the Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011⁵¹ give effect to the incorrectly implemented provisions of the Directive on Privacy and Electronic Communications⁵²?

According to the Explanatory Memorandum attached to SI 2011/1340⁵³, the Directive on Privacy and Electronic Communications⁵⁴ was introduced as part of the Regulatory Framework for Electronic Communications⁵⁵ to ensure proper protection for individuals and businesses in the arena of electronic communications, networks, and services.

The main vehicle for transposing the Directive on Privacy and Electronic Communications into UK law was the Privacy and Electronic Communications (EC Directive) Regulations 2003⁵⁶, although some of the measures contained within the Directive were already provided for in existing UK legislation.

An example of this is the offence of unlawful interception contained in s1(1) of RIPA⁵⁷.

As mentioned above, the original transposition of the Directive on Privacy and Electronic Communications⁵⁸ was completed in 2003. In April 2009 the European Commission issued a letter of formal notice (Article 226) setting out its view that the UK had not properly

51 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

52 Directive on privacy and electronic communications art 5(1)

53 Home Department, Explanatory Memorandum to the Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011, 2011 No. [XXXX]

54 Directive on privacy and electronic communications

55 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") OJ L108 33

56 Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426

57 The Regulation of Investigatory Powers Act 2000 s1(1)

58 Directive on privacy and electronic communications

transposed Article 5(1) of the Directive on Privacy and Electronic Communications⁵⁹ and Articles 2(h), 24 and 28 of the Data Protection Directive 1998⁶⁰.

As already noted above, the European Commission identified three areas of defective transposition:

(1) By limiting the offence in section 1(1) of RIPA⁶¹ to intentional interception, the UK had failed to create a sanction for **all** unlawful interception as required by Article 5(1) of the Directive on Privacy and Electronic Communications⁶² and Article 24 of the Data Protection Directive⁶³.

(2) The UK had failed to create an independent authority responsible for the supervision of all interception activities as required by Article 28 of the Data Protection Directive⁶⁴.

(3) The UK had wrongly made it lawful to intercept a communication where the interceptor has a 'reasonable belief'⁶⁵ in the other party's consent to the interception. Pursuant to Article 5(1) of the Directive on Privacy and Electronic Communications⁶⁶ and 2(h) of the Data

59 Directive on privacy and electronic communications art 5(1)

60 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h), 24 and 28

61 Regulation of Investigatory Powers Act 2000 s1(1)

62 Directive on privacy and electronic communications art 5(1)

63 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 24

64 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 28

65 Regulation of Investigatory Powers Act 2000 s 3(1)

66 Directive on privacy and electronic communications art 5(1)

Protection Directive⁶⁷, consent to interception should be ‘freely given, specific and informed’⁶⁸.

According to the Explanatory Memorandum attached to SI 2011/1340⁶⁹ the Government has conceded the defective transposition identified in points (1) and (3) above. This statutory instrument addresses the deficiencies by:

(a) introducing into RIPA⁷⁰ a sanction for “unintentional” unlawful interception to sit alongside the existing offence of intentional unlawful interception currently found in section 1(1) of the Regulation of Investigatory Powers Act 2000; and

(b) amending section 3(1) of the Regulation of Investigatory Powers Act 2000 by removing the existing qualification that interception of a communication may be authorised where there are, “reasonable grounds for believing” that a person has consented to the interception.

The Government has not conceded the alleged defective transposition identified at point (2) above.

Therefore, the net effect of SI 2011/1340⁷¹ is that

- It amends RIPA⁷² with a view to correctly implementing the provisions of the Directive on Privacy and Electronic Communications⁷³.

67 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

68 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

69 Home Department, Explanatory Memorandum to the Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011, 2011 No. [XXXX]

70 Regulation of Investigatory Powers Act 2000 s1(1A)

71 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

72 Regulation of Investigatory Powers Act 2000

73 Directive on Privacy and Electronic Communications 2003 art 5(1)

- It maintains the existing criminal offence found under Section 1(1) of RIPA⁷⁴, but it abolishes the defence of implied consent formerly found under section 3(1) of RIPA.⁷⁵

Therefore under the provisions of SI 2011/1340⁷⁶, consent to an interception has to be expressly given in order for it to be lawful, and you can no longer raise as a defence that you believed you had reasonable grounds for believing that the person affected had consented to you intercepting their communications.

- SI 2011/1340⁷⁷ creates a new civil liability, which is inserted after Section 1(1) of RIPA⁷⁸. Accordingly, Section 1(1A) of the Regulation of Investigatory Powers Act 2000 (as amended) states that:

the Interception of Communications Commissioner may serve a monetary penalty notice on a person if the Commissioner—

(a) considers that the person—

(i) has without lawful authority intercepted, at any place in the United Kingdom, any communication in the course of its transmission by means of a public telecommunication system, and

(ii) was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception concerned, and

74 Regulation of Investigatory Powers Act 2000 s1(1)

75 Regulation of Investigatory Powers Act 2000 s 3(1)

76 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

77 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

78 Regulation of Investigatory Powers Act 2000 (as amended) s1(1A)

(b) does not consider that the person has committed an offence under Section 1(1) of the Regulation of Investigatory Powers Act 2000⁷⁹.

So effectively, the new civil liability found under Section 1(1A) of RIPA⁸⁰ abolishes the requirement to show intent and requires the person to have expressly consented to the interception. Therefore, with regard to civil liability, the Regulation of Investigatory Powers Act 2000 (as amended) now appears to correctly implement the provisions of the Directive on Privacy and Electronic Communications⁸¹.

- However, it is arguable that section 1(1) of RIPA⁸², which deals with criminal liability, still conflicts with the provisions of the Directive on Privacy and Electronic Communications in that it still imposes a requirement that you have to show intent, whereas the Directive imposes no such requirement.

79 Regulation of Investigatory Powers Act 2000 (as amended) s1(1A)

80 Regulation of Investigatory Powers Act 2000 (as amended) s1(1A)

81 Directive on Privacy and Electronic Communications 2003

82 Regulation of Investigatory Powers Act 2000 s1(1)

Direct effect and indirect effect; how EU law gives effect to directives which have not been correctly implemented into national law.

Under EU law, there is a principle called direct effect, which may be broadly defined as ‘the provisions of binding EU law which are sufficiently clear, precise and unconditional to be considered justiciable can be invoked and relied on by individuals before national courts⁸³’, or more narrowly, as ‘the capacity of a provision of Union law to confer rights on individuals’.⁸⁴

The ECJ has found in general that all EU law may have direct effect, provided

- (i) it is sufficiently clear, precise and unconditional in its wording
- (ii) Any time limits for implementing the directive have expired and
- (iii) It is claimed by and against the relevant addressees.

