
July 2009
About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK’s leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty’s policy papers are available at

Contact

Isabella Sankey                        Anita Coles
Director of Policy                    Policy Officer
Direct Line 020 7378 5254             Direct Line: 020 7378 3659
Email: bellas@liberty-human-rights.org.uk Email: anitac@liberty-human-rights.org.uk
Introduction

1. The Regulation of Investigatory Powers Act 2000 (RIPA) is a complex piece of legislation governing surveillance by public authorities. It grants extremely broad access to highly intrusive surveillance powers for a wide array of public authorities without any judicial oversight. From the moment the Act was introduced Liberty has expressed concern over the breadth of power it contains. We take no issue with the use of intrusive surveillance powers per se. While intrusive surveillance will always engage Article 8 of the Human Rights Act 1998 (HRA)\(^1\) (right to privacy) such intrusion can be justified if it falls within the legitimate purposes set out under Article 8 (e.g. if done to prevent crime and threats to national security) and if it can be shown to be necessary and proportionate in all the circumstances. Unfortunately, broadly speaking, RIPA does not provide sufficient safeguards to meet this test. While we are pleased that the Home Office has launched this current consultation,\(^2\) we are disappointed that the consultation confines itself to a very narrow remit - proposing only minor amendments to secondary legislation. We believe that a wider-ranging consultation is required. This would include in its remit: who should authorise the use of RIPA powers, which bodies have access to such powers and for what purposes such access is available. It would also consider what further safeguards are required to ensure that RIPA complies with human rights standards. In our response to this consultation, we set out our broader concerns with RIPA. We hope that the government might consider broadening the scope of the current consultation to include these other very pressing issues.

Brief background to surveillance powers pre-RIPA

2. Until the introduction of the Interception of Communications Act 1985 there was no statutory regulation of the interception of communications (other than some specific offences regarding postal employees and interference with postal communications).\(^3\) Before 1985 the practice was for the Secretary of State to issue...

---

\(^1\) Article 8 (right to privacy) of the European Convention on Human Rights as incorporated by the HRA.


\(^3\) Section 20 of the Telegraph Act 1868 made it a criminal offence if any Post Office official "shall, contrary to his duty, disclose or in any way make known or intercept the contents or any part of the contents of any telegraphic message or any message entrusted to the [Post Office] for the purpose of transmission".
an executive warrant for interception, although there were no legal consequences if such a warrant was not obtained. The 1985 Act was introduced following a European Court of Human Rights ruling in 1984 that held that the UK was in breach of its obligations under the European Convention on Human Rights (ECHR) as interferences with the right to privacy were not covered by legislation and as such were not “in accordance with law”.\(^4\) Additionally, until 1989 the security and intelligence services were not governed by statute and the only official published details of their work was the Maxwell-Fyfe Directive (a Directive named after the Home Secretary who issued it), which set out an administrative Charter governing the Security Service’s work. The Security Service Act 1989 replaced the 1952 Directive putting MI5 on a statutory footing for the first time. The Intelligence Services Act 1994 similarly placed MI6 and GCHQ on a statutory footing, but it wasn’t until the Security Service Act 1996 that an attempt was made to define what criminal conduct could lead to the grant of an interception warrant or a warrant to enter property by the security and intelligence services.

3. In relation to intrusive surveillance (the use of electronic surveillance devices on private property, but not the bugging of telephones or interception of post), there was only Home Office guidelines to govern its use, but no statutory provision, until the advent of the Police Act 1997. This Act introduced a Code of Practice on Intrusive Surveillance that came into force in February 1999.

**Introduction to RIPA**

4. After the introduction of the HRA, RIPA was introduced in an attempt to build human rights safeguards – the tests of necessity and proportionality – in to the authorisation of surveillance. In introducing the Bill, the then Home Secretary Jack Straw MP described the Bill as “a significant step forward for the protection of human rights in this country.”\(^5\) Yet, although it was at least a step forward, as the Act attempted to remain faithful to those that had passed before it\(^6\) the result is a byzantine piece of legislation that is as confusing as it is insidious.

---

\(^4\) See Malone v UK, 1984, ECHR, Application no. 8691/79. See in particular paragraph 79 “it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive”.


\(^6\) See for example Mr Straw’s comments in introducing the Bill: “We start from the regime established by the Interception of Communications Act 1985, and we have been faithful to many of its key tenets”. Hansard HC Debs. Vol 345, col 769, 6 March 2000.
5. The Act itself is extremely complicated. The Court of Appeal has labelled it “a particularly puzzling statute” and Lord Bingham in the House of Lords has described it as “perplexing” noting that “the trial judge and the Court of Appeal found it difficult to construe the provisions of the Act with confidence, and the House has experienced the same difficulty”.

When one of the most eminent jurists in the land finds it difficult to comprehend an Act of Parliament it certainly raises very real doubts over its accessibility. This is particularly troubling given the large number of bodies that now have access to powers contained within it (as will be dealt with in more detail below). This difficulty is compounded by the fact that it has spawned an unprecedented number of statutory instruments (over 30) which must be consulted in order to fully understand the remit of RIPA’s powers.

6. A simple, and accurate, summary of RIPA is nigh on impossible, however, it may be useful to try to set out the types of surveillance covered by RIPA and the methods of authorisation and access before turning to what changes we believe need to be made. In general terms RIPA deals with five different types of surveillance, listed below in order of their apparent intrusiveness:

1. **Interception of communications:** this is usually intercepting a person’s telephone or accessing the content of a person’s private emails or correspondence. The Secretary of State must issue a warrant to authorise the interception of communications and it is a power only available to policing and intelligence services (or overseas authorities in the exercise of an International Mutual Assistance Agreement). In 2007 the Home Secretary issued 1881 interception warrants.

