Not a silver bullet… but a bullet nonetheless

Ending the ban on the use of intercept material in criminal proceedings

Introduction

On 23 July 2018 the news broke that the Government had supplied evidence to US authorities concerning Alexanda Kotey and El Shafee Elsheikh. The men were accused of being part of a group who murdered journalists and aid workers in Syria and created notorious propaganda videos for the so-called Islamic State.

There is nothing unusual about international evidence sharing – the Government receives over 8,000 mutual legal assistance requests a year. But what made this case extraordinary was that Ministers had shared evidence without first seeking an assurance that the men would not face the death penalty in the US. Shadow Home Secretary Diane Abbott criticised the action as undermining the UK's longstanding opposition to capital punishment, arguing that Ministers cannot be '…a little bit in favour of the death penalty. Either we offer consistent opposition, or we do not.'[1]

Kotey and Elsheikh had strong connections to the UK, having formerly been British citizens. Two of their alleged victims were UK nationals. But Ministers preferred to supply evidence to support a trial in the US rather than domestically. Former Director of Public Prosecutions Lord MacDonald described this as 'an abdication of sovereignty'.[2]

Why did Ministers not seek a trial in the UK? Lord MacDonald hinted at one possible reason: British-collected intercept material relevant to the case would be admissible in US courts. But it is banned even from being mentioned in UK courts. It is submitted that the ban is illogical

[1] HC Deb 23 July 2018, vol 645, col 726
[2] https://www.theguardian.com/law/2018/jul/24/uk-may-face-legal-challenge-over-us-extradition-of-isis-pair

and undermines the proper prosecution of serious crime and terrorism in the UK. This essay explains why and how the ban should be ended.

What is interception?

Interception can be described as the act of making the content of a communication available to a person who is neither the sender nor an intended recipient of that communication.

State interception of communications is arguably as old as communications technology itself. The first public reference to the practice can be traced to the Proclamation of May 25th, 1663 which restricted the opening of letters or packets to those authorised by the Principal Secretary of State.[3] In 1984 the European Court of Human Rights noted:

> The power to intercept telephone messages has been exercised in England and Wales from time to time since the introduction of the telephone.[4]

Prior to the Interception of Communications Act 1985 ("IOCA"), there was no statutory basis for the interception of telephone communications in the UK. In fact, the Government had expressly declined to bring forward legislation, arguing it would undermine the secret nature of the techniques used. IOCA was introduced in response to the European Court of Human Right's judgment in *Malone v United Kingdom*.[5]

Malone was on trial for handling stolen goods when he learned that a telephone call he had made had been intercepted. The interception had been authorised under warrant from the Home Secretary. But there was no statutory basis for the Home Secretary's power to issue a warrant. Nor was it claimed to flow from the royal prerogative. Malone challenged this in the domestic

[3] Report of the Committee of Privy Councillors appointed to inquire into the interception of communications (Cmnd 283) (1957), para. 9. Available at https://www.fipr.org/rip/Birkett.htm
[4] *Malone v United Kingdom* (1985) 7 E.H.R.R. 14 at [28]
[5] Ibid

courts but the case was dismissed as being non-justiciable. The European Court of Human Rights found that the practice of interception was an unjustified breach of Article 8 ECHR as it was not conducted 'in accordance with law'.

Whilst IOCA brought the interception of telephone communications into statute law, it also sought to minimise its justiciability. Section 9 of IOCA stated:

> (1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest—
>
> (a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below ; or
>
> (b) that a warrant has been or is to be issued to any of those persons.

IOCA was replaced by the Regulation of Investigatory Powers Act 2000 ("RIPA"), which in turn has been replaced by the Investigatory Powers Act 2016 ("IPA"). Although the law and technology concerning the interception of communications have been transformed since 1985, the ban on the use of intercept material has persisted. It is now contained in section 56 of IPA.