However, in the case of *Marshall*⁸⁵, the ECJ held that the ‘direct effect of a directive could not be pleaded against an individual but only against a Member State’⁸⁶. Therefore, directives have only vertical and not horizontal direct effect.

However, to counter the limiting effect of *Marshall*⁸⁷ the ECJ has encouraged the application and effectiveness of directives by developing the principle of harmonious interpretation (indirect effect). This requires national law to be interpreted “in the light of the wording and

⁸³ P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) 180

⁸⁴ P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) 180

⁸⁵ Case 152/84 *Marshall v Southampton and South West Hampshire Area Health Authority (teaching)* [1986] ECR 723

⁸⁶ P Craig and G de Búrca, *EU Law Text, Cases and Materials* (4th edition, OUP) 282

⁸⁷ Case 152/84 *Marshall v Southampton and South West Hampshire Area Health Authority (teaching)* [1986] ECR 723

purpose of the directive⁸⁸”. By this, the ECJ has tried to ensure that directives would be given some effect even where they had not been properly implemented.

The *Von Colson* case is the leading authority on this issue.⁸⁹ In this case, it was held by the ECJ that “national courts are required to interpret their national law in the light of the wording and the purpose of the directive⁹⁰”. Furthermore, the *Marleasing* case⁹¹ established that national courts are obliged to interpret national law in the light of an inadequately implemented or non-implemented directive even in cases between individuals.

According to Craig and de Búrca:⁹²

The case of *Marleasing*⁹³ also clarified that the obligation of harmonious interpretation applies even in a case where the national law predates the directive, and has no specific connection with the directive. In *Marleasing* there was no domestic implementing legislation which could be interpreted in the light of the directive but only domestic law which pre-dated the Directive and was not designed to implement it.

The same principle could be applied to the Regulation of Investigatory Powers Act 2000. RIPA⁹⁴ predates the Directive on Privacy and Electronic Communications⁹⁵, as it came out in 2000, whereas the Directive on Privacy and Electronic Communications⁹⁶ came into force in October 2003.

88 C-14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891 art 26

89 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

90 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891 art 26

91 C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR 1-4135

92 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p202

93 C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR 1-4135

94 The Regulation of Investigatory Powers Act 2000

95 Directive on Privacy and Electronic Communications 2003

96 Directive on Privacy and Electronic Communications 2003

Whilst s1(1) of RIPA⁹⁷ was presumed (according to the Home Office⁹⁸) as implementing s5(1) of the Directive on Privacy and Electronic Communications⁹⁹, there is no mention of the Directive on Privacy and Electronic Communications¹⁰⁰ in RIPA¹⁰¹, and the other provisions of Directive 2002/58/EC¹⁰² were implemented using the Privacy and Electronic Communications (EC Directive) Regulations 2003.¹⁰³

In *Pfeiffer*¹⁰⁴, the ECJ confirmed the point made in *Marleasing*¹⁰⁵ and ruled that the obligation of interpretation applies to the national legal system as a whole and not only to specific legislation.

Therefore, to summarize, the general legal position would appear to be that:

- ▲ RIPA¹⁰⁶ is a key statute in the pending cases on phone hacking by certain members of the press.
- ▲ S1(1) of RIPA¹⁰⁷ was supposed to implement s5(1) of the Directive on Privacy and Electronic Communications,¹⁰⁸ which prohibits *listening, tapping, storage or other kinds of interception or surveillance of communications ...by persons other than users, without the consent of the users concerned.*

97 The Regulation of Investigatory Powers Act 2000 s1(1)

98 Home Office Consultation paper: Regulation of Investigatory Powers Act 2000: Proposed amendments effecting lawful interception 2010: A consultation

99 Directive on Privacy and Electronic Communications 2003

100 Directive on Privacy and Electronic Communications 2003

101 The Regulation of Investigatory Powers Act 2000

102 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF>

103 The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2003 No. 2426
<http://www.legislation.gov.uk/ukSI/2003/2426/contents/made>

104 Joined Cases C-397/01 to C-403/01 *Bernhard Pfeiffer and Others v Deutsches Rotes Kreuz, Kreisverband Waldshut eV* ECR I-8835

105 C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR I-4135

106 The Regulation of Investigatory Powers Act 2000

107 The Regulation of Investigatory Powers Act 2000

108 Directive on Privacy and Electronic Communications 2003 art 5(1)

- ⌘ The Regulation of Investigatory Powers Act 2000 specifies that the interception must be made intentionally. Under the provisions of the Directive on Privacy and Electronic Communications¹⁰⁹, there is no such requirement – it is a strict liability offence, and there is no requirement to show that the offence was committed intentionally, merely that it was committed.
- ⌘ RIPA¹¹⁰ also had a defence that the interception of a communication was lawful if the person who intercepted a communication had ‘reasonable grounds for believing¹¹¹, that consent to do so has been given. These UK law provisions did not comply with Article 2(h) of the Data Protection Directive¹¹² that defines consent as “*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*”. Statutory instrument 2011/1340¹¹³ has now removed the defence of implied consent, and also introduced into RIPA¹¹⁴ a sanction for ‘unintentional unlawful interception’¹¹⁵ broadly consistent with Article 5(1) of the Directive on Privacy and Electronic Communications¹¹⁶.
- ⌘ EU law has supremacy over national law.¹¹⁷

109 Directive on Privacy and Electronic Communications 2003 art 5(1)

110 The Regulation of Investigatory Powers Act 2000

111 Regulation of Investigatory Powers Act 2000 art 3(1)

112 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

113 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

114 Regulation of Investigatory Powers Act 2000

115 Regulation of Investigatory Powers Act 2000 (as amended) s1(1A)

116 Directive on Privacy and Electronic Communications 2003 art 5(1)

117 See Case C-6/64 *Flaminio Costa v ENEL* [1964] ECR 585,593, Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* [1978] ECR 629

- ⤴ Where a directive has not been correctly implemented a national court is required to interpret a case before it which concerns an incorrectly implemented directive in the “light of the wording and purpose of the directive¹¹⁸”.
- ⤴ Where a directive is transposed belatedly into a Member State’s domestic law (as is the case here with Directive 2002/58/EC¹¹⁹) the national courts are bound to interpret domestic law so far as possible, once the period for transposition has expired,
 - ⤴ in the light of the wording and the purpose of the directive concerned
 - ⤴ with a view to achieving the results sought by the directive,
 - ⤴ favouring the interpretation of the national rules which is the most consistent with that purpose
 - ⤴ in order thereby to achieve an outcome compatible with the provisions of the directive.¹²⁰

Application

In *Simmenthal*¹²¹ the ECJ made clear that a Community measure rendered inapplicable any conflicting national law. It also held that:

A national court which is called upon, within the limits of its jurisdiction, to apply provisions of Community law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting

118 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

119 Directive on Privacy and Electronic Communications 2003 art 5(1) read in the light of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data art 2(h), 24 and 28 OJ L 281

120 Case C-212/04 *Konstantinos Adeneler and Others v Ellinikos Organismos Galaktos (ELOG)* [2006] ECR I-6057

121 Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* [1978] ECR 629

provision of national legislation, even if adopted subsequently, and it is not necessary for the court to request or await the prior setting aside of such provisions by legislative or other constitutional means.”