2. **Intrusive surveillance:** this involves covert (undercover) surveillance in residential premises or private vehicles, e.g bugging a person’s home or car. The method of authorisation is complicated but essentially the Secretary of State grants authorisation by a warrant for applications by the intelligence services, whereas senior officials in the relevant organisation authorise applications by police forces, the Serious Organised Crime Agency (SOCA), Her Majesty’s Revenue or Customs (HMRC) or the Office of Fair Trading.

---

(OFT). In non-urgent cases, a Surveillance Commissioner must approve the warrant before it becomes effective (in urgent cases a Commissioner’s approval is not required). Confusingly, if the surveillance involves entry onto private premises (i.e. to place the bug, which includes entry into office premises) or interference with wireless telegraphy, this is dealt with in respect of police under Part 3 of the Police Act 1997 (1997 Act), and in respect of intelligence services, under section 5 of the Intelligence Services Act 1994. Authorisation mechanisms under these Acts are largely similar to RIPA. In 2007-2008 there were 355 intrusive surveillance authorisations under RIPA and 2,493 property interference authorisations under the 1997 Act. The number of warrants issued to the security services is not made public.

3. **Directed surveillance**: this is covert surveillance in a public place, such as covertly monitoring the movements and actions of specific targets, e.g. following them around, covertly listening in or filming in public spaces (this does not apply to CCTV as this is visible filming, unless the CCTV is to be used to follow a specific individual). This can be self-authorised by the public authority that wishes to have access. This power is available to a wide array of public authorities including, in addition to the police and intelligence services, over 470 local authorities and numerous other agencies. In 2007-2008 law enforcement agencies obtained 18,767 directed surveillance authorisations, and other public authorities obtained 9,535 authorisations.

4. **Covert Human Intelligence Sources (CHIS)**: A CHIS is a person who, under direction from a public authority, establishes or maintains a personal or other relationship in order to (covertly) use the relationship to obtain information or disclose information gained from the relationship. This includes undercover

---

10 No definition of what constitutes an ‘urgent’ case is set out in RIPA, however, the Draft Code of Practice on Covert Surveillance and Property Interference contained in this consultation provides that a case is not normally to be regarded as urgent unless in the judgment of the person giving the authorisation, the time it would take to get the authorisation would be likely to endanger life or jeopardise the investigation or operation in question.
13 Ibid at para 7.2 and 7.3.
agents and informants. This power is available to numerous public authorities including local authorities. In 2007-2008 there were 4,498 CHIS recruited by law enforcement agencies and all other public authorities recruited 204 CHIS.\textsuperscript{14}

5. \textbf{Communications data}: this contains the record of a communication, such as a telephone call, email or website visited – it does not contain the content of the communication. There are three types of data covered by this:

(a) Traffic data: this tells you where the mobile phone, internet connection etc was located at the time the communication took place – e.g. where a mobile phone was when it received or made a call;

(b) Service use: this tells you how a communication occurred (i.e. was it via email, a text or a phone call etc), the date and time it occurred and how long it lasted;

(c) Subscriber information: this tells you any information held by the person who has signed up to the communications service, for example the name and address and any direct debit details of the user.

The power to acquire service use data and subscriber information is available to numerous public bodies, including law enforcement agencies, over 470 local authorities and around 110 other public authorities. Acquisition of traffic data is limited to bodies that show they require it to fulfil their statutory functions and local authorities have no access to it. During the year ended 2007 public authorities as a whole made 519,260 requests for communications data, with 1,707 requests made by local authorities.\textsuperscript{15}

\textbf{Authorisation of surveillance under RIPA}

\textit{Interception of communications}

7. As can be seen above, no authorisations under RIPA are made on application to a court of law. Most surveillance techniques are self-authorising, i.e. within the public body exercising the surveillance. For the highly intrusive method of

\textsuperscript{14} Ibid at para 7.4 and 7.5.
\textsuperscript{15} See the \textit{Report of the Interception of Communications Commissioner for 2007}, at paras 3.7 and 3.26.
interception of communications a warrant authorising the interception is granted by the executive. Executive authorisation of this intrusive surveillance technique is of huge concern. The failure to provide any independent judicial scrutiny of applications for such intrusive surveillance fails to provide a proper mechanism for accountability. As we said when RIPA was introduced into Parliament in 2000:

Retention of executive rather than prior judicial authorisation of interception is fundamentally objectionable. That the executive should secretly authorise itself to commit clandestine interferences with important rights is neither acceptable nor necessary. The Government has failed to advance any satisfactory case for failure to adopt a judicial procedure... Judicial involvement maintains public confidence in the investigatory framework... We consider it essential that in all cases covered by clause 5, authority to intercept should be sought from a High Court or equivalent judge.16

8. The European Court of Human Rights has stressed the importance of judicial involvement in targeted surveillance. In *Klass v Germany*17 the Court said that “in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge”. More recently in *Dumitru Popescu v Romania (no. 2)*,18 the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body’s activity. Most other States with comparable legal systems require judicial authorisation before such warrants can be authorised. In America,19 federal investigative or law enforcement officers are generally required to obtain judicial authorisation for intercepting ‘wire, oral and electronic’ communications, and a court order must be issued by a Judge of a US

---

18 No. 71525/01, § 61, 26 April 2007: 70-73, and cited with approval in *Case of Iordachi v Moldova*, 25198/02, 10 February 2009.
District Court or a US Court of Appeals.\textsuperscript{20} In Australia, law enforcement interception warrants must be issued by an eligible Judge or a nominated Administrative Appeals Tribunal judge.\textsuperscript{21} In Canada it is unlawful to intercept private communications unless the interception is in accordance with an authorisation issued by a judge,\textsuperscript{22} and in New Zealand police can only intercept a private communication in tightly prescribed circumstances, including requiring a warrant or emergency permit that can only be issued by a High Court Judge.\textsuperscript{23} It is clear then that other comparable jurisdictions require independent judicial authorisation before interception warrants can be authorised. There is therefore no reason to argue that judicial authorisation is impractical or unworkable.