The effect of section 9 and its successors is that although interception is permitted by legislation, discussing interception in court is banned. A person in Malone's position today would have no way of confirming whether interception had occurred. If prosecuting counsel were to confirm a defendant's suspicions that his communications had been intercepted they would risk committing an offence punishable by up to 5 years' imprisonment.[6]

[6] Section 59 Investigatory Powers Act 2016. Alternatively, they may have committed an offence under section 4 of the Official Secrets Act 1989.

Why is intercept material excluded from criminal evidence?

The Attorney General issues guidance[7] which explains the policy behind the ban. It states:

> It has been long-standing Government policy that the fact that interception of communications has taken place in any particular case should remain secret and not be disclosed to the subject. This is because of the need to protect the continuing value of interception as a vital means of gathering intelligence about serious crime and activities which threaten national security. The Government judges that if the use of the technique in particular cases were to be confirmed, the value of the technique would be diminished because targets would either know, or could deduce, when their communications might be intercepted and so could take avoiding action by using other, more secure means of communication.

In practice this means that the interception of communications is subject to a policy of neither confirm nor deny. If prosecutors are asked whether interception has occurred in a particular case, they are advised to say:

> I am not in a position to answer that, but I am aware of sections 17 and 18 of the Regulation of Investigatory Powers Act 2000 and the Attorney General's Guidelines on the Disclosure of Information in Exceptional Circumstances under section 18.[8]

Problems with the ban

Intercept material can be highly incriminating. This is one reason why it has intelligence value. It may be the crucial evidence that would support a conviction. But section 56 of IPA excludes

[7] Attorney General's Guidelines for Prosecutors: Section 18 of the Regulation of Investigatory Powers Act 2000 (England and Wales). Presumably an updated version, taking into account the Investigatory Powers Act 2016 will be published soon.

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/16324/Intercept_Guidelines_-_reformatted.pdf

this material from criminal evidence and denies the prosecutor or the courts any discretion in the matter. We have examined its possible relevance to the case of Kotey and Elsheikh. We will now consider two cases which illustrate directly the value of intercept material in our criminal justice system, and which show why the policy argument set out in the Attorney General's guidance is undermined by the various exceptions to the ban.

In June 2018, 18 year old Safaa Boular was found guilty of offences contrary to section 5 of the Terrorism Act 2006. At her trial, a recording was played of Miss Boular talking to her sister Rizlaine. Using a rudimentary code, they discussed Rizlaine's plans to commit a terror attack alongside their mother, Mina Dich. Safaa was already in custody when the call took place, and she used the prison telephone to talk to her sister.[9] Prison telephones are not classed as public telephone systems by the IPA, and intercepted prison telephone calls are admissible in court.[10] As the BBC noted:

> This conversation was a key part of the evidence against Rizlaine Boular and Mina Dich, leading to their guilty pleas.[11]

Mobile phones abound in prisons in 2018. But if Safaa Boular's phone call had taken place on a smuggled mobile phone, the content of the call could not have been used as evidence against her or the other defendants. The remaining evidence may not have been sufficient to secure their pleas or their convictions after trial. We will never know what effect the recording of the call had on the jurors who found Safaa guilty, but it seems fair to infer that it had some effect.

Intercept products are admissible in closed material proceedings and some closed tribunals, including in proceedings for Terrorism Prevention and Investigation Measures ("TPIMs").[12] It

[9] https://www.cps.gov.uk/cps/news/teenager-convicted-uk-terror-plot
[10] Investigatory Powers Act 2016, Schedule 3, paragraph 2
[11] https://www.bbc.com/news/uk-44359958
[12] Investigatory Powers Act 2016, Schedule 3, paragraphs 4 - 17

may have been possible to use the intercepted phone call to support applications for TPIMs against the Boular sisters and their mother. But TPIMs are a poor substitute for criminal convictions, particularly when there would be sufficient evidence to convict were it not for section 56 of IPA.