Therefore, the cases of *Von Colson*,¹²² *Marleasing*¹²³ and *Adeneler*¹²⁴ support the view that any national law judge who is dealing with a case of unlawful interception of communications under either s1(1) or s1(2) of RIPA¹²⁵, will be under a duty to interpret cases of unlawful interception of communications which took place between 31 October 2003 (which was the transposition date of the Directive on Privacy and Electronic Communications) and the 15 June 2011 (which was the day before SI 2011/1340¹²⁶ came into force) ‘in the light of the wording and purpose’¹²⁷ of the directive¹²⁸.

Furthermore, according to Craig and De Burca,¹²⁹ the *Simmenthal* principle does not require the national court to invalidate or annul the provision of national law that conflicts with EC law, but rather refuse to apply it.

On that basis, for cases where the unlawful interception of communications took place between 31 October 2003 and 15 May 2011, a national law judge could refuse to apply the offending parts of RIPA¹³⁰ on the basis that they conflict with Article 5(1) of the Directive on Privacy and Electronic Communications, and Article 2(h) of the Data Protection Directive¹³¹.

122 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

123 Case C 106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR I-4135

124 Case C-212/04 *Konstantinos Adeneler and Others v Ellinikos Organismos Galaktos (ELOG)* [2006] ECR I-6057

125 The Regulation of Investigatory Powers Act 2000

126 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

127 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

128 Directive on Privacy and Electronic Communications 2003

129 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p 263

130 The Regulation of Investigatory Powers Act 2000

131 Directive on Privacy and Electronic Communications 2003 art 5(1) read in the light of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of

However, different rules apply depending on whether the case is dealing with an issue of civil liability or an issue of potential criminal liability and these will be examined in more detail below.

individuals with regard to the processing of personal data and on the free movement of such data
art 2(h), 24 and 28 OJ L 281

© Claire Bradley. Reproduction of any part of this text is not authorised except with the author's permission.

CIVIL CASES**Possible implications of the application of the principle of harmonious interpretation in relation to civil cases of interception of communications without lawful authority (under s1(2) of RIPA¹³²)**

It is worth remembering that the obligation of harmonious interpretation applies to all national law, and not only to national law implementing a directive.¹³³ So s1(1) of RIPA¹³⁴ was supposed to implement s5(1) of the Directive on Privacy and Electronic Communications¹³⁵. However, s1(2) of RIPA¹³⁶ also conflicts with the provisions of the Directive on Privacy and Electronic Communications¹³⁷ and the Data Protection Directive¹³⁸ on the issues of intent and consent.

In civil cases a national court judge would be under an obligation of harmonious interpretation to ensure that s1(2) of RIPA¹³⁹ was interpreted in the light of the wording and purpose of both the Directive on Privacy and Electronic Communications¹⁴⁰ and the Data Protection Directive¹⁴¹, possibly by striking out the offending provisions as follows:

132 The Regulation of Investigatory Powers Act 2000

133 Case C 106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR I-4135

134 The Regulation of Investigatory Powers Act 2000

135 Directive on Privacy and Electronic Communications 2003 art 5(1)

136 The Regulation of Investigatory Powers Act 2000

137 Directive on Privacy and Electronic Communications 2003 art 5(1)

138 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

139 The Regulation of Investigatory Powers Act 2000

140 Directive on Privacy and Electronic Communications 2003 art 5(1)

141 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data art 2(h), 24 and 28 OJ L 281

S1(2) It shall be an offence for a person—

(a) ~~intentionally and~~ without lawful authority, and.

(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,.

to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.

S1(6) The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if—

(a) he is a person with a right to control the operation or the use of the system; or

(b) he has the express ~~or implied~~ consent of such a person to make the interception.

Whilst a judge may refuse to apply offending provisions of national law to bring the national law provisions in line with the wording and purpose of the Directive (known as the exclusionary effect¹⁴²) they may not normally substitute provisions directly from the Directive into national law (substitution effect¹⁴³). However, in this case the offending provisions can be removed or dis-applied without any need for substitution so the issue should not arise.

However, as a general principle, the methodology that a national law judge uses to discharge its duty of harmonious interpretation lies with the judge alone.

142 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p206

143 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p206

CRIMINAL CASES OF UNLAWFUL INTERCEPTION OF COMMUNICATIONS

General principles applying to the principle of harmonious interpretation in relation to criminal cases of interception of communications without lawful authority (under s1(1) of RIPA¹⁴⁴)

S1(1) of RIPA¹⁴⁵ imposes a criminal liability, and was supposed to implement Article 5(1) of the Directive on Privacy and Electronic Communications¹⁴⁶ which prohibits:

listening, tapping, storage or other kinds of interception or surveillance of communications ...by persons other than users, without the consent of the users concerned.¹⁴⁷

In relation to criminal law matters, there are limitations on the ability of the courts to interpret national law provisions in the light of a directive. The case of *Arcaro*¹⁴⁸ summarises the position:

“...in applying national law, the national court called upon to interpret a directive is required to do so, as far as possible, in the light of the wording and purpose of the directive in order to achieve the result pursued by the directive and thereby comply with the third paragraph of Article 189 of the Treaty.

However, that obligation of the national court to refer to the content of the directive when interpreting the relevant rules of its national law reaches a limit where such an interpretation leads to

144 The Regulation of Investigatory Powers Act 2000 s1(1)

145 The Regulation of Investigatory Powers Act 2000 s1(1)

146 Directive on Privacy and Electronic Communications 2003 art 5(1)

147 Directive on Privacy and Electronic Communications 2003 art 5(1)

148 Case C-168/95 *Luciano Arcaro* [1996] ECR I-4705

- *the imposition on an individual of an obligation laid down by a directive which has not been transposed or, more especially,*

- *where it has the effect of determining or aggravating, on the basis of the directive and in the absence of a law enacted for its implementation, the liability in criminal law of persons who act in contravention of that directive's provisions.*

Whilst it is reasonable for an individual not to be subject to an obligation laid down by a directive which has not been transposed into national law, especially where it has the effect of determining or aggravating a criminal liability, it is questionable whether that has happened here.