9. There are real concerns over transparency and accountability with Executive warrants and the potential for conflicts of interest. As we said in our report, \textit{Overlooked}, in 2007:

\begin{quote}
There is no reason to suggest, that any Minister sets out to act in an inappropriate manner. However, the responsibilities of the Executive are diverse and potentially conflicting. There is a wider obligation to the public’s safety, to detect and prevent crime and to ensure that state enforcement agencies are able to operate effectively. This range of obligations does not necessarily lend itself to objectivity when determining whether interception is warranted in an individual case. Even if a Home Secretary were to act in a manner of absolute propriety on every occasion he or she were asked to authorise a warrant, Executive authorisation can lead to allegations of ‘rubberstamping’. Without some arm’s length independence from the authorising body, there will always be suspicions that proper protocol and safeguards are not being observed. It would be in the
\end{quote}

\textsuperscript{20} Also in America, under the \textit{Foreign Intelligence Surveillance Act} 1978, if the interception involves the acquisition of communications of any US person within the US, it must be conducted after first obtaining a court order.
\textsuperscript{21} \textit{Telecommunications (Interception and Access) Act} 1979, section 39, as amended by the \textit{Telecommunications Act} 1997. Note that Federal warrants relating to national security can be authorised by the Attorney General. See also the various States and Territories that have enacted legislation in order to make the Federal provisions applicable to State and Territory Police, see for example the \textit{Telecommunications (Interception) (State Provisions) Act} 1988 (Victoria).
\textsuperscript{22} Canada \textit{Criminal Code}, Part VI, section 186.
\textsuperscript{23} Part 11A of the \textit{Crimes Act}, and under the \textit{Misuse of Drugs Amendment Act} 1978.
interests of both the Executive and the agencies seeking authorisation if an independent judge were needed.\textsuperscript{24}

10. Issuing warrants authorising the interception of private communications is clearly a very heavy burden to place on one individual. As noted above, in 2007 the Home Secretary issued 1881 interception warrants, or over 5 a day on average (not including the number of intelligence service warrants granted for intrusive surveillance, however many that may be). By way of comparison, the total number of federal and state wiretap authorisations issued in the entire United States (by federal and state courts) in 2008 was 1891.\textsuperscript{25} How one person can effectively and properly review that number of warrants every day, in addition to his or her other highly pressing duties as Home Secretary, raises some serious questions. The former Home Secretary David Blunkett has recalled the level of pressure he was under when Home Secretary:

\begin{quote}
My whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign government warrants in the middle of the night. My physical and emotional health had cracked.\textsuperscript{26}
\end{quote}

It is clear that the exercise of such powers must be subject to a proper system of checks and balances which includes independent judicial oversight before interception warrants are authorised. Liberty has long argued that if interception is properly authorised in this way any evidence obtained through the use of intercept should be admitted as evidence in court.\textsuperscript{27} The UK is virtually the only country in the developed world to bar the use of intercept evidence, and it is hoped that this bar will soon be lifted in light of recommendations made by the Chilcot review.\textsuperscript{28} However, it

\begin{footnotes}
\textsuperscript{26} See: \url{http://www.guardian.co.uk/politics/2006/oct/07/uk.davidblunkett}
\end{footnotes}
is essential as part of these changes that such surveillance is properly authorised by judicial warrant.

Intrusive surveillance

11. Authorisations for intrusive surveillance differ according to which body is requesting access to intrusive surveillance powers. In respect of the intelligence services, authorisation must be given by a warrant issued by the Secretary of State (similar to that for interception of communications), the numbers of which are not made publically available. Requests for access by the police, SOCA, HMRC and the Office of Fair Trading can be self-authorised in urgent cases but otherwise require authorisation by a Surveillance Commissioner (being a person who holds or has held judicial office, yet they are not acting in a judicial capacity as Surveillance Commissioner). Intrusive surveillance is, as the name indicates, highly intrusive and could in fact be more intrusive than the interception of communications. The bugging of a family home, which records the conversations and movements of everyone in that home, seriously interferes with the right of all people in that home to respect for their private and family life. It is not enough, as proposed in the Draft Code of Practice, to simply require the authorising officer to make an assessment of "the risk of collateral intrusion".29 Executive authorisation, self-authorisation (in urgent cases which will allow surveillance for up to 72 hours) and even authorisation by a Surveillance Commissioner acting in a non-judicial capacity, does not provide sufficient transparency or accountability in determining whether surveillance is necessary or proportionate.

12. Yet again the UK lags behind other comparable jurisdictions in providing an appropriate accountability mechanism. America, with its constitutional protection, requires judicial authorisation for warrants to search a person's home or bug their premises.30 In New Zealand, there is legislation requiring application to a High Court judge to install and use tracking devices, which would otherwise constitute an

---

29 See paras 3.8-3.11 of the Draft Code of Practice on Covert Surveillance and Property Interference, contained in this Consultation at p 65.
30 See the Fourth Amendment: 'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' See also a report from the ACLU, Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, 2003, available at: http://www.aclu.org/privacy/gen/15162pub20030115.html#attach
unlawful trespass.\textsuperscript{31} In Australia federal and State jurisdictions have enacted legislation to require law enforcement officials to obtain a warrant from a court before using listening or video devices.\textsuperscript{32} In Canada, the Criminal Code requires a judge to issue a warrant authorising the use of any device or investigative technique or procedure which includes video surveillance and covert entry into premises.

