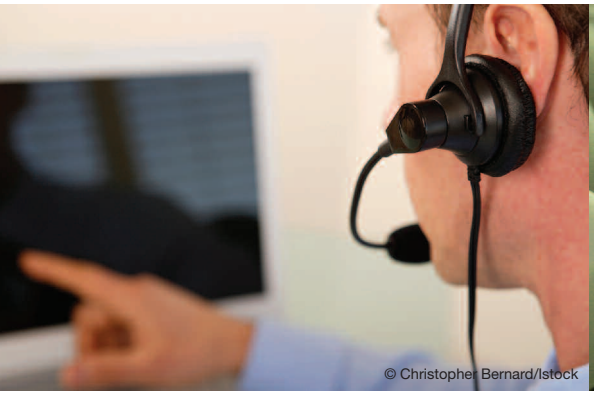
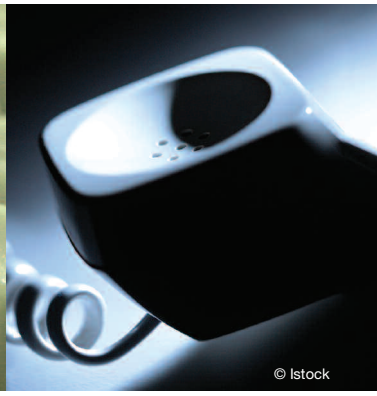
the policefoundation
improving policing for the benefit of the public

The briefing

Series 1, Edition 7 – August 2009





Police interception of communications

This Police Foundation Briefing looks at police interception of communications and identifies some of the key issues which arise from the use of these powers.

Introduction

Technological advances in surveillance have given the police access to a wide range of intelligence, from stored database information to CCTV footage. Most of this type of surveillance is discernable – CCTV cameras are visible to the public and suspects are informed when DNA or other details are stored on the Police National Computer.

But the police also use covert, hidden forms of surveillance where they have identified a suspect and need to gather intelligence without the knowledge of that person. This may include the undercover wearing of a recording device, bugging private locations such as a suspect's house or car, the use of informants and the interception of telephone calls, post and email. The information obtained is used by the police in a number of ways; for the investigation of cases, including

the discovery of leads or planned criminal activity; to disrupt or hinder criminal plots; or to acquire a broader understanding of large-scale criminal activity such as terrorism.

The police have access, without a warrant, to communications *data* such as telephone numbers, billing information, websites accessed and mobile phone locations. These pieces of information can provide intelligence about the movements and associates of a suspect. When more intelligence is needed a warrant can be granted to allow the police to access the *content* of a suspect's communication without that person's knowledge. This Police Foundation Briefing looks at the police use of interception of a communication's content(1). It examines the structure and regulation of interception and some of the main concerns with the present system, including the use of intercepted material as evidence in court.

The legal framework

Where there is evidence of a suspect's involvement in serious crime or terrorism, the police can apply for a warrant to intercept that suspect's communications allowing all communication (email, post, telephone calls and mobile calls) to be read, seen or heard. The Home Secretary may grant the warrant under Section 5 of the Regulation of Investigatory Powers Act (RIPA) 2000 for any of the following three purposes:

- In the interests of national security
- To prevent or detect serious crime
- To safeguard the economic interests of the UK

The issuing of the warrant must comply with the Human Rights Act 1998, which requires that the Home Secretary is satisfied that the interception is necessary and proportionate.

The Home Secretary should also consider the privacy of those people who are not subject to a warrant but who might nonetheless be on the receiving end of a telephone call. All intercepting bodies must also follow the Interception of Communications Code of Practice(2).

The warrant can require any UK based postal, Internet Service Provider or telephone company to intercept communications and to provide access to current as well as stored communications. A limited number of authorised bodies can apply for the warrant, including the police, the security services and HM Revenue and Customs. An interception warrant is valid for 3 months. Warrants for serious crime can be renewed for a further 3 months, while warrants to protect national security or secure economic well-being can be renewed for a further 6 months. The person whose communication is being intercepted will be unaware of the interception and under Section 19 of RIPA it is actually an offence to reveal the existence and details of an interception warrant so any communications service supplier must also keep the information secret.

In 2007 2026 interception warrants (including telephone and postal) were granted under RIPA in England, Wales and Scotland(3).