The obligation under RIPA¹⁴⁹ and the Directive on Privacy and Electronic Communications¹⁵⁰ is essentially the same i.e. a person is not allowed to unlawfully intercept communications. The Regulation of Investigatory Powers Act 2000 has added elements that are not found in the Directive¹⁵¹, namely it has added that intent is required. RIPA¹⁵² has also added a defence under Article 3(1) of permitting the interception of communications if one had “reasonable grounds for believing¹⁵³” consent had been given.

Therefore, the obligations on an individual in relation to unlawful interception are coming from both the directive and the national law provisions, but the offending parts of the national

149 The Regulation of Investigatory Powers Act 2000 s1(1)

150 Directive on Privacy and Electronic Communications 2003 art 5(1)

151 Directive on Privacy and Electronic Communications 2003

152 The Regulation of Investigatory Powers Act 2000 s1(1)

153 Regulation of Investigatory Powers Act 2000 art 3(1)

legislation are adding elements that are not to found in the parent directive, and therefore they could arguably be removed without changing the obligations on the parties.

The question here is, does removing the offending provisions found in RIPA¹⁵⁴ have the effect the of “*determining or aggravating, on the basis of the directive and in the absence of a law enacted for its implementation, the liability in criminal law of persons who act in contravention of that Directive’s*”¹⁵⁵ provisions?

It is arguable that it does not. It is not the directive¹⁵⁶ that has the effect of determining or aggravating liability in criminal law of persons who act in contravention of that directive’s¹⁵⁷ provisions. Section 1(1) of RIPA¹⁵⁸ clearly enacts the obligation to not unlawfully intercept communications, in line with Article 5(1) of the Directive on Privacy and Electronic Communications 2003.

Alternatively, one could argue that striking out the added elements in the Regulation of Investigatory Powers Act 2000, (particularly on the issue of intent), has the effect of creating a legal disadvantage for the defendant by reducing the burden of proof required.

According to Craig and de Burca¹⁵⁹, the *Arcaro* judgement seems to suggest that:

Where an interpretation of national law in the light of a directive amounted to ‘the imposition on an individual of an obligation laid down by the directive’¹⁶⁰ it went too far and is neither permitted nor required by EU law... This implies that a distinction has to be made between the ‘imposition

154 The Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

155 Directive on Privacy and Electronic Communications 2003 art 5(1)

156 Directive on Privacy and Electronic Communications 2003

157 Directive on Privacy and Electronic Communications 2003 art 5(1)

158 The Regulation of Investigatory Powers Act 2000 s1(1)

159 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p205

160 P Craig, ‘Directives: Direct effect, Indirect Effect and the Construction of National Legislation’ (1997) 22 ELRev 519

of an obligation' on an individual, which is not permitted, and the creation of other kinds of legal disadvantage or detriment for that party falling short of a legal obligation, which is permitted.¹⁶¹

However, the ECJ appears to have subsequently developed a more nuanced view of the position. In the case of *Kofoed*¹⁶² the ECJ held:

Although it is true that the requirement of a directive compliant interpretation cannot reach the point where a directive, by itself and without national implementing legislation, may create obligations for individuals or determine or aggravate the liability in criminal law of persons who act in contravention of its provisions, a Member State may nevertheless, in principle, impose a directive-compliant interpretation of national law on individuals (see, to that effect, Kolpinghuis Nijmegen, paragraphs 12 to 14, and Arcavo, paragraphs 41 and 42)¹⁶³.

...it is therefore for the national court to ascertain whether there is, in (national) law, a provision or general principle prohibiting (abuse of rights or other provisions on tax evasion or tax avoidance which might be interpreted in accordance with Article 11(1)(a) of Directive 90/434) and thereby justify taxation of the exchange of shares in question (see also Case 8/81 Becker [1982] ECR 53, paragraph 34)¹⁶⁴.

161 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p205

162 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007)

163 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007) [45]

164 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007) [46]

*If so, it will be for the national court to determine whether the conditions for the application of those national provisions are satisfied in the main proceedings*¹⁶⁵.

*Kofoed*¹⁶⁶ upholds the principle found in *Arcaro*¹⁶⁷ but would appear to go on and suggest that if there is in national law, a provision or general principle prohibiting the unlawful interception of communications, which might be interpreted in accordance with Article 5(1) of the Directive on Privacy and Electronic Communications¹⁶⁸ then it would be open to the Member States (in principle) to impose a directive compliant interpretation of national law on individuals.

So is the Regulation of Investigatory Powers Act 2000 capable of being interpreted in a directive compliant way? Arguably it is. As in the civil cases outlined above, RIPA¹⁶⁹ could be interpreted in the light of the Directives¹⁷⁰ by striking out the offending parts of the Act¹⁷¹, which could then read as follows:

s1(1) It shall be an offence for a person (~~intentionally~~) without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—

(a) a public postal service; or

(b) a public telecommunication system.”

165 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007) [47]

166 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007)

167 Case C-168/95 *Luciano Arcaro* [1996] ECR I-4705

168 Directive on Privacy and Electronic Communications 2003

169 Regulation of Investigatory Powers Act 2000

170 Directive on Privacy and Electronic Communications 2003 art 5(1) and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h), 24 and 28.

171 Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

s3 (1) Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which, ~~or which that person has reasonable grounds for believing~~ is both

(a) a communication sent by a person who has consented to the interception;
and.

(b) a communication the intended recipient of which has so consented.”

One of the key consequences of interpreting s1(1) and s3(1) in this directive compliant way is that this would have the effect of changing the offence of unlawful interception currently found in s1 (1) of RIPA¹⁷² to a strict liability offence. It is potentially easier to find companies and individuals criminally liable in the case of strict liability offences¹⁷³.

Furthermore, rather than trying to prove “directing mind”¹⁷⁴ (which is normally required for offences requiring intent), in the case of strict liability offences an option is to apply the extended or extensive construction principle of vicarious liability¹⁷⁵, although this will obviously depend on the facts of the individual case.

*Kofoed*¹⁷⁶ appears to suggest that it is a matter for the national court to determine whether the conditions for the application of those national provisions within RIPA¹⁷⁷ could be given a directive compliant interpretation. are satisfied in the main proceedings.