13. Again, it is clear that there is a need for an independent judicial authorisation before intrusive surveillance should be used. For the reasons outlined above, the Home Secretary is not best placed to objectively review decisions as to when warrants should be granted. The government argues that national security grounds preclude judicial authorisation, but there are many safeguards that can be imposed in order to protect national security – as is the practice in other jurisdictions and indeed in our courts when matters of national security come before it. It is also unacceptable that law enforcement agencies can self-authorise intrusive surveillance powers in urgent cases (particularly as if it is ‘not reasonably practicable’ a person with a lesser rank can orally provide authorisation).\textsuperscript{33} There is no definition of urgent in RIPA, but the Codes of Practice provide that something could be considered ‘urgent’ if to wait would be “likely to jeopardise the investigation or operation in question”. This is a subjective assessment with no prior independent oversight and allows intrusive surveillance for up to 72 hours. Again, this should require independent judicial oversight – any urgency can surely be dealt with by out-of-hours and on-call judges. While authorisation by the Surveillance Commissioner in all other cases is preferable to that of executive or self-authorisation, this still provides concerns over transparency and accountability as the Surveillance Commissioner is not acting in a judicial capacity when authorising such warrants. We believe that all authorisations for interception of communications and intrusive surveillance should be made by judicial warrant.

\textit{Other types of surveillance}

14. The three other types of surveillance are all self-authorised and require no prior external authorisation at all. Authorisation is simply by a designated person within the organisation seeking access to surveillance. While this consultation

\textsuperscript{31} \textit{Summary Proceedings Act 1957} sections 200A to 200P (inserted in 2003).
\textsuperscript{32} See for example the \textit{Surveillance Devices Act 2004} (Commonwealth), the \textit{Surveillance Devices Act 1998} (Western Australia) and the \textit{Surveillance Devices Act 1999} (Victoria).
\textsuperscript{33} See section 34 of RIPA.
proposes increasing the seniority of the person authorising the surveillance, this still fails to provide for any independent oversight of the exercise of these powers. Most worryingly, the draft Codes on directed surveillance and the use of a CHIS contained in this consultation provide that authorising officers should *generally* not be responsible for authorising their own activities but states that it is recognised that this is not always possible, “*especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons*.” It is entirely unacceptable for a person to be allowed to self-authorise their own use of directed surveillance or recruitment of a CHIS. These covert surveillance techniques are highly intrusive and should be independently authorised. Considerations of necessity and proportionality can only be properly made by someone without any conflict, or perceived conflict, of interest. A public official within a public authority that may not exercise such powers on a regular basis is also not best placed to determine when conduct will or will not unnecessarily or disproportionately interfere with a person's right to a private and family life. There is a range of severity of intrusion within the use of such surveillance powers. Depending on the intrusiveness of the surveillance, the use of some of these powers may require authorisation by a magistrate. This would provide greater transparency and accountability, and independent consideration of issues of proportionality, without becoming a particularly convoluted process.

**Reasons for exercise of powers under RIP**

15. The circumstances in which RIP powers can be granted are broad and ill-defined. For all five types of surveillance, authorisations can be given if it is considered necessary in the interests of national security; it is for the purpose of preventing or detecting crime or of preventing disorder; or it is in the interests of (or for interception warrants: to safeguard) the economic well-being of the UK. In relation to interception of communications and intrusive surveillance this is restricted to preventing ‘*serious* crime’ and does not extend to ‘preventing disorder’. In respect of directed surveillance, the use of a CHIS and accessing communications data additional authorisations can also be given if it is considered necessary in the

34 See *Draft Code of Practice on Covert Surveillance and Property Interference* at para 5.7 and the *Draft Code of Practice on Covert Human Intelligence Sources* at para 5.7.

35 See sections 5 (interception), 32 (intrusive), 28 (directed), 29 (CHIS) and 22 (communications data) of RIP.

36 Section 81(2) and (3) of RIP and section 93(4) of the *Police Act 1997* defines serious in this context as involving violence, or the offence results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose or it is an offence for which a person could be reasonably expected to be imprisoned for three years or more.
interests of public safety, to protect public health and to assess or collect any tax, duty or other type of government charge. Communications data can also be accessed in an emergency to prevent death or to prevent or mitigate injury or any damage to a person’s mental or physical health. For directed surveillance, CHIS and communications data, the Secretary of State can make orders extending the purpose for which authorisations can be made. To date orders have only been made in relation to communications data: to allow communications data to be accessed to investigate alleged miscarriages of justice and to assist in identifying deceased persons or persons unable to identify themselves because of a physical or mental condition.\(^{37}\) The Annex to this consultation response sets out in greater detail when authorisations can be granted and for what purpose.

16. The heads under which surveillance can be authorised are unnecessarily broad and vague. No definition is given as to what is, for example, ‘in the interests of national security’ or the ‘economic well-being of the UK’. We do know, however, that the government takes an alarmingly expansive view of what may be justified in the name of the ‘economic well-being of the UK’ - we have recently seen the government argue that restricting drug-users access to welfare benefits is justified to further that aim.\(^{38}\) As there is no appropriate judicial approval given before these powers are exercised, whatever the relevant authority subjectively decides is in the interests of national security or the economic well-being of the UK is what will be used to authorise the surveillance. Human rights standards require that in the exercise of targeted surveillance there must be adequate safeguards to protect the citizen against excessive intrusion or other abuses of rights. The use of broad and vague notions such as ‘national security’ and ‘economic well-being’ gives rise to a real risk that the disproportionate use of surveillance will be authorised, going beyond what is necessary to protect the public from harm. This could interfere unacceptably with political and other lawful activity that ought to go unimpeded in a democratic society. We believe that these grounds should be better defined, particularly as the prevention or detection of crime, or serious crime, is already included which should capture the majority, if not all, of the grounds on which surveillance needs to be authorised.

---


17. The grounds for which RIPA allows surveillance have clearly been chosen as they are the main grounds on which the right to privacy under Article 8 of the HRA can be limited. However, just because they form grounds on which this right may be limited where it is necessary and proportionate to do so, this does not mean that targeted surveillance can be automatically justified for all these purposes. On the spectrum of intrusions into the private sphere, targeted surveillance is already at the more intrusive end. The less serious the need for the use of surveillance the less likely it is to be necessary and proportionate to limit the right to privacy. We also note that a number of grounds on which surveillance can be granted do not form part of the justifiable exceptions in Article 8, in particular in relation to communications data access which can be authorised to assess or collect any tax, duty, levy or other imposition, contribution or charge payable to a government department. The ability of the Secretary of State to expand the list by an order also contrasts with the prescriptive nature of Article 8. This raises serious concerns over the compatibility of RIPA powers with Article 8 of the HRA.