In professional communications, such as between lawyer and client or doctor and patient, confidentiality must be maintained unless the communication is deemed to be for a criminal purpose. Currently, unless required by national security, communications by MPs cannot be intercepted (the so-called Wilson Doctrine). This practice has been criticised by the Interception of Communications Commissioner on the basis

that it allows MPs potentially to engage in criminal activity without the risk of being investigated and thereby sets them above the law. The Wilson Doctrine was set out in 1966 by the then Prime Minister, Harold Wilson and in September 2007, in response to a written parliamentary question, Prime Minister Gordon Brown confirmed the Doctrine was still valid (4).

In 2005 and 2006 Scotland Yard monitored conversations between MP Sadiq Khan and his constituent and childhood friend Babar Ahmed. The conversations were taped in prison, where Ahmed was being held on terrorist charges. An inquiry into the taping was conducted by the Chief Surveillance Commissioner, Sir Christopher Rose (5), which held that the conversation was not covered by the Wilson Doctrine as it was a face to face conversation and the correct procedures had been followed. The government has agreed to review the codes of practice relating to conversations between an MP and his or her constituents with a view to making them confidential however they take place.

Section 8(4) of RIPA allows for a particular type of warrant to be granted in situations which do not require the name of a person or premises to be stated. It gives permission for mass surveillance of the external traffic of a telecommunications network. In order for this warrant to be granted, it must comply with the Section 5 requirements (national security, serious crime or economic well-being) and it must be used to intercept external communications (i.e. communications sent to or received from outside the UK). Section 8(4) warrants are used principally to search for keywords that might alert security authorities to the existence of terrorist cells or terrorist activity.

Currently, RIPA warrants are authorised by the Secretary of State rather than a judge. Although a judge (the Interception of Communications Commissioner) does review past authorisations and prepares a report, this only occurs after interceptions have taken place. There are concerns that, with an executive authorised system, an excessive number of warrants may be granted, with the danger of political considerations taking precedence. The criteria the Home Secretary must consider are based on relatively abstract notions such as economic interests and national security posing concerns that the executive is insufficiently independent to balance the considerations of individual and state.

Police use of interception

The Serious and Organised Crime Agency (SOCA) carries out interception on behalf of the police, who see it as an essential tool in the fight against serious crime and terrorism. In 2007 the Prime Minister requested a review of the use of intercept evidence, which was published in February 2008 (6). It summarises the main advantages of intercept intelligence as: allowing covert monitoring of a suspect with little safety risk for officers; providing a more flexible and less intrusive tactic than eavesdropping or covert entry into a suspect's private residence; and providing quality leads on proposed criminal activity. Whether in real time, or after a crime has been committed, interception can also help the police identify suspects or stolen property. The Review made particular mention of kidnap cases, where intercept intelligence has been a large factor in the low rate of kidnap fatalities (with no kidnap deaths since 1999).

There is little published information on how the police use interception intelligence or how the operations are carried out due to the necessarily covert nature of the act. National security issues surrounding warrant cases make it difficult for the police to demonstrate publicly the value of interception. For similar reasons, there is also a dearth of independent research on the effectiveness of intercept and in particular its impact in reducing, preventing or detecting crime. Much of what is known is based on anecdote, such as the following quote from Sir Paul Kennedy, Intelligence Services Commissioner:

"It is my view that during 2006 interception played a vital part in the battle against terrorism and serious crime, and one that would have not been achieved by other means. I am satisfied that the intelligence and law enforcement agencies carry out this task diligently and in accordance with the law."

Similarly, the Chilcot Review quotes SOCA as stating that interception, together with communications data, is the single most powerful tool for responding to serious and organised crime and that very few major criminal investigations do not involve interception,(7) but this cannot be supported by any publically available data.

Intercept information as evidence

By law, any information gathered by interception has been used for criminal intelligence purposes rather than as evidence (although there are a few exceptions in a narrow range of financial cases). In practice it means that this intelligence can help police with their investigation but, even if a suspect admits to a crime on a tapped telephone, such admissions will not be allowed in court.

The rationale for this rule is based on concerns that the use of such information could put police and intelligence agencies at risk by exposing their operational methods or that it could encourage criminals to change their style of communication. The use of intercept evidence could also place an onerous administrative burden on security services to keep and produce large amounts of evidence and there are also issues, such as the right to privacy of the person on the other end of the telephone call, that need to be considered.

The UK is the only common law country that does not allow intercept evidence to be used in court .

Human rights groups such as Liberty(8) and Justice(9) have criticised the ban on intercept evidence on the basis that it is counter-productive and unnecessary. They claim that the use of intercept evidence may make for a fairer trial by allowing all the evidence against the accused to be contested. Further, the period of pre-charge detention could potentially be reduced if the police were able to adduce evidence obtained through interception, rather than needing additional time to find further evidence in support of the prosecution case.

