A Question of Trust: Legal professional privilege in the spotlight once more

JULY 13, 2015

Introduction

"*A Question of Trust*", David Anderson QC's recently published report on the legislative framework that governs the interception of, and collection of information about, communications by public authorities in the UK (the "**Report**") reaffirmed the substantive importance of the legally privileged nature of communications between a client and his lawyer.

In doing so, the Report raised two important questions that provide the focus of this article:

- How absolute is the protection afforded by legal professional privilege ("**LPP**") for a client to consult with his lawyer in confidence?
- How do you build a legislative framework that is sufficiently robust to reconcile the tension between LPP—a concept described as forming the "*cornerstone of a society governed by the rule of law*"[1]—and the need to detect and prevent increasingly real and sophisticated criminality and threats to public safety?

A confidential consultation

The ability of a defendant to be able to consult with his lawyer in confidence, without fear that the facts may afterwards be disclosed and used to his prejudice, is a fundamental human right long established at common law in the UK.[2]

The consequences of a defendant being reluctant to speak openly with his lawyer are potentially devastating. Without the full facts, counsel may not be aware of all the defences available to defeat an allegation, resulting in perfectly proper defences not being put forward at trial. This goes to the heart of the criminal justice system. Only those who are guilty should be convicted: not those for whom a sound defence could not be advanced at trial because a defendant was too afraid to share the full facts with his lawyer for fear of eavesdropping.

The right of a detainee to consult with his lawyer in private is also explicitly provided for by section 58(1) of the Police and Criminal Evidence Act 1984 ("**PACE**"). The importance of this statutory right was shown by the decision of the Court of Appeal in *R v Grant*[3]. In *Grant*, the police eavesdropped

on conversations between Grant and his lawyers and the court held that this called for a stay of the proceedings on the ground of abuse of process, even without proof of any prejudice to the defendant. As we shall see below in *Re McE*[4] however, section 58(1) is not an absolute right, it is capable of being overridden.

The right to a confidential consultation is not confined to these shores. The European Court of Human Rights has also ruled that the confidentiality of communications between a client and his lawyer is necessary to guarantee effective legal representation.[5] Both article 6 (the right to a fair trial) and article 8 (the right to privacy) of the European Convention on Human Rights (the "**ECHR**") may be engaged.

An absolute right?

Clearly then, LPP is a substantive right. It's central importance to the administration of justice in the UK and more widely across Europe is reflected in common law and statute. But is it an unqualified, absolute right?

The answer, in short, is no. There are a number of established areas where communications that would otherwise appear to benefit from the protection of LPP, do not do so.

The most widely known of the exceptions to LPP is the 'iniquity' or 'crime/ fraud' exception.[6] Strictly speaking not an exception, the iniquity principle provides that LPP does not attach to communications made, or information held, between a lawyer and his client which are themselves part of a crime or fraud, or which seek or give legal advice about how to facilitate the commission of a fraud or a crime. To do otherwise would confer an unjustified immunity on dishonest lawyers.

The protection offered by LPP is also, on occasion, excluded by statute. Sections 291(1)(b) and 311(1) of the Insolvency Act 1986, for example, provide that documents must be disclosed to the Official Receiver and to a trustee in bankruptcy respectively, regardless of whether they benefit from LPP.

Crucially, neither article 6 nor article 8 of the ECHR impose an absolute prohibition on the convert surveillance of legal consultations, provided it is authorized by law and is proportionate.

The approach of the courts to statutory interpretation

At this point, it is important to note the principle of legality: the courts' presumption that a statute is not generally intended to override fundamental human rights (such as LPP). Per Lord Hoffmann in *ex p Simms*[7]:

> "*In the absence of express language or necessary implication to the contrary, the courts therefore presume that even the most general words were intended to be the subject of the basic rights of the individual*."

The relevance of this principle is not restricted to constitutional academics. The courts' approach to statutory interpretation is significant in light of the fact that the UK's legislative framework governing investigatory powers does not contain any express language in respect of LPP. In light of the House

of Lords decision in Re *McE* (see further below) this is critically important.

Investigative powers: the existing legislative framework

The interception of, and collection of information about, communications by public authorities in the UK is governed by the Regulation of Investigatory Powers Act 2000 ("**RIPA**"), together with secondary legislation and codes of practice (the "**Codes**").[8]

Under RIPA, public authorities in the UK such as the Metropolitan Police, the National Crime Agency, MI5 (the Security Service), MI6 (the Secret Intelligence Service) and GCHQ are granted powers to:

- Intercept communications (for example by phone tapping);
- Acquire communications data; and
- Employ surveillance (to secretly monitor people's activities by means of tailing or bugging for example) and covert human intelligence sources (("**CHIS**"), such as undercover police officers).

Re McE

Remarkably, given the invasive nature of the investigative powers granted by it, there is no explicit reference to LPP in RIPA. The significance of this statutory silence was underlined in 2009 when, in *Re McE*, the House of Lords held that Part 2 of RIPA permitted the covert surveillance of meetings between defendants and their lawyers, even though such communications might be covered by legal professional privilege. The decision applies equally to the other investigative techniques under RIPA: the use of CHIS, the interception of communications and the acquisition of communications data.