18. We are also concerned by the ability for so many public authorities to have access to powers of directed surveillance, the use of a CHIS or acquisition of communications data on the basis of the prevention or detection of any crime or the prevention of disorder. The notion of ‘disorder’ is obviously extremely broad and subjective and could conceivably cover pre-emptive action against those exercising their right to protest. By contrast, interception and intrusive surveillance is limited to ‘serious’ crime. What constitutes ‘serious’ crime is defined in RIPA and the 1997 Act as being an offence that involves violence or results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose or is an offence for which a person could be reasonably expected to be imprisoned for three years or more.39 This is a very broad definition of what constitutes serious crime and it is difficult to see why surveillance powers should be used against a person to detect any other type of crime. It is arguable that the use of powers of surveillance under RIPA, with their necessary interference in private life, should only be exercised in order to prevent or detect serious crimes (given the breadth of the definition of ‘serious’). The government should provide concrete examples of why such powers are needed in order to detect non-serious crimes. In making this argument we do not suggest that non-serious crimes should not be properly investigated, rather, there is a need to explain why other methods of investigation and enforcement cannot be

---

39 See section 81(2) and (3) of RIPA and section 93(4) of the Police Act 1997.
used in such circumstances. If non-serious crimes were excluded as grounds on which directed surveillance, the use of a CHIS and access to communications data could be obtained, this would arguably reduce many of the contentious decisions in relation to when it is and is not proportionate to use such surveillance powers.40 Alternatively, and perhaps more appropriately, access to such powers of surveillance should be restricted to the police and other law enforcement agencies to deal with. The powers are currently provided to a myriad of public authorities with little obvious justification.

Access to powers under RIPA

19. As already noted, the number of bodies that have access to different RIPA powers varies according to the level of intrusion. Thus, access to interception of communications powers is fairly tightly defined – limited to law enforcement agencies and the security services. Intrusive surveillance powers are broader with access additionally granted to Her Majesty’s Revenue and Customs and the Office of Fair Trading. However, access to the remaining three types of surveillance has been extended to a vast array of bodies. In respect of directed surveillance and the use of CHIS these are set out in Schedules I and II to RIPA – which has been amended by statutory instrument to include a number of other bodies. RIPA lists the police, SOCA, the intelligence services and HMRC as the bodies with access to communications data. However, this can be extended by an order made by the Secretary of State41 and numerous orders have been made extending the list of public authorities with access now granted to over 470 local authorities and to bodies as diverse as the Charity Commission, the Gangmasters Licensing Authority, NHS services and the Pensions Regulator, to name just a few.

20. In 2007-2008 only 154 local authorities made use of their powers to obtain communications data, which means that up to 300 local authorities made no use of these powers.42 The Interceptions Communications Commissioner has stated that a large number of local authorities have “struggled to achieve the best possible level of compliance with the Act and Code of Practice”, mainly because they make infrequent

40 For example, in the last 18 months we have seen these powers being used to police school catchment areas, check on owners that do not clean up after their dogs, people putting the bins out on the wrong night etc. Clearly none of which are serious offences.
41 See section 25(1) of RIPA and the definition of ‘relevant public authority’, paragraph (g), read together with section 22(3).
use of their powers and staff are not properly trained. The Chief Surveillance Commissioner has similarly said that local authorities tend to resort to covert activity as a last resort but that when they do they “have a tendency to expose lack of understanding of the legislation” and there is a “serious misunderstanding of the concept of proportionality”. He also said that the inexperience of some authorising officers is matched in many cases by poor oversight “and a tendency for Chief Executives not to understand the risks that face their authorities”. A clear example of disproportionate use is found in an authorisation given by Poole Borough Council in 2008. In this case the local authority used directed surveillance powers to track the movements of a couple and their children for up to three weeks in order to verify whether the family lived within the right school catchment area. Liberty is currently representing the family who have brought a complaint before the Investigatory Powers Tribunal arguing that the action was clearly disproportionate (and was in fact, an unlawful use of RIPA as no crime had been, or could have been suspected of having been, committed).

21. Given a clear majority of local authorities don’t use RIPA powers and that there appears to be widespread misunderstanding of the Act by those that do use it serious questions are raised as to why local authorities need access to these powers at all. Local authorities have powers to enforce a number of regulatory offences including dealing with trading standards, benefit fraud and environmental protection. While we don’t doubt that it is necessary that investigations take place to prevent or detect possible breaches of these laws, we do not consider that local authorities should have the power to covertly follow around and film suspects, to employ undercover operatives or to access data showing all information held on a person by a communications service provider, what calls they made and received, and most worryingly, which websites they have visited. This is not to say that it is never appropriate that these methods of surveillance be used against a person in order to investigate such offences. rather, it is not a power that should be given to the staff of

43 Ibid at para 3.28.
46 We are also concerned that an example has been included in the Draft Code of Practice on Covert Surveillance and Property Interference, para 3.7, example 2, part of this Consultation, at p 65, which states that fabricating a false address within a school catchment area is fraud, given it is not clear that this would constitute a ‘fraud’. We do not see that this would amount to an offence under the Fraud Act 2006, as appears to have been recognised by Harrow LBC when it dropped its prosecution of Mrinal Patel.
local authorities. Surveillance powers are inherently intrusive and offences should only be investigated in this way by trained law enforcement officers. Local authorities can continue to investigate offences under their remit using non-intrusive methods of investigation, but if surveillance is required to properly investigate an offence Liberty submits that this should be referred to the police for investigation.