172 Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

173 Crown Prosecution Service, *Legal Guidance on Corporate Prosecutions* para 16 (www.cps.gov.uk, 15/11/2011) http://www.cps.gov.uk/legal/a_to_c/corporate_prosecutions/index.html accessed 15/11/2011

174 Crown Prosecution Service, *Legal Guidance on Corporate Prosecutions* para 20 (www.cps.gov.uk, 15/11/2011) http://www.cps.gov.uk/legal/a_to_c/corporate_prosecutions/index.html accessed 15/11/2011

175 Crown Prosecution Service, *Legal Guidance on Corporate Prosecutions* para 16 (www.cps.gov.uk, 15/11/2011) http://www.cps.gov.uk/legal/a_to_c/corporate_prosecutions/index.html accessed 15/11/2011

176 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007

Furthermore, if it is impossible to interpret national law in conformity with a directive, a national court would be under an obligation to dis-apply the national law provisions insofar as they are incompatible with a Directive. This principle was clarified in the recent joined cases of *Balkan and Sea Properties ADSITs and Provadinvest OOD*¹⁷⁸, which concerned issues relating to tax evasion. The companies concerned argued that the relevant national law was not compatible with Article 80(1) of the VAT Directive, and sought for that provision of European Union law to be applied directly.

The ECJ held¹⁷⁹ that:

Article 80(1) of the VAT Directive must be interpreted as conferring on companies...the right to rely on it directly to oppose the application by the referring court of provisions of national legislation that are contrary to it (see, by analogy, Flughafen Köln-Bonn, paragraph 33).

In that case, should it prove impossible to interpret the relevant provisions of (national law) in conformity with Article 80(1) of the VAT Directive, the national court would have to dis-apply those provisions insofar as they are incompatible with Article 80(1).

The principles of these cases, if applied to RIPA¹⁸⁰ would appear to suggest that if a national court was unable to interpret RIPA¹⁸¹ in conformity with s5(1) of the Directive on Privacy and Electronic Communications and the Data Protection Directive¹⁸², it would have to dis-

177 Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

178 Joined cases *Balkan and Sea Properties ADSITs* (C-621/10), *Provadinvest OOD* (C-129/11) OJ C-174/15

179 Joined cases *Balkan and Sea Properties ADSITs* (C-621/10), *Provadinvest OOD* (C-129/11) OJ C-174/15 [60]

180 Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

181 Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

182 Directive on Privacy and Electronic Communications 2003 art 5(1) and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals

apply those provisions in so far as they are incompatible with Article 5(1) of Directive 2002/58/EC¹⁸³ and Article 2(h) of Directive 95/46/EC¹⁸⁴.

Arguably, the requirement to show intent and the defence of implied consent create exemptions to the obligation to respect people's privacy that the Directive is trying to address.

In particular, RIPA¹⁸⁵ provides that in order to prove the offence under the provisions of s1(1) you have to show intent, and s3(1) also provides a defence that you are exempted from criminal liability if you had "reasonable grounds for believing" that consent had been given. These provisions have the effect of exempting natural and legal persons of their liability, as it is very difficult to prove intent in such cases. Also the defence found under s3(1) of the Regulation of Investigatory Powers Act 2000 will have the effect of exempting most natural and legal persons from criminal liability. This is probably best demonstrated by the fact that, over the last five years, (according to the Home Office)¹⁸⁶, only 8 cases have been successfully prosecuted under s1(1) of RIPA¹⁸⁷ despite the fact that the alleged interception of communications without lawful authority appears to have been widespread by certain elements of the tabloid press.

-
- with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),
- 183 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF>
- 184 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h).
- 185 The Regulation of Investigatory Powers Act 2000
- 186 Home Office Consultation paper: Regulation of Investigatory Powers Act 2000: Proposed amendments effecting lawful interception 2010: A consultation
<http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-amend-effect-lawful-incep?view=Binary> p4
- 187 The Regulation of Investigatory Powers Act 2000

The case of *Ruiz Bernaldez*¹⁸⁸ would appear to suggest that a national court judge would have the option, even in a criminal case, to exclude provisions of national law that created exemptions to the obligation that the Directive was trying to address. Arguably, the requirement under RIPA¹⁸⁹ to show intent and the defence of implied consent create exemptions to the obligation to respect people's privacy that the Directive is trying to address. Therefore, applying the principle found in *Ruiz Bernaldez*¹⁹⁰, a national court judge would appear to have the option, (even in a criminal case), to exclude the requirement for intent¹⁹¹ and the defence of implied consent found under s3(1) of RIPA, as those provisions have the effect of creating exemptions to the obligation that the Directive on Privacy and Electronic Communications was trying to address.

188 Case C129/94 *Rafael Ruiz Bernaldez* [1996] ECR I-1847

189 The Regulation of Investigatory Powers Act 2000 s1(1) and s3(1)

190 Case C129/94 *Rafael Ruiz Bernaldez* [1996] ECR I-1847

191 The Regulation of Investigatory Powers Act 2000 s1(1)

*The Ruling in Centrosteeel*¹⁹²

A third option that could be available to a national court, tasked with trying to reconcile the requirement of harmonious interpretation of national law in the light of the wording and purpose of the parent directive, bearing in mind the constraints imposed on this principle with regard to criminal law cases, would be to apply a civil liability eg damages rather than a criminal sanction.

In *Centrosteeel*¹⁹³, Advocate General Jacobs supported the view put forward in *Arcaro*¹⁹⁴, with one important caveat. He suggests that if a judge in a national court was dealing with a criminal matter, and felt as a consequence that it would push the obligation of harmonious interpretation too far to interpret national law in a criminal case in the light of the wording and purpose of a directive, particularly where this would have the effect of determining or aggravating a criminal liability, the judge would the option of imposing on an individual a civil liability or a civil obligation which would not otherwise have existed. In his Opinion¹⁹⁵ he stated that:

*In Arcaro*¹⁹⁶... the obligation of the national court to refer to the content of the directive when interpreting the relevant rules of its own national law reaches a limit where such an interpretation leads to the imposition on an individual of an obligation laid down by a directive which has not been transposed or, more especially, where it has the effect of determining or aggravating, on the basis of the directive and in the absence of a law enacted for its implementation, the liability in criminal law of persons who act in contravention of that directive's provisions.

192 Case C-456/98 *Centrosteeel v Adipol* [2000] ECR-1 6007 Opinion of AG Jacobs

193 Case C-456/98 *Centrosteeel v Adipol* [2000] ECR-1 6007 Opinion of AG Jacobs

194 Case C-168/95 *Luciano Arcaro* [1996] ECR 1-4705

195 Case C-456/98 *Centrosteeel v Adipol* [2000] ECR-1 6007 Opinion of AG Jacobs

196 Case C-168/95 *Luciano Arcaro* [1996] ECR 1-4705

That statement might appear to impose drastic limitations on the principle of interpretation of national law in accordance with Community directives. I do not consider, however, that the statement should be read in that way. It was made in the context of criminal proceedings, and the Kolpinghuis case cited by the Court also concerned criminal liability. In so far as the wording might appear to apply outside the criminal context, it is difficult to reconcile both with the Court's prior and subsequent case-law.