The Chilcot Review supports 'in principle' the admission of intercept evidence in terrorism and serious crime cases, subject to a number of conditions designed to protect security agencies. However, the Review held that introducing intercept evidence would only result in a 'modest' increase in successful prosecutions and listed a number of concerns, such as the administrative burden and the danger of compromising security techniques

and agencies. The Review suggested a model of an intercept evidence system that could be incorporated into the UK. In response to the Chilcot Review, the Government has agreed to look again at the possibility of a limited use of interception evidence in court, subject to satisfying a number of operational requirements.

RIPA oversight and accountability

In order to balance civil liberties and security, RIPA has a number of safeguards and checks with three different commissioners overseeing its use: The Interception of Communications Commissioner, the Intelligence Services and the Chief Surveillance Commissioner. Evidence submitted to the House of Lords Review of Surveillance (10) suggests that having three separate bodies could be confusing and that sometimes conflicting advice is given. The Commissioners also have minimal resources for investigating claims and limited powers of sanction, leading to concerns that the system of interception is insufficiently accountable.

The Interception of Communications Commissioner reports annually on all interceptions and refers complaints about surveillance or interception to an Investigatory Powers Tribunal. The Tribunal looks at the legality of an interception warrant and awards compensation where such warrants are deemed to have been improperly granted. The Tribunal has been criticised as an inadequate safeguard since it can only investigate cases where a warrant for interception has been granted, rather than unauthorised interceptions. Further, the Tribunal's decision cannot be challenged in the courts. Due to the covert and delicate nature of the information before it, the Tribunal holds hearings in private and has attracted criticism for its lack of transparency (11).

As the issue of a warrant is secret and the target will not know an interception is occurring, it is difficult for an individual to contest a warrant. All the safeguards, therefore, apply only after the communication has been intercepted. Similarly, current safeguards only check that the correct procedure has been followed in cases where a warrant has been issued. If telephone tapping takes place illegally without a warrant, this is a matter for the police. The Constitutional Committee of the House of Lords has recommended that once surveillance of an individual has been completed, he should be informed and, if the surveillance is found to be unlawful, suitably compensated (12).

The current structure of interception in place in the United Kingdom has been criticised by human rights groups, the judiciary, opposition spokespeople and academics. Recent reports from The Home Affairs Select Committee (13) and the House of Lords (14) have raised a number of concerns. There are arguments that the UK is out of line with the rest of the world in regard to the decision-making and accountability of interception, although the recommendations in the Chilcot Review (15) and the House of Lords report, if adopted, may go some way towards remedying this. The balance between civil liberties and security in the field of interception is particularly delicate yet, due to the need for the investigation to remain under cover, the process and analysis behind the decision to intercept a communication also has to be conducted out of sight, so currently any safeguard checks can only take place after the interception has occurred.

What happens in other countries?

In most Western countries, a dual system operates, with judicially authorised interceptions for law enforcement purposes and administratively authorised interceptions for intelligence purposes. There are however variations on this general approach. In France, for example, the Prime Minister may authorise interceptions for the purposes of safeguarding national security, scientific and economic well-being or to prevent terrorism. In Ireland, interception for law enforcement in serious criminal cases, or where the security of the state is threatened, is authorised by the executive (Minister of Justice), while in Canada and the US, all interceptions are authorised by a judge, except for cases (in Canada) where there is a threat to national security.

In most other countries, intercept evidence is usually admissible in court and has to be disclosed to the defence. The Chilcot Review considered the use of intercept evidence abroad and concluded that the admission of such evidence did not result in higher conviction rates for serious crime than in the UK. The Review also emphasised that EU countries have a different justice system, where a magistrate performs both an investigatory and a judicial function. The model system recommended by the Chilcot Review is one in which all intercept evidence is potentially admissible, as long as the required evidential standards are met (16).

The future

The number of communications events per year in the UK will rise from around 230 billion in 2006 to nearly 450 billion in 2016 (17).

In anticipation of an increase in the volume and sophistication of communications, the UK Government is currently developing the Interception Modernisation Programme (IMP). Initially, proposals included the creation of a single, central database to store information relating to both the data and the content of all communications. However, after concerns were raised in August 2009 over the need to keep access to data and content separate,(18) it was announced that this aspect of the IMP had been abandoned (19).