22. In addition, there are a number of particular public bodies whose access to RIPA powers is questionable. The consultation lists all of the bodies which have access, and gives only a brief summary as to why such powers are deemed necessary. Thus, for example, the Ambulance Services are stated as being provided with RIPA powers for the prevention or detection of crime or disorder and use RIPA to “investigate assaults on staff, inappropriate and hoax 999 calls”.47 No explanation is given as to why the Ambulance Services need access to this power to investigate assaults on staff rather than relying on the police to investigate such assaults. It may be that the Ambulance Services need access to communications data to deal with hoax calls, for example, but not to deal with other matters that should be more properly dealt with by the police. The Charity Commission is stated as needing powers to use CHIS, directed surveillance and access communications data because it investigates “charity misconduct or mismanagement” such as fraud etc to allow the public to be confident that the money given to charities actually does go to good causes. Again, while this may be an important aim, it is difficult to see why matters cannot be referred to the police when such surveillance powers are necessary, rather than the Charity Commission exercising directed surveillance powers or going about recruiting covert intelligence sources. Additionally, the Fire and Rescue Services are listed as needing access to the three surveillance methods to take enforcement action in respect of deliberate fire setting – yet arson would seem to be a matter best investigated by the police if surveillance techniques are necessary. The list goes on and on.

23. If the government wishes to justify the use by such a disparate range of public authorities of invasive surveillance techniques it needs to more fully explain why such bodies need these powers and why it is best left with these bodies rather than the police. As indicated by two Surveillance Commissioners there is a lack of understanding of RIPA and its powers within public authorities and a lack of appropriate oversight. This cannot be remedied by simply revising a Code of

---

47 See Consultation at page 28.
Practice. Many of these powers are rarely used by such bodies and should arguably be left to law enforcement agencies where staff are better trained and more accountable. Indeed, the more powers given to public authorities, the more difficult it is for the surveillance Commissioners to have proper oversight of the exercise by each body of RIPA powers.

Other areas of concern with RIPA

Interception

24. Aside from the level at which interception of communications is authorised, we also have a number of other concerns in the application of RIPA to such powers. In particular, that the requirement to obtain a warrant to intercept communications is not required if one party to the communication consents to the interception and there is a lower level of authorisation (i.e an authorisation under intrusive or directed surveillance or the use of a CHIS).\(^48\) Why should the party who is unaware of the interception and surveillance, and whose privacy is impacted upon in just the same way as any other person whose communications are intercepted, be subjected to surveillance with lower safeguards of authorisation? We believe any interception of communications must be authorised by a judicial warrant.

25. Section 2(2) of RIPA provides that a person will only have intercepted a communication if he or she “modifies or interferes” with a telecommunications system or its operation, or monitors transmissions. The Draft Code of Practice contained in this consultation provides an example of interception that would not require an interception warrant (although would require authorisation for intrusive surveillance). It states that installation in a private car of an eavesdropping device with a microphone which records or monitors speech will not require an interception warrant even if both ends of a telephone conversation within that car are also recorded.\(^49\) This allows intrusion into personal privacy to the same extent as interference by means of interception and yet levels of authorisation are lower. This seems to be a loophole within RIPA that could easily be exploited in order to bypass current authorisation arrangements. Any intrusive surveillance that records telephone conversations and effectively acts as a form of interception should be subject to

\(^48\) See section 3 of RIPA.
\(^49\) See Draft Code of Practice on Covert Surveillance and Property Interference, para 2.10, page 59 of the Consultation.
stringent authorisation methods – requiring, as should all intrusive surveillance – authorisation by judicial warrant.

_Intrusive surveillance_

26. Similar problems exist in relation to the definition of intrusive surveillance. Intrusive surveillance is defined as not covering devices that are not actually placed in premises or vehicles unless the device “consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle”.\(^\text{50}\) This therefore allows recording, videoing, photography (i.e. using long-range lenses) etc. to be used on a target which may provide the same level of information about a person's intimate private life, but just not of the exact level of detail as a bug/camera in the premises would. Authorisation for this practice could be self-authorised by the relevant public authority (using directed surveillance). Again, there appears to be no rational policy justification as to why there should be a much lower level of authorisation when the level of interference with personal privacy is just as intrusive.

_CHIS (or 'undercover agents')_

27. The use of covert human intelligence sources by potentially hundreds of public authorities raises its own particular concerns. This technique can involve using an individual to exploit their relationship with another person to obtain information about that person which is then disclosed to the public authority. This intrusive technique raises some serious issues about entrapment and is particularly alarming given that RIPA provides that restrictions on intrusive surveillance do not apply to the conduct of a CHIS who is recording information.\(^\text{51}\) So for example, a local authority could recruit a 16 year old to spy on his or her parents, get them to covertly record conversations and film events occurring in the home, and there would be no need for any authorisation other than by an official within that authority.\(^\text{52}\) This type of surveillance, which has proved controversial even in its use by law enforcement agencies, is even more so when used by a local council. We believe

---

\(^{50}\) Section 26(5) of RIPA.  
\(^{51}\) See section 48(3) of RIPA.  
\(^{52}\) Note, the _Regulation of Investigatory Powers (Juveniles) Order 2000_, SI 2000/2793, provides that children under 16 should not be used as a source if it would be to use a relationship with his or her parent. This implicitly means that children aged 16-18 can be used to monitor their parents.
that RIPA should be amended to require that if a CHIS is going to act, in effect, as a form of intrusive surveillance, authorisation for intrusive surveillance must be first obtained. Otherwise, the low level of authorisation for the use of a CHIS could be used in order to bypass the more restrictive requirements of authorisation required for intrusive surveillance.