In summary, I am of the opinion that the Court's case-law establishes two rules: (1) a directive cannot of itself impose obligations on individuals in the absence of proper implementation in national law; (34) (2) the national courts must nevertheless interpret national law, as far as possible, in the light of the wording and purpose of relevant directives. While that process of interpretation cannot, of itself and independently of a national law implementing the directive, have the effect of determining or aggravating criminal liability, it may well lead to the imposition upon an individual of civil liability or a civil obligation which would not otherwise have existed.

Craig and de Burca¹⁹⁷ appear to take the view that *Centrosteeel*¹⁹⁸, whilst ruling out the interpretation of non-implementing national law in such a way as to aggravate or determine an individual's criminal liability, does not rule out an obligation on national courts to interpret non-implementing national law in such a way as to impose a civil liability or obligation on such an individual, which would not otherwise have existed.

197 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p205

198 Case C-456/98 *Centrosteeel v Adipol* [2000] ECR-I 6007, Opinion of AG Jacobs, supported by AG Kokott

On that basis, it would be potentially open to a national law judge to create an additional civil liability in relation to the interception of communications, without lawful authority, even if that civil obligation would not otherwise exist under UK law.

Permitted derogations from the Directive on Privacy and Electronic Communications¹⁹⁹

We will now go on to consider any derogations that could potentially be invoked, to justify the unlawful interception of communications principle, enshrined in Article 5(1).²⁰⁰ According to Article 15(1) of the Directive on Privacy and Electronic Communications:²⁰¹

Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5...of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard

- (i) national security (i.e. State security),
- (ii) defence,
- (iii) public security, and
- (iv) the prevention, investigation, detection and prosecution of criminal offences or
- (v) of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC²⁰².

199 Directive on Privacy and Electronic Communications 2003

200 Directive on Privacy and Electronic Communications 2003 art 5(1)

201 Directive on Privacy and Electronic Communications 2003 art 15(1)

202 Under s13(1) of Directive 95/46/EC, Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

What is interesting here is that there is no explicit public interest defence.

The UK government may only restrict the scope of the rights and obligations provided for in Article 5 of the Directive on Privacy and Electronic Communications²⁰³ on the grounds of national security (i.e. State security), defence, public security, and the prevention, investigation, and the detection and prosecution of criminal offences.

Article 15(1)²⁰⁴ then goes on to state that all the measures referred to Article 15(1) shall be in accordance with general principles of Community law. These general principles of Community law include those found in the Charter of Fundamental Rights of the European Union (which the UK opted out of) and the European Convention on Human Rights and Fundamental Freedoms.

-
- (b) defence;
 - (c) public security;
 - (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
 - (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
 - (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
 - (g) the protection of the data subject or of the rights and freedoms of others.

203 Directive on Privacy and Electronic Communications 2003 art 5(1)

204 Directive on Privacy and Electronic Communications 2003 art 15(1)

Conclusion

In conclusion, the general position would appear to be that:

- ⤴ RIPA²⁰⁵ is a key statute in the pending cases on phone hacking by certain members of the press.
- ⤴ S1(1) of RIPA²⁰⁶ was supposed to implement s5(1) of the Directive on Privacy and Electronic Communications,²⁰⁷ which prohibits *listening, tapping, storage or other kinds of interception or surveillance of communications ...by persons other than users, without the consent of the users concerned.*
- ⤴ The Regulation of Investigatory Powers Act 2000 specifies that the interception must be made intentionally. Under the provisions of the Directive on Privacy and Electronic Communications²⁰⁸, there is no such requirement – it is a strict liability offence, and there is no requirement to show that the offence was committed intentionally, merely that it was committed.
- ⤴ RIPA²⁰⁹ also had a defence that the interception of a communication was lawful if the person who intercepted a communication had ‘reasonable grounds for believing²¹⁰, that consent to do so has been given. These UK law provisions did not comply with Article 2(h) of the Data Protection Directive²¹¹ which defines consent as “*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*”. Statutory

205 The Regulation of Investigatory Powers Act 2000

206 The Regulation of Investigatory Powers Act 2000

207 Directive on Privacy and Electronic Communications 2003 art 5(1)

208 Directive on Privacy and Electronic Communications 2003 art 5(1)

209 The Regulation of Investigatory Powers Act 2000

210 Regulation of Investigatory Powers Act 2000 art 3(1)

211 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h)

instrument 2011/1340²¹² has now removed the defence of implied consent, and also introduced into RIPA²¹³ a sanction for ‘unintentional unlawful interception’²¹⁴ broadly consistent with Article 5(1) of the Directive on Privacy and Electronic Communications²¹⁵.

- ⌘ EU law has supremacy over national law.²¹⁶
- ⌘ Where a directive has not been correctly implemented a national court is required to interpret a case before it which concerns an incorrectly implemented directive in the “light of the wording and purpose of the directive²¹⁷”.
- ⌘ Where a directive is transposed belatedly into a Member State’s domestic law (as is the case here with Directive 2002/58/EC²¹⁸) the national courts are bound to interpret domestic law so far as possible, once the period for transposition has expired,
 - ⌘ in the light of the wording and the purpose of the directive concerned
 - ⌘ with a view to achieving the results sought by the directive,
 - ⌘ favouring the interpretation of the national rules which is the most consistent with that purpose
 - ⌘ in order thereby to achieve an outcome compatible with the provisions of the directive.²¹⁹

212 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

213 Regulation of Investigatory Powers Act 2000

214 Regulation of Investigatory Powers Act 2000 (as amended) s1(1A)

215 Directive on Privacy and Electronic Communications 2003 art 5(1)

216 See Case C-6/64 *Flaminio Costa v ENEL* [1964] ECR 585,593, Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* [1978] ECR 629

217 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

218 Directive on Privacy and Electronic Communications 2003 art 5(1) read in the light of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data art 2(h), 24 and 28 OJ L 281

Implications

Given that RIPA²²⁰ did not correctly implement the provisions of s5(1) of the Directive on Privacy and Electronic Communications²²¹ and also provisions of the Data Protection Directive²²², a number of options would appear to be available to a national law judge looking to discharge his/her duty of harmonious interpretation. It would be a matter for the judge how they interpreted and discharged this obligation to interpret RIPA²²³ ‘in the light of the wording and purpose’²²⁴ of the Directive on Privacy and Electronic Communications²²⁵ and the provisions of the Data Protection Directive²²⁶. This would potentially vary depending on whether the case concerned a civil or a criminal liability. Furthermore, there are certain key timelines that will need to be borne in mind, as different principles will apply, depending on when the offence took place.