TPIMs are only available in cases concerning terrorism-related activity. *Malone* was not a terror case. And the interception of communications continues to have value well beyond terror cases. In *Knaggs*[13] communications intercepted by the Dutch authorities formed part of the prosecution evidence in a conspiracy to import cocaine and other drugs into the UK. Knaggs and his associates were convicted and sentenced to a total of over 80 years' imprisonment.

Intercepted communications were admissible in *Knaggs* because they had been intercepted in accordance with Dutch law. The Court of Appeal noted that ban on the use of intercept products extends to materials obtained by overseas authorities under mutual assistance warrants, but found that cooperation between UK and Dutch authorities had been more informal in this case. The UK authorities had not procured the interception and it therefore did not fall to be excluded under section 18 of RIPA.[14] *Knaggs* has been described as an example of how the ban on using intercept products in court encourages 'international law enforcement arbitrage'.[15] It is certainly difficult to understand the policy justification for excluding evidence obtained under a mutual assistance warrant but admitting evidence obtained overseas by more informal means.

Boular and *Knaggs* illustrate the utility of intercept products in securing convictions for serious offences. Crucially, in each case, slightly different facts would have engaged the ban on the

[13] *R v Knaggs and others* [2018] EWCA Crim 1863
[14] The law in force at the time, which is essentially replicated by the Investigatory Powers Act 2016.
[15] https://crimeline.co.uk/uk-ban-on-eavesdropping-encourages-a-culture-of-international-law-enforcement-arbitrage/

use of intercept products, eroding or even destroying the basis for convictions that were undoubtedly in the public interest. They show the need to repeal section 56 of IPA.

How would law reform work?

Having demonstrated the increasing undesirability of the ban on the use of intercept material as criminal evidence, this essay proposes a simple solution. That is, to repeal section 56 of IPA along with section 3(7), 7A(9) and 8(6) of the Criminal Procedure and Investigations Act 1996 ("CPIA"). Repealing section 56 of IPA would enable interception to be discussed during criminal proceedings. Repealing the aforementioned provisions of the CPIA would enable the prosecution to use interception material as part of their case against the accused. It would also require the prosecution to disclose unused intercept material to the defence where the test for disclosure is also met.

Law reform would not lead to a flood of intercept material coming before the criminal courts or disclosed to defendants. Prosecutors would need to decide whether any available intercept material was necessary for them to put their case. Many cases where interception takes place would doubtless continue to be prosecuted without such material. Prosecutors would not be required to make disclosures where the CPIA test was not also met. As Lord Bingham stated in *R v H*:

> If material does not weaken the prosecution case or strengthen that of the defendant, there is no requirement to disclose it. […] Neutral material or material damaging to the defendant need not be disclosed.[16]

[16] *R v H* [2004] 2 A.C. 134

Even where intercept material does meet the test for disclosure, it would be open to the prosecution to seek a ruling that disclosure would not be in the public interest.[17] This would exclude the evidence from the case entirely.

Furthermore, a range of statutory and common law measures can be deployed to minimise the risks associated with handling sensitive evidence in the criminal courts. The common law permits parts – or even all – of a trial to be held *in camera* where strictly necessary to enable justice to be done.[18] Reporting restrictions can be imposed. And whilst there is no restriction on jurors discussing evidence presented in open court, it is an offence to disclose information about their deliberations.[19] So the precise effect of intercept material on a jury's verdict would not become known.

Interception is not solely undertaken by our intelligence agencies. Nor is it solely deployed for national security purposes. 3007 new interception warrants were issued in 2016, across nine interception agencies.[20] Of those 3007 warrants, 65% were for the purpose of preventing or detecting serious crime.[21] Where a warrant is issued f or the purpose of preventing or detecting serious crime there should be a presumption that the fruits of that warrant are admissible as criminal evidence.