28. The draft Code of Practice on the use of CHIS states that directed surveillance can be used on a potential covert source before approaching them to undertake a task.53 This is surveillance of a person who may not be suspected of having been involved in any criminal activity – it is therefore difficult to see how surveillance in such circumstances can be justified (particularly by non-law enforcement agencies). The Draft Code of Practice also provides that only in the most exceptional circumstances (undefined) should a vulnerable individual be authorised to act as a CHIS. Such a person is described as being one who “is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or [be] unable to protect himself against significant harm or exploitation.”54 In such circumstances, it is difficult to envisage any situation at all in which it would be appropriate to use such a person as a covert intelligence source. Allowing authorisations in ‘exceptional circumstances’ imposes a burden on the authorising officer to make hugely sensitive judgements – judgements which in our view should not be being made at all. These are all issues the government must respond to as a matter of urgency if we are to retain public faith and confidence in our system of surveillance.

Disclosure to target

29. Section 19 of RIPA makes it an offence for state officials to disclose the existence and contents of a warrant to intercept communications. Disclosure of the use of other surveillance mechanisms is not prohibited, but nor is it required, other than to the relevant Surveillance Commissioner who must report in general terms on its use. Therefore, a person subjected to surveillance is unlikely to ever be made aware of that fact unless they are told by the relevant public authority of the surveillance. As Liberty submitted in its second reading briefing when RIPA was introduced as a Bill in 2000:

53 See Draft Code of Practice on Covert Human Intelligence Sources, para 3.26 (part of this consultation, page 105).
54 Ibid, para 4.18, and page 108 of the Consultation.
The individual’s right to complain of an infringement of rights is reduced to a matter of chance – for example, the individual might become aware of interception only after a security service leak. Scrutiny arrangements such as those envisaged by Part IV can only work effectively if those affected by interception are given notice as soon as practicable (usually after completion of the investigation) that it has been carried out.\textsuperscript{55}

If a person’s Article 8 right to privacy has been infringed, in order to have access to an effective remedy as required under human rights law, the person must first be made aware of a possible breach. This was stated by the European Court of Human Rights in \textit{Klass v Germany} in 1978 and reiterated in \textit{Weber and Saravia v Germany} in 2006:

\begin{quote}
The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see Klass and Others, cited above, pp. 26-27, § 57).\textsuperscript{56}
\end{quote}

We believe that once an investigation has been completed, or once that person is no longer under any suspicion, he or she should be notified of the relevant surveillance.

\textit{Breach of RIPA and the Investigatory Powers Tribunal}

30. It is an offence under section 1 of RIPA to intercept any communication in the UK without lawful authority. However, it is not an offence under RIPA to carry out intrusive surveillance, directed surveillance, use a CHIS or access communications data (although this may be an offence under the \textit{Data Protection Act 1998}, s 55). Therefore, the main consequence for a public authority in carrying out these types of


\textsuperscript{56} \textit{Weber and Saravia v Germany}, 2006, application 54934/2000, paragraph 135.
surveillance without authorisation is the possibility of civil action being taken against them under the Human Rights Act. However, the majority of actions taken under the HRA in respect of the use of RIPA powers \(^{57}\) must be taken before the Investigatory Powers Tribunal (IPT). While Liberty does not usually support the creation of new criminal offences given the excessive amounts of criminal law that already exists, we believe that there is a clear need to make it an offence to carry out unlawful intrusive surveillance, directed surveillance and the unauthorised use of a CHIS. Unlawful access to communications data should be an offence under RIPA, with appropriate penalties. This would then make it an offence for public authorities that act outside the law in carrying out surveillance, and would provide legal protection for the public from private investigators and those that unlawfully use surveillance mechanisms in circumstances where there is an expectation of privacy. This is essential if the state is to comply with its positive obligations under Article 8 to respect people's legitimate right to a private and family life.

31. Further, the procedure of the IPT is fundamentally flawed. The IPT is under no duty to hold oral hearings \(^{58}\) before which a person may be represented and even if it does decide to hold a hearing (purely at its discretion) all of the Tribunal’s proceedings, including the oral hearings, must be conducted in private. \(^{59}\) RIPA itself provides that, subject to any rules made by the IPT, the IPT can only notify the complainant whether they have won or lost. \(^{60}\) Rules made in 2000 provide that if the IPT finds in the complainant’s favour the IPT must provide him or her with a summary of their determination, including findings of fact. Note, however, that this is merely a summary of the determination and if a complainant loses no reasons at all will be given. Most astoundingly, there is no right of appeal from the IPT. Section 67(8) of RIPA provides that rulings by the IPT are not subject to appeal and cannot be questioned in any court, unless the Secretary of State orders otherwise. Section 67(9) provides that it is the duty of the Secretary of State to make such orders in relation to most categories of proceedings and complaints, yet no such orders have yet been made. This is because despite most of section 67 being brought into force in October 2000, subsection 67(9) has never been brought into force. This effectively means that in most cases in which a person seeks to argue

---

\(^{57}\) See section 65 of RIPA that essentially requires a person who has an HRA complaint in respect of interception of communications or access to communications data to go to the IPT, and to also go before the IPT in respect of the other three types of surveillance if the action is against the intelligence services, the armed forces, the police, SOCA or HMRC.


\(^{59}\) See rule 9(6), ibid.

\(^{60}\) See section 68(4) of RIPA.
that a public authority has used unlawful surveillance against them, they are required to bring proceedings before the IPT, which must hold proceedings in secret, may not hold an oral hearing, will not give proper reasons for its findings and which there is no right of appeal. This is arguably a breach of Article 6 of the HRA itself which requires a fair and public hearing, and the right under Article 13 of the ECHR to an effective remedy. These provisions should be overhauled as a matter of urgency in order to provide an appropriate mechanism for the independent determination of any complaints regarding the lawfulness of surveillance methods. How can the public have any confidence in a process which is held in secret, gives little or no reasons for its decisions and whose judgment cannot be brought into question in any court of law?