- (i) Cases of unlawful interception of communications that took place between the 28th July 2000 (date of Royal Assent of RIPA²²⁷) and 30th October 2003 will be governed by RIPA.
- (ii) Civil cases of unlawful interception of communications, which took place between the 31 October 2003 (date by which the provisions of Directive 2002/58/EC²²⁸ were due

219 Case C-212/04 *Konstantinos Adeneler and Others v Ellinikos Organismos Galaktos (ELOG)* [2006] ECR I-6057

220 The Regulation of Investigatory Powers Act 2000

221 Directive on Privacy and Electronic Communications art 5(1)

222 Specifically, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h), 24 and 28.

223 The Regulation of Investigatory Powers Act 2000

224 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

225 Directive on Privacy and Electronic Communications

226 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h), 24 and 28.

227 The Regulation of Investigatory Powers Act 2000

228 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)

to be implemented into national law) and 15th June 2011(day before SI 2011/1340²²⁹ came into force) should be interpreted using the principle of harmonious interpretation as outlined above. For offences that occurred within this period, RIPA should be interpreted in the light of the wording and purpose of the Directive on Privacy and Electronic Communications²³⁰.

(iii) For cases of unlawful interception of communications which took place from the 16th June 2011 (which is when SI 2011/1340²³¹ came into force) to the present the situation is more nuanced. Civil cases should be interpreted in the light of SI 2011/1340,²³² as this now correctly reflects Article 5(1) of the Directive on Privacy and Electronic Communications and Article 2(h) of the Data Protection Directive.²³³

(iv) For offences of unlawful interception of communications, which fall with s1(1) of RIPA (criminal liability),²³⁴ and which took place between 31st October 2003-15th June 2011, these cases may be interpreted as outlined below.

(v) Given that s1(1) of RIPA²³⁵ is still not correctly implementing the provisions of Article 5(1)²³⁶ in that there is still a requirement to show intent, a national court could arguably still interpret s1(1) of RIPA²³⁷ ‘in the light of the wording and purpose of the

229 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

230 Directive on Privacy and Electronic Communications art 5(1) read in conjunction with the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),24 and 28.

231 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

232 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

233 Directive on Privacy and Electronic Communications art 5(1) read in conjunction with the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),24 and 28.

234 The Regulation of Investigatory Powers Act 2000

235 The Regulation of Investigatory Powers Act 2000

236 Directive on Privacy and Electronic Communications art 5(1)

237 The Regulation of Investigatory Powers Act 2000

Directive'²³⁸, within the limits of the doctrine as they apply to criminal law cases. Therefore, potentially, criminal cases of interception of communications which took place after 16th June 2011 could still be interpreted using the principle of harmonious interpretation, as summarized below.

In relation to cases being brought under an infringement of s1(1) of the Regulation of Investigatory Powers Act 2000, (which deals with criminal liability), a national court judge could

- decide that in relation to breaches of s1(1) of RIPA,²³⁹ (in particular on the issue of intent), that it would push the principle of harmonious interpretation too far to interpret RIPA²⁴⁰ in such a way that it would have the effect of *determining or aggravating, on the basis of the directive and in the absence of a law enacted for its implementation*²⁴¹, the liability in criminal law of persons who had acted in contravention of Article 5(1) of the Directive on Privacy and Electronic Communications. Depending on the facts of the case, the judge may reach the conclusion that interpreting national law in the light of a directive would have the effect of 'imposing on an individual an obligation laid down by the directive'²⁴², which is 'neither permitted nor required by EU law'²⁴³.
- If, on the other hand, the national law judge felt that the effect of applying the principle of harmonious interpretation would have the effect of creating 'a legal disadvantage or detriment for that party falling short of a legal obligation, then this

238 C- 14/83 *Von Colson and Kamann v Land Nordrhein Westfalen* [1984] ECR 1891

239 The Regulation of Investigatory Powers Act 2000

240 The Regulation of Investigatory Powers Act 2000

241 Case C-168/95 *Luciano Arcaro* [1996] ECR 1-4705

242 Case C-168/95 *Luciano Arcaro* [1996] ECR 1-4705

243 P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP) p205

could be permitted²⁴⁴. However, a request for a preliminary ruling would possibly need to be made to the European Court of Justice to clarify whether it would be appropriate to do so, depending on the facts of the case.

- Thirdly, a national court judge could adopt the more nuanced view taken by the ECJ in *Kofoed*²⁴⁵ and impose a ‘directive-compliant interpretation of national law on individuals²⁴⁶’. Furthermore, joined cases *Balkan and Sea Properties ADSIT and, Provadinvest OOD*²⁴⁷ would appear to suggest that if a national court was unable to interpret RIPA²⁴⁸ in conformity with s5(1) of the Directive on Privacy and Electronic Communications²⁴⁹, it would have to dis-apply the RIPA²⁵⁰ provisions in so far as they were incompatible with Article 5(1) of Directive 2002/58/EC²⁵¹ and Article 2(h) of Directive 95/46/EC²⁵².
- In addition, the case of *Ruiz Bernaldez*²⁵³ would appear to suggest that a national court judge would have the option to exclude provisions of national law that created exemptions to the obligations that the Directives²⁵⁴ were trying to address. With regard to the Regulation of Investigatory Powers Act 2000, these exemptions could be

244 P Craig and G de Búrca, EU Law Text, Cases and Materials (5th edition, OUP) p205

245 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007)

246 Case 321/05 *Hans Markus Kofoed v Skatteministeriet*, (Judgment of the Court (First Chamber), 5 July 2007)

247 Joined cases *Balkan and Sea Properties ADSITs* (C-621/10), *Provadinvest OOD* (C-129/11) OJ C-174/15

248 The Regulation of Investigatory Powers Act 2000

249 Directive on Privacy and Electronic Communications 2003 art 5(1)

250 Regulation of Investigatory Powers Act 2000

251 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 art 5(1) (Directive on privacy and electronic communications)

252 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h), 24 and 28.

253 Case C129/94 *Rafael Ruiz Bernaldez* [1996] ECR I-1847

254 Directive on Privacy and Electronic Communications 2003 art 5(1) and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h), 24 and 28.

construed as including the requirement for intent and the defence found under s3(1) of the Act, which taken together have the effect of exempting most natural and legal persons from criminal liability.

- The final option for a national law judge could be to strike out the offending provisions of s1(1) of the Regulation of Investigatory Powers Act 2000, and then impose a civil liability, ie damages rather than a fine, in line with the decision in *Centrosteeel*²⁵⁵. It is perhaps worth noting that under the revised rules relating to interception, found in SI 2011/1340²⁵⁶, which aims to implement the provisions of the Directive on Privacy and Electronic Communications²⁵⁷, a fine of £50,000 may be payable for each offence of a person intercepting communications without lawful authority.
- In relation to the civil claims being brought under s1(2) of the Regulation of Investigatory Powers Act 2000, the same process of striking out the offending provisions could occur, given that in civil claims a national court judge is under a duty to apply the principle of harmonious interpretation, and the constraints that apply to criminal cases are not present in relation to civil claims.