In short, section 27(1) of RIPA states that covert surveillance carried out in accordance with the Act, "*shall be lawful for all purposes."* It was held that the generality of the phrase "*for all purposes*" was unqualified and overrode the right to a private consultation conferred by section 58(1) of PACE.

In interpreting RIPA, the majority held (consistent with Lord Hoffman's statement in *ex parte Simms*, above) that although it was silent on LPP, RIPA was far from general or ambiguous:

> "*the very essence of its provisions was to enable fundamental privacy rights to be overridden to an extent that was no more than necessary under precise conditions that were sufficiently strict and regulated*."[9]

Crucially however, the House of Lords held that the "*precise conditions*" and safeguards provided for in RIPA and the Code of Practice for surveillance did not offer sufficient protection (to ensure that such surveillance complied in all respects with the requirements of the ECHR) in a case where privileged communications would be gathered.

Belhadj[10]

The finding in *Re McE* as to the lack of sufficient statutory protection in the exercise of investigatory powers when targeting privilege communications was reaffirmed by the declaration of the

Investigatory Powers Tribunal (the "**IPT**") in *Belhadj*.

In February this year, the IPT held that the approach of the UK Government to the interception, analysis, use, disclosure and destruction of legally privileged communications contravened Article 8 of the ECHR between 2010 and February 2015. This ruling (the first time that the IPT has found in favour of an individual claimant in an open judgment) came after the Government had already conceded that its policy concerning the interception of privileged communications had been unlawful.

New codes of practice issued under RIPA

Following *Belhadj* the Government published a new code of practice for the acquisition, disclosure and retention of communications data (the "**Acquisition Code**") and a new draft code of practice for the interception of communications ("**Draft Interception Code**") to purportedly strengthen the protections afforded to privileged material and communications.

Draft Interception Code

The Draft Interception Code now provides that where the interception is intended to intercept legally privileged communications, the Secretary of State must be satisfied that there are "*exceptional and compelling circumstances that make the warrant necessary*."[11]

Where privileged communications will be 'collaterally' intercepted, i.e. where privileged communications are not deliberately targeted by a public authority but where there is a risk of their interception, the application for a warrant should identify the steps which will be taken to mitigate the risk of obtaining material benefitting from LPP.

Acquisition Code

The new Acquisition Code sets out that communications data are not subject to LPP but that it may be possible to "*infer an issue of sensitivity from the fact that someone has regular contact with, for example, a lawyer*."[12] In such circumstances, "*special consideration*" should be given to necessity and proportionality.[13]

A satisfactory response?

The Draft Interception Code (currently subject to public consultation) has been criticized for not offering strong enough protections in instances where the target of the interception is legally privileged communications.

The first two criticisms relate to the wording of the Code.

Firstly, it is not precisely clear what amounts to the "*exceptional and compelling circumstances*" which the Secretary of State must be satisfied of before granting such a warrant. The Code does state that such circumstances will arise only in a very restricted range of cases and provides as examples a, "*threat to life or limb*" or to "*national security*" where the interception is reasonably regarded as likely to, "*yield intelligence necessary to counter the threat*."[14] The phrase "*threat to life or limb*" however is unnecessarily vague. It foreseeably encompasses an overly broad spectrum of

offences ranging from instances where physical injury results from a lack of reasonable care through to international terrorist attacks.

The second criticism relates to the lack of clarity on what use may be made of any privileged communications that are intercepted. The Draft Interception Code provides that "*other than in exceptional circumstances*" privileged material "*must not be acted on or further disseminated.*"[15] Rather unhelpfully, the Code does not define what these "exceptional circumstances" may be. This goes to the heart of the concern that clients will be inhibited from being full and frank with their lawyers: for most clients the key concern is not that the confidential communications may be disclosed but that the matter disclosed may then be used to their detriment. Indeed, although RIPA was held to override section 58(1) of PACE, section 78 of the same statute could well provide a route for the defence to seek to exclude any legally privileged evidence that the prosecution seeks to rely on that was obtained through the use of investigatory powers.

The final criticism is more conceptual. Whilst the Draft Interception Code heightens the hurdle that must be overcome before a warrant will be granted to intercept legally privileged communications, it also fails to address what for many is the fundamental issue: RIPA, as interpreted in *Re McE*, continues to permit public authorities in the UK to deliberately target and access legally privileged communications.

A Question of Trust

David Anderson QC's Report assesses the effectiveness of RIPA and examines the case for a new or amended law. Its scope goes beyond counter-terrorism into counter-espionage, missing persons investigations, internet enabled crime (such as cyber-attacks) and general crime.