**Conclusion**

32. As already stated, we believe this consultation should have a much broader remit to consider properly all of the issues raised above. Instead, and disappointingly, the consultation merely seeks to tinker around the edges rather than propose a long-term workable solution. While we welcome changes to the level of authorisations within public authorities, substantial changes need to be made to the manner in which authorisations are made. We note that the consultation does ask whether any public authority should be removed from the RIPA framework. Yet, as already explained, without proper descriptions and explanations as to why the government believes surveillance powers are required for each public authority it is difficult to specify which public authorities should have their access to RIPA powers removed. There appear to be very compelling arguments to remove local authorities from those that have access to such powers. However, if there were restrictions on when surveillance powers could be used (i.e. only for serious crimes) or greater regulation of authorisation processes, this may be less necessary. In the absence of a more substantial review of RIPA we argue that local authorities are not best placed to have access to covert surveillance powers. As recent controversy over local authority use of RIPA has demonstrated, the British public do not expect to be spied

---

61 As indicated by the Questions to the Parties to *Kennedy v UK* (application no. 26839/05) currently before the European Court of Human Rights. The Court has asked the UK government to answer whether the proceedings before the IPT, taking into account the absence of the right of appeal, constituted a fair hearing within the meaning of Article 6 and whether the applicant had an effective remedy for any breach of Articles 6 and 8 under Article 13.

62 At the very least section 67(9) should be brought into force and orders made under it allowing such appeals.
on by staff from their local council, especially not for minor regulatory offences. The same applies to many of the other numerous public bodies that have access to these powers. Unless the government can establish the clear necessity for such bodies to have access to surveillance, other than for mere convenience, there should be a radical overhaul of the bodies with access. It is impossible for us to say however, with the limited information provided in this consultation, as to which of these bodies do or do not need these powers. Without such information it is unreasonable to ask respondents to the consultation which public authorities should be removed and if so, what “alternative tools should they be given to enable them to do their jobs”.

33. Further, the consultation proposes adding or removing grounds on which surveillance can be authorised by particular bodies without any proper explanation being given. For example, it is proposed that Immigration Removal Centres should be given the powers of directed surveillance and the conduct and use of CHIS. No reason is given as to why this might be necessary. Suffice to say that this is certainly not the moment to be extending the number of bodies with access to RIPA powers or the powers each body has access to. A full and proper consultation, giving appropriate levels of information to respondents, is essential if the Home Office wishes to properly engage and “get the balance right between supporting law enforcement and respecting privacy”. The limitations of this consultation mean that it is unlikely that such a balance will be properly achieved without a more radical overhaul of RIPA.

Anita Coles

---

63 See questions 1 and 2 of the government’s Consultation.
64 See page 41 of the Consultation.
65 See the (now former) Home Secretary’s Foreword to this Consultation.
ANNEXURE
WHEN AUTHORISATIONS FOR SURVEILLANCE CAN BE MADE

<table>
<thead>
<tr>
<th>When authorisation is necessary</th>
<th>Type of surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the interests of national security</td>
<td>All 5 types of surveillance</td>
</tr>
<tr>
<td>For the purpose of preventing or detecting serious(^{66}) crime</td>
<td>Interception of communications</td>
</tr>
<tr>
<td></td>
<td>Intrusive surveillance</td>
</tr>
<tr>
<td></td>
<td>Property interferences under the 1997 Act (i.e. bugging a house by the police)</td>
</tr>
<tr>
<td>For the purpose of preventing or detecting any crime or preventing disorder</td>
<td>Directed surveillance</td>
</tr>
<tr>
<td></td>
<td>CHIS</td>
</tr>
<tr>
<td></td>
<td>Communications Data</td>
</tr>
<tr>
<td>For safeguarding the economic well-being of the UK</td>
<td>Interception of communications</td>
</tr>
<tr>
<td>In the interests of the economic well-being of the UK</td>
<td>Intrusive Surveillance</td>
</tr>
<tr>
<td></td>
<td>Directed surveillance</td>
</tr>
<tr>
<td></td>
<td>CHIS</td>
</tr>
<tr>
<td></td>
<td>Communications Data</td>
</tr>
<tr>
<td>To give effect to an international mutual assistance agreement to prevent or detect serious crime</td>
<td>Interception of communications</td>
</tr>
<tr>
<td>In the interests of public safety</td>
<td>Directed surveillance</td>
</tr>
<tr>
<td></td>
<td>CHIS</td>
</tr>
<tr>
<td></td>
<td>Communications Data</td>
</tr>
<tr>
<td>For the purpose of protecting public health</td>
<td>Directed surveillance</td>
</tr>
<tr>
<td></td>
<td>CHIS</td>
</tr>
<tr>
<td></td>
<td>Communications Data</td>
</tr>
<tr>
<td>For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department</td>
<td>Directed surveillance</td>
</tr>
<tr>
<td></td>
<td>CHIS</td>
</tr>
<tr>
<td></td>
<td>Communications Data</td>
</tr>
<tr>
<td>In an emergency, to prevent death or prevent or mitigate injury or damage to a</td>
<td>Communications Data</td>
</tr>
</tbody>
</table>

\(^{66}\) Section 81(2) and (3) of RIPA and section 93(4) of the Police Act 1997 defines serious in this context as involving violence, or the offence results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose or it is an offence for which a person could be reasonably expected to be imprisoned for three years or more.
<table>
<thead>
<tr>
<th>person’s physical or mental health</th>
<th>To assist investigations into alleged miscarriages of justice&lt;sup&gt;67&lt;/sup&gt;</th>
<th>Communications Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To assist in indentifying a person who has died or is unable to identify him or herself because of a physical or mental condition (other than one resulting from crime), or to obtain information regarding next-of-kin&lt;sup&gt;68&lt;/sup&gt;</td>
<td>Communications Data</td>
</tr>
</tbody>
</table>

<sup>67</sup> See SI 1878/2006.

<sup>68</sup> Ibid.