Benefits of law reform

Ending the statutory ban on the use of intercept products in court could increase public confidence in the authorities' ability to disrupt crime and bring offenders to justice. The contribution of intercept material to public confidence in the justice system was noted as far

[17] See section 3(6) CPIA
[18] See *In re Guardian News and Media Ltd and others* [2016] EWCA Crim 11
[19] Juries Act 1974, section 20D
[20] IOCCO annual report 2016, p38
[21] Defined by section 81(3) of RIPA and now section 263 of IPA as a crime for which an adult first-time offender could reasonably expect a sentence of three years' custody or more, or which involves the use of violence, substantial financial gain or conduct by a large number of persons in pursuit of a common purpose

back as 1923. In the trial of Irish nationalist Art O'Brien and others for seditious conspiracy, Mr Justice Swift stated:

> …it was no doubt a matter of surprise to the jury to learn of the mass of correspondence passing between London and Dublin and of relief to know that the authorities in this country were not so blind or stupid as they were sometimes thought to be and that they knew a little more of what was going on than those who did these things either suspected or imagined.... It is well for this country that there is an organisation – when it is suspected that a crime is about to be perpetrated – which has a means of watching the suspected persons.[22]

Post-1985 it would be a criminal offence for a judge to make such a statement before a jury.

In December 2017 the Bar Council's Law Reform committee argued that intercept evidence should be admissible in court with the leave of the judge.[23] This essay goes further – arguing that intercept evidence should be admissible on the same basis as other relevant evidence. It should not require the leave of the judge. This approach has previously been supported by NGOs including Liberty[24] and JUSTICE[25]. In what amounts to the most comprehensive independent report on intercept evidence, JUSTICE stated that:

> Intercept evidence may not be a silver bullet but it is a bullet nonetheless. The time has come for the UK to join the ranks of common law countries that allow such ammunition in the fight against terrorism.

[22] Birkett report, para 149
[23] Bar Council response to the Regulation of Investigatory Powers Act 2000: revised codes of practice, December 2017, para 23
[24] https://www.libertyhumanrights.org.uk/news/blog/5-reasons-why-we-need-intercept-evidence-court
[25] *Intercept evidence: Lifting the Ban*, JUSTICE, 2006

The common law countries JUSTICE refers to are Australia, Canada, New Zealand, South Africa, and the United States. Other democracies use intercept evidence in criminal proceedings too, notably the Netherlands.

In 2010, the Coalition programme for government stated that Ministers would "seek to find a practical way to allow the use of intercept evidence in court"[26]. Given the number and range of authoritative voices in favour of such a move, it is submitted that this was a laudable aim. This was followed up with a command paper, published in December 2014. This summarised previous reviews of the policy, and conducted a cost-benefit analysis of potential law reform. The paper concluded that ending the ban on the use of intercept material in court could be technically difficult and that law reform should not take place "at this time".[27]

It is submitted that the outcome of the review was essentially a foregone conclusion, as it drew exclusively upon earlier studies that also supported a continued ban. The time has come for the Government to justify the ban from a point of principle, or to bring it to an end.

Furthermore, ending the ban on the use of intercept evidence would support the overriding objective of the criminal justice system: to deal with cases justly and, in particular, to acquit the innocent and convict the guilty.[28] As the cases of Boular and Knaggs show, intercept evidence can help to secure convictions in some of the most serious crimes against our society.

Conclusion

The ban on the use of intercept material in criminal proceedings undermines our ability to prosecute the most serious crimes. As can be demonstrated by its absence in numerous other

[26] *The Coalition, our programme for government, p.24,* May 2010, available at https://www.gov.uk/government/publications/the-coalition-documentation
[27] HM Government, 2014, *Inter*cept *as Evidence* (Cm 8989). HMSO
[28] Criminal Procedure Rules, rule 1.1

democracies, it is not necessary to protect the public interest in maintaining secrecy around intelligence gathering. Repeal would boost public confidence in the administration of justice. It would be relatively simple and would not lead to a flood of sensitive material becoming disclosable. For these reasons, this law reform is practical, desirable and useful. **(2999 words)**