A detailed consideration of each of the Report's 373 pages falls outside the scope of this article but the Report does make the following pertinent recommendations in respect of restricting access by public authorities to communications data that benefits from LPP:

- All warrants should be judicially authorized by a Judicial Commissioner at a newly established body: the Independent Surveillance and Intelligence Commission ("**ISIC**");[16]
- When the communications data sought relates to a person who is known to be a member of a profession that handles privileged or confidential communications (e.g. lawyers, doctors, MPs), the new law should provide for special considerations and arrangements to be in place, and the authorization, if granted, should be flagged for the attention of ISIC;[17]
- If communications data is sought for the purposes of determining matters which are legally privileged (such as the identity of a witness being contacted by a lawyer), the designated person should be obliged either to refuse the request or refer the matter to the ISIC for a Judicial Commissioner to decide whether to authorize the request;[18] and
- A Code of Practice, and/or ISIC guidance, should specify:
  - the rare circumstances in which it may be acceptable to do seek communications data for such a purpose; and
  - the circumstances in which such requests should be referred to ISIC.[19]

The Legal Community's Response

Whilst welcoming many of the points raised by David Anderson QC, the Bar Council and the Law Society did not accept the Report's suggestion that the state needs the power to eavesdrop on conversations between a client and his lawyer, even in exceptional circumstances.[20]

The only scenario, in their view, where the law should permit public authorities to seek access to privileged information is where the lawyer-client relationship is being abused for a criminal purpose —in line with the long established iniquity exception.

Conclusion

To conclude we must return to address the two questions posited at the outset of the article; the answers to which are intertwined.

LPP and the ability for a defendant to consult, in confidence, with his lawyer is a substantive right but it is a qualified one. The majority in *Re McE* held that RIPA overrides PACE and that the surveillance of privileged communications by public authorities was permitted.

What must be remembered however is that the majority also held (emphatically supported in *Belhadj*) that RIPA and the Codes did not ensure that such surveillance was carried out in a manner compatible with the right to privacy under article 8 of the ECHR, i.e. the Codes failed to ensure that authorizations were only given in circumstances where the surveillance would be both necessary and proportionate to one of the legitimate aims permitted by article 8(2)—in the interests of national security or public safety for example. The Codes, as redrafted in response to *Belhadj,* do not go far enough to remedy this.

The task of reconciling the right to a confidential consultation and the need to detect and prevent increasingly sophisticated criminality ought not to be seen as a zero sum game. As Lord Philips rightly stated in *Re McE*: "*covert surveillance is of no value if those subject to it suspect that it may be taking place*."[21] The Codes should be redrafted to clearly and stridently govern the authorization and use of the fruits of any surveillance of privileged communications. Such a step would be mutually beneficial: those in custody would be reassured that, save in exceptional circumstances, any consultation that they have with their lawyer will take place in private and the public authorities, should it be deemed necessary and proportionate for them to carry out such surveillance, would do so with an increased likelihood that it would actually yield intelligence necessary to counter any threat.

The Report certainly leaves the reader in no doubt about the urgent need for wholesale reform of RIPA: "*incomprehensible to all but a tiny band of initiates*"[22] and the unsatisfactory state of the current legislative framework governing investigatory powers: "*a system characterized by confusion, suspicion and incessant legal challenge.*"[23] It is to be hoped that the Government acts accordingly.

---

[1] The Report, June 2015, page 232, para 12.65

[2] R (Morgan Grenfell & Co Ltd) v Special Commissioner of Income Tax [2002] UKHL 21, [2003] 1 AC 563 [7]

[3] R v Grant [2005] 2 CR App R 28

[4] McE v Prison Service of Northern Ireland [2009] UKHL 15, [2009] 1 AC 908

[5] Brennan v UK (App no. 39846/98) (2002) 34 EHRR 18 [62]

[6] R v Cox and Railton (1884) 14 QBD 153

[7] R v Secretary of State for the Home Department, ex p Simms [2000] 2 AC 115 (HL) at page 131

[8] Including, amongst others, the Code of Practice for the Interception of Communications (dated 8 September 2010) and the Covert Surveillance and Covert Human Intelligence Sources Codes of Practice (dated 10 December 2014)

[9] McE v Prison Service of Northern Ireland [2009] UKHL 15, [2009] 1 AC 908, para 63

[10] Belhadj & Others v Security Service & Others [2015] UKIPTrib 13_132-H

[11] Draft Interceptions Code, para 4.8

[12] Acquisition Code, paras 3.72-3

[13] Ibid, para 3.74

[14] Draft Interception Code, para 4.8

[15] Ibid, para 4.13

[16] The Report, recommendation 22

[17] Ibid, recommendation 67

[18] Ibid, recommendation 68

[19] Ibid, recommendation 69

[20] http://www.barcouncil.org.uk/media/374039/mp_briefing_lpp_150624.pdf

[21] McE v Prison Service of Northern Ireland [2009] UKHL 15, [2009] 1 AC 908, para 51

[22] The Report, page 8, para 35

[23] The Report, page 9, para 38

Authors

Lloyd Firth

COUNSEL

lloyd.firth@wilmerhale.com

+44 (0)20 7872 1014