Conclusion

The ability to intercept information is an important tool for the police and security services and is used for intelligence and information gathering in relation to past as well as future criminal and terrorist activity. However, the current system of executive rather than judicial warrant authorisation has raised concerns and adequate safeguards should be put in place to address civil liberty and privacy issues, which would enable the police to make fairer and more appropriate use of valuable intelligence. Little is published about how effective interception is in reducing and preventing serious crime since its covert nature precludes easy access for research purposes, but the use of interception would benefit from independent research, under controlled conditions, to assess its impact as well as its wider repercussions.

The Government's approach to surveillance and information gathering has traditionally focused on the 'nothing to hide nothing to fear,' doctrine. According to Tony McNulty, former Minister of State at the Home Office: "If people are involved in entirely legitimate activities then they do not have to worry about RIPA at all."(20) However, the rate at which the methods and authorised users of surveillance systems are expanding has attracted concern from a number of sources, including Dame Stella Rimington, the former head of MI5 (21).The Information Commissioner's Office warned in 2006 that expansion of surveillance could have long term adverse effects on society, undermining trust and fostering a climate of suspicion (22) and the International Commission of Jurists has raised concerns about the normalisation of exceptional laws: that as a society we become accustomed to a new balance whereby laws that were originally enacted to fight serious crime or terrorism slowly become part of our everyday life, paving the way for ever more restrictive legislation to be enacted (23). With increasingly sophisticated methods of communication, these concerns are unlikely to recede.

Notes and references

1. For information on communications data where the police look at information *about* a communication, such as numbers dialled, mobile phone location and website access, see the Home Office consultation document *Protecting the Public in a Changing Communications Environment* available at http://www.homeoffice.gov.uk/documents/cons-2009-communications-data
2. Home Office (2002) *Interception of Communications: Code of Practice,* London: The Stationery Office
3. Privacy International (18 December 2007) *PHR2006*
4. House of Commons Hansard written answers for 12 September 2007, Surveillance, available at http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070912/text/70912w0013.htm#07091234000025
5. Report of Investigation by The Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner, (February 2008) *Report on Two Visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill* Cm 7336, London: The Stationery Office
6. *The Privy Council Review of Intercept as Evidence – Report to the Prime Minister and Home Secretary, 30 Jan 2008,* Cm 7324, London: The Stationery Office
7. *The Privy Council Review of Intercept as Evidence – Report to the Prime Minister and Home Secretary, 30 Jan 2008,* Cm 7324, London: The Stationery Office
8. Crossman G. et al, (2007) *Overlooked: Surveillance and Personal Privacy in Modern Britain,* London: Liberty
9. Metcalfe E. (2006) *Intercept Evidence: Lifting the Ban,* Justice
10. House of Lords Constitution Committee Second Report (February 2009) *Surveillance Citizens and the State,* London: The Stationery Office
11. Metcalfe E. (2009) *Secret Evidence,* Justice
12. House of Lords Constitution Committee Second Report (February 2009) *Surveillance Citizens and the State,* London: The Stationery Office
13. Home Affairs Committee (June 2008) Fifth Report *A Surveillance Society?,* London: The Stationery Office
14. House of Lords Constitution Committee Second Report (February 2009) *Surveillance Citizens and the State,* London: The Stationery Office
15. *The Privy Council Review of Intercept as Evidence – Report to the Prime Minister and Home Secretary, 30 Jan 2008,* Cm 7324, London: The Stationery Office
16. *The Privy Council Review of Intercept as Evidence – Report to the Prime Minister and Home Secretary, 30 Jan 2008,* Cm 7324, London: The Stationery Office
17. Home Office estimation, cited in *The Privy Council Review of Intercept as Evidence – Report to the Prime Minister and Home Secretary, 30 Jan 2008,* Cm 7324, London: The Stationery Office

18. For example; LSE Policy Engagement Network (June 2009) *Briefing on the Interception Modernisation Programme,* LSE
19. Information Commissioner's Office (August 2009) *ICO Statement on the Interception Modernisation Programme* available at: *http://www.ico.gov.uk/upload/documents/pressreleases/2009/ico_statement_imp.pdf*
20. Home Affairs Committee (June 2008) Fifth Report *A Surveillance Society?,* London: The Stationery Office
21. The Daily Telegraph (2009) 'Dame Stella Rimington: Home Office hits back at ex-MI5 chief's 'police state' warning', 17 February 2009
22. Surveillance Studies Network for the Information Commissioner (2006) *A Report on the Surveillance Society,* Information Commissioner's Office
23. Eminent Jurists Panel on Terrorism, Counter-terrorism (2009) *Assessing Damage, Urging Action,* International Commission of Jurists

£3.50