

# Intercept Evidence: A tool in the fight against terrorism?

---

Eric Metcalfe

Director of Human Rights Policy

JUSTICE



# What is intercept evidence?

---

An 'intercept' is the covert interception of a private communication, including:

- Telephone calls (including VoIP)
- Fax transmissions
- Mobile phone calls (including text messages)
- Email and IM
- Ordinary post

# What is intercept evidence?

---

- Interceptions are governed by the Regulation of Investigatory Powers Act 2000 ('RIPA')
- The Home Secretary has power to issue interception warrants for a number of purposes, including:
  - the interests of national security; and
  - preventing or detecting serious crime

# The ban on intercept evidence

---

- Section 17 of RIPA prohibits any evidence that may disclose or 'tend to disclose' the existence of an intercept warrant
- Statutory ban has only existed since 1985 but reflects decades-long government practice of not disclosing telephone intercepts in court cases

# The ban on intercept evidence

---

- Reflects long-standing government concern that disclosure of intercepts would ‘compromise interception capability’
- Specifically, concern that criminals and terrorists would gain valuable information concerning methods of interception

# The ban on intercept evidence

---

Other arguments against lifting the ban include:

- Fear of damaging relationship between police and intelligence services
- Fear of hampering ability to adapt to changes in communications technology
- Concern over increasing the burden on police and intelligence services
- Intercept material inappropriate in adversarial criminal proceedings

# The ban on intercept evidence

---

Number of exceptions to intercept ban include:

- Intercept made with knowledge of one party
- Intercepts made outside the UK
- Intercepts of calls to or from a prison or mental hospital (e.g. the Soham murders)
- Recordings of telephone calls made via bugging rather than direct interception

# The ban on intercept evidence

---

No ban on the admissibility of evidence from covert surveillance in general, including:

- A covert listening device (a bug) in a suspect's house, office or vehicle
- A concealed microphone worn by an informant
- External video or audio surveillance of a suspect's home or office

# Public Interest Immunity

---

- Right to a fair trial means that the prosecution must disclose to the defendant any material ‘reasonably capable’ of undermining prosecution case or assisting the case for the accused
- But prosecution not obliged to disclose other material, including material that is ‘either neutral in its effect or which is adverse to the defendant’ (*R v H* [2004] UKHL 3 per Lord Bingham)

# Public Interest Immunity

---

- Prosecution can apply to court under section 3(6) of the Criminal Procedure and Investigations Act 1996 to prevent disclosure if the court ‘concludes it is not in the public interest to disclose it’
- Most common reason for non-disclosure is the need to protect identity of informants, undercover agents, or scientific or operational techniques (such as surveillance methods)

# Public Interest Immunity

---

The entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to protect witnesses at risk of reprisals, or keep secret police methods of investigation of crime, which must be weighed against the rights of the accused.

*Rowe and Davis v UK* (2000) EHRR 1, para 61

# Public Interest Immunity

---

PII principles protect interception capabilities in:

- Australia
- Canada
- EU
- Israel
- New Zealand
- South Africa
- United States

# Prosecuting with intercept evidence

---

Law enforcement agencies at all levels of government have uniformly found electronic surveillance to be one of the most important tools – if not *the* most important tool available to them in the prevention, investigation, and prosecution of many serious types of crime. This tool has been critical in fighting terrorism, organized crime ... and in saving numerous innocent lives.

FBI Director Louis Freeh, January 1999

# Prosecuting with intercept evidence

---

- Numerous successful prosecutions of terrorism offences in the US since 9/11 using intercept evidence
- Most suspects plead guilty when faced with recordings of incriminating telephone calls or emails
- No evidence that use of intercept evidence in other jurisdictions has led to deterioration of intercept capability

# Impact on policing and intelligence

---

Relationships between the NSA and the US Department of Justice and between the ASIO and the various law enforcement agencies in Australia are now much closer than they were. [The] suggestion that the relationship between the intelligence agencies is unique in terms of the information flows between them is now more difficult to sustain.

Crown Prosecution Service study, June 2005

# Impact on policing and intelligence

---

I have long been in favour of intercept evidence being used in court. The court can then weigh it up. At the moment, nobody can test it.

Sir Ian Blair, February 2005

You can be very selective about the things you are going to transcribe if you are very precise in your investigation and focused.

Assistant Commissioner Andy Hayman,  
February 2006

# Impact on policing and intelligence

---

Any attempt to intercept communication outside RIPA would be unlawful. Article 8 ECHR requires that all interceptions must be governed by law:

- *Malone v United Kingdom* (1984) 7 EHRR 14
- Interception of Communication Act 1985
- *Halford v United Kingdom* (1997) 24 EHRR 523
- RIPA 2000

# Why allow intercept evidence?

---

Allowing intercept evidence would:

- Increase the likelihood of convicting terrorists
- Reduce pressure for extended pre-charge detention in terrorism cases
- Increase the fairness of trials
- Ensure consistency between the use of intercept evidence and evidence from covert surveillance

# Why allow intercept evidence?

---

Intercept evidence consistent with the principle of due process and the right to a fair trial, unlike:

- Indefinite detention without trial (Part 4 of the Anti-Terrorism Crime and Security Act 2001)
- Control orders, including house arrest, on the basis of suspicion (Prevention of Terrorism Act 2005)
- Extension of pre-charge detention to 28 days (Terrorism Act 2006)

# Why allow intercept evidence?

---

While terrorism poses difficult questions for every country, it poses especially difficult questions for democratic countries, because not every effective means is a legal means .... This is the fate of democracy, as not all means are acceptable to it, and not all methods employed by its enemies are open to it. Sometimes a democracy must fight with one hand behind its back. Nonetheless, it has the upper hand.

Aharon Barak, President of the Israeli Supreme Court