

# Wiretaps: The forbidden fruit

FEBRUARY 4, 2016

Foreign observers of the ongoing trial of five defendants at Southwark Crown Court as part of Operation Tabernula (the UK's largest ever insider dealing investigation) may be surprised to note a significant type of evidence that neither the prosecution nor the defence will be introducing: telephone calls intercepted, in the UK, by the use of wiretaps.

Onlookers expecting to witness wiretap evidence being presented to the jury, as seen to devastating effect in the *Galleon*<sup>1</sup> insider trading trial of Raj Rajaratnam in the US in 2011, will be left disappointed. The UK remains the, "only country in the common law world that prohibits completely the use of intercepted communications as evidence in criminal proceedings."<sup>2</sup>

This post examines the UK's current legal framework governing the inadmissibility of intercept evidence (its rationale, inconsistencies and consequences) and the potential detrimental impact of the inadmissibility of intercept evidence on the fairness of criminal prosecutions.

# **Current framework**

The interception of communications in the UK is governed by the Regulation of Investigatory Powers Act 2000 (RIPA).

Under RIPA, the term 'intercepted communications' refers to the covert interception of private communications (including landline and mobile telephone calls, email and ordinary post) by law enforcement and intelligence agencies. The use of information gleaned from such intercepted communications as evidence in civil or criminal proceedings is known as 'intercept evidence.'<sup>3</sup>

Despite the fact that RIPA permits the interception of communications, section 17 prohibits the use in UK courts of intercept evidence which has been collected under a warrant in the UK.<sup>4</sup>

Intercept evidence is used only as a source of intelligence in the UK; not of evidence.

#### Rationale

The legislative bar to intercept evidence being adduced in criminal proceedings has a long legal and political heritage which can be distilled into two basic concerns: secrecy and security and an administrative burden.

#### Secrecy and security

The first argument goes that if intercept evidence were admissible, the intelligence agencies' methods and sources of interception would be revealed and suspects would develop new methods to avoid interception, thereby jeopardising the ability of the state to detect and investigate future criminal activity.

#### Administrative burden

The second argument is that the making admissible of intercept evidence would place an intolerable burden on courts and prosecutors under the 'equality of arms' principle.

That is, under English law, defendants must receive a fair trial under conditions that do not place them at a disadvantage compared to the prosecution. Practically, this means that the defence should have access to all the material on which the prosecution relies (as well as any material capable of undermining the prosecution case or assisting the defence). For the use of intercept material as evidence to be consistent with a fair trial, therefore, all relevant intercepted material collected by an intercepting agency during the course of an investigation would need to be retained, transcribed and catalogued to an evidential standard in order for it potentially to be made available to the defence.<sup>5</sup>

Both points have merit but are not persuasive. The first is wishful thinking in the extreme: serious organised criminals have long been aware of the state's interception capabilities. The second is simply an observation: resourcing concerns ought never seriously to be weighed against an individual's right to a fair trial.

# Incoherent and inconsistent

As has been noted by other commentators, there is an inherent incoherence to RIPA—a scheme which seeks to authorise an activity (intercepting communications), acknowledges that that activity may lead to material which will be relevant at trial and then seeks to suppress that material and even the fact of its existence.<sup>6</sup>

To incoherence add inconsistency. Whilst intercept evidence is inadmissible, numerous other types of covert surveillance evidence *are* admissible, including a telephone conversation that has been:

- recorded by a covert listening device (such as a bug or a hidden microphone);<sup>7</sup>
- made to, or from, a prison; or
- recorded by one of the participants.<sup>9</sup>

The major flaw in the regime, however, is with regard to communications intercepted outside the UK. There is no bar (under Section 17) to admitting intercept evidence in UK criminal proceedings that was lawfully obtained in a foreign jurisdiction, even if the means by which that evidence was gathered would have been unlawful in the UK. UK courts have been willing to admit such evidence on a number of occasions in respect of the prosecution of drug offences.<sup>10</sup>

Conversely, section 17 also does not prohibit communications intercepted in the UK being

introduced as evidence in foreign courts, providing that the UK intelligence agencies are willing to provide them to their foreign counterparts.

### Consequences

The potential introduction, via the purported 'back door', of foreign wiretap evidence into UK criminal prosecutions is of particular significance given the increased trend for international cooperation in law enforcement, particularly between authorities in the UK and the US.

The prosecution brought by the Financial Services Authority (the FSA, as was) in *Blue Index*, which resulted in three people pleading guilty to charges of insider dealing, was notable for involving a parallel, coordinated investigation by the FSA and the US Securities and Exchange Commission, Department of Justice and Federal Bureau of Investigation.<sup>11</sup> The continued deployment of such coordinated trans-Atlantic investigations will only heighten the possibility of wiretap evidence being introduced into UK criminal prosecutions in this way.

#### Reform?

The draft Investigatory Powers Bill, published by the Government on 4 November 2015 with the intention of replacing RIPA and establishing a new, fit for purpose framework for the interception of communications, simply reaffirms the status quo.

Given the inconsistencies highlighted above, however, and the increasingly multi-jurisdictional nature of criminal investigations, it may seem a question of when, rather than if, the UK Government looks again at the admissibility of intercept evidence (in what would be the ninth separate review undertaken since 1993). Unless and until it does, intercept evidence will remain of investigative value only in the UK.

<sup>&</sup>lt;sup>1</sup> http://www.ft.com/cms/s/0/db661a10-7bfe-11e0-9b16-00144feabdc0.html#axzz3z7pz7dqo

<sup>&</sup>lt;sup>2</sup> JUSTICE, "Intercept Evidence: Lifting the Ban", October 2006, page 3.

<sup>&</sup>lt;sup>3</sup> Intercept evidence should be distinguished from other forms of covert surveillance such as recordings made using covert listening devices (e.g. concealed microphones or bugs) to eavesdrop on suspected criminals. Oddly, and as is noted in this post, such covert surveillance evidence *is* admissible in criminal proceedings, see *R v E* [2004] EWCA Crim 1243.

<sup>&</sup>lt;sup>4</sup> Section 18 of RIPA provides for a limited number of exceptions to this prohibition. These largely relate to statutory offences protecting the integrity of postal and telecommunications systems, immigration appeals, public inquiries and a small number of civil proceedings which provide for material to be heard in closed session.

<sup>&</sup>lt;sup>5</sup> In the case of *Natunen v Finland* the European Court of Human Rights ruled that the destruction of intercept material before trial and without disclosure to the defendant was inconsistent with the defendant's Article 6 (fair trial) rights, as the defence had valid reasons for seeking to examine the material - Application No 21022/04) ECtHR Judgment of 31 March 2009.

- <sup>6</sup> Ormerod, D, "Telephone Intercepts and their Admissibility", Criminal Law Review 2004, 15-38, 31.
- $^7$  R v E [2004] EWCA Crim 1243 and R v Smart and Beard [2002] EWCA Crim 772.
- <sup>8</sup> Section 4(4) of RIPA and R v Allan and others [2001] EWCA Crim 1027.
- <sup>9</sup> Section 48(4) of RIPA.
- <sup>10</sup> R v P [2002] 1 A.C. 146, R v Maguire [2009] EWCA Crim 462.
- <sup>11</sup> http://www.fsa.gov.uk/library/communication/pr/2012/060.shtml

# Authors



Lloyd Firth

 $\smile$ 

lloyd.firth@wilmerhale.com

C

+44 (0)20 7872 1014