In this paper we have examined various possible options that could be considered, but ultimately the decision on how best to discharge this obligation rests purely with the national law judge.

255 Case C-456/98 *Centrosteeel v Adipol* [2000] ECR-I 6007, Opinion of AG Jacobs

256 The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 SI 2011/1340

257 Directive on Privacy and Electronic Communications 2003 art 5(1)

The net effect of the UK government's failure to correctly implement s5(1) of Directive 2002/58/EC and the provisions of the Data Protection Directive²⁵⁸ is that under European law, the legal framework for dealing with unlawful interception of communications claims is arguably different to that hitherto presumed. The requirement, laid in down RIPA²⁵⁹, to show intent is removed, as is the defence that the person intercepting the communication believed they had implied consent to do so. This would appear to suggest that under EU law, phone tapping could be construed as being a strict liability offence, which would also change the legal principles that apply to corporate liability in such cases.

Furthermore, in module 4 of the Leveson Inquiry, the Inquiry will hear proposals for potential press regulatory solutions. Specifically, the Inquiry will be examining

- 1) what a regulatory regime should do;
- 2) how it should be structured to achieve that; and
- 3) the detailed rules that are put in

The correct application of Article 5(1) of the Directive on Privacy and Electronic Communications²⁶⁰ using the legal mechanisms outlined above, would appear to strike a balance between respecting the freedom of the press whilst at the same time enforcing peoples' right to keep their communications private. There has already been some debate on whether the UK needs a privacy law, to protect individuals from having their communications unlawfully intercepted without their consent. The reality is that it already exists – Directive

258 Directive on Privacy and Electronic Communications 2003 art 5(1) and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),24 and 28.

259 Regulation of Investigatory Powers Act 2000

260 Directive on Privacy and Electronic Communications 2003 art 5(1)

2002/58/EC. There is no public interest defence under Directive 2002/58/EC²⁶¹, just a general prohibition against:

listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).

Therefore, under the provisions of the Directive on Privacy and Electronic Communications²⁶², in order to bring a successful claim, all a person needs to show is that their communications have been intercepted without their consent. There is no requirement to show intent, and nor can someone raise as a defence that they had the implied consent of the victim/claimant to do so.

The Directive on Privacy and Electronic Communications²⁶³ would appear to strike an effective balance between respecting people's right to privacy without hindering the right to freedom of expression that a free press must enjoy in a democracy.

Given the problems of implementation that have occurred, the rights and obligations found under Article 5(1) of the Directive on Privacy and Electronic Communications²⁶⁴ and the Data Protection Directive²⁶⁵ will be given effect by the national courts applying the principle of

²⁶¹ Directive on Privacy and Electronic Communications 2003 art 5(1)

²⁶² Directive on Privacy and Electronic Communications 2003 art 5(1) read in conjunction with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),24 and 28.

²⁶³ Directive on Privacy and Electronic Communications 2003 art 5(1) read in conjunction with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),24 and 28.

²⁶⁴ Directive on Privacy and Electronic Communications 2003 art 5(1)

²⁶⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 2(h),24 and 28.

harmonious interpretation, within the parameters and constraints imposed on them under European law.

Statement of Truth

I believe the facts stated in this witness statement are true.

Signed

-

Date 11/07/2012

Bibliography

Legislation

UK Legislation

Acts

The Regulation of Investigatory Powers Act 2000

Statutory Instruments

- Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426
- The Electronic Communications Postal Services - The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011
SI 2011/1340 <http://www.legislation.gov.uk/ukxi/2011/1340/made>

EU Law

- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (“Framework Directive”) OJ L108 33
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector OJ L201/37 (Directive on privacy and electronic communications)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281

EU Cases

C-14/83 Von Colson and Kamann v Land Nordrhein Westfalen [1984] ECR 1891 art 26 C-106/89

Marleasing SA v La Comercial Internacional de Alimentacion SA [1990] ECR I-4135
Joined Cases

C-397/01 to C-403/01 Bernhard Pfeiffer and Others v Deutsches Rotes Kreuz, Kreisverband Waldshut eV ECR I-8835

Case C-6/64 Flaminio Costa v ENEL [1964] ECR 585,593,

Case 106/77 Amministrazione delle Finanze dello Stato v Simmenthal SpA [1978] ECR 629

Case C-212/04 Konstantinos Adeneler and Others v Ellinikos Organismos Galaktos (ELOG) [2006] ECR I-6057

Case C-168/95 Luciano Arcaro [1996] ECR I-4705

Case 321/05 Hans Markus Kofoed v Skatteministeriet, (Judgment of the Court (First Chamber), 5 July 2007)

Joined cases Balkan and Sea Properties ADSITs (C-621/10), Provadinvest OOD (C-129/11) OJ C-174/15

Case C129/94 Rafael Ruiz Bernaldez [1996] ECR I-1847

Case C-456/98 Centrosteeel v Adipol [2000] ECR-I 6007 Opinion of AG Jacobs

Government publications

Keir Starmer QC 'Statement made on behalf of: The Crown Prosecution Service Witness: Keir Starmer QC, Director of Public Prosecutions Statement No:1 Statement made 7th February 2012, p16

Home Office Consultation paper: Regulation of Investigatory Powers Act 2000: Proposed amendments affecting lawful interception 2010: A consultation
<http://www.homeoffice.gov.uk/publications/consultations/ripa-effect-lawful-intercep/ripa-amend-effect-lawful-incep?view=Binary>

Crown Prosecution Service, Legal Guidance on Corporate Prosecutions para 16
(www.cps.gov.uk , 15/11/2011) http://www.cps.gov.uk/legal/a_to_c/corporate_prosecutions/index.html
accessed 15/11/2011

European Commission publications

European Commission press release IP/09/570: Telecoms: Commission launches case against UK over privacy and personal data protection, © European Union, 1995-2012

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en> Date accessed 10/11/2011

European Commission press release IP/09/1626: Telecoms: Commission steps up UK legal action over privacy and personal data protection, © European Union, 1995-2012

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626> Date accessed 10/11/2011

European Commission document: Electronic Communications - 2002 Regulatory Framework Infringement procedures opened for incorrect implementation p20

http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/infringements/inf_proc_incorr_impl_111111.pdf Date accessed 10/11/2011

Books

P Craig and G de Búrca, *EU Law Text, Cases and Materials* (4th edition, OUP) 282

P Craig and G de Búrca, *EU Law Text, Cases and Materials* (5th edition, OUP)

180,202,205,206,263

Articles

P Craig, 'Directives: Direct effect, Indirect Effect and the Construction of National Legislation

(1997) 22 ELRev 519