UNITED KINGDOM

The Regulation of Investigatory Powers Bill

An Open Letter by Amnesty International to Members of the House of Lords

This document contains an Open Letter by Amnesty International which has been sent to members of the House of Lords on 13 June 2000. The new Bill is presently being considered by the House of Lords.

Amnesty International's monitoring of the human rights situation in the United Kingdom has revealed that existing practices involving surveillance and undercover operations have resulted in human rights violations by law enforcement officials. The organization is concerned that this draft legislation, the Regulation of Investigatory Powers (RIP) Bill, while expanding the scope of permissive surveillance, fails to provide sufficient safeguards to ensure accountability and protection of human rights.

The RIP Bill, which is currently before the House of Lords, if passed, could lead to violations of fundamental human rights, enshrined in the European Convention and other human rights treaties to which the UK is a party. Amnesty International agrees with other NGOs -- including Liberty, Justice and Foundation for Information Policy Research -- in many of their detailed criticisms and suggested amendments to the draft legislation. Amnesty International believes that the provisions, if applied, will violate individuals' rights to privacy and fair trial and may have a chilling effect on the non-violent exercise of fundamental rights of freedom of expression and association.

Furthermore, Amnesty International is writing to you in order to express concern that provisions in the draft legislation, if applied, could undermine the effectiveness of organizations such as Amnesty International in defending human rights and victims of human rights violations throughout the world. Some provisions would impact Amnesty International's ability to communicate confidentially with victims of human rights violations (both in their countries and in the UK in relation to the refugee determination process); they would also impact the confidentiality of communications between the International Secretariat of Amnesty International in London and its sections and affiliated groups throughout the world.

The RIP Bill legalises a variety of intrusive surveillance techniques: the bugging of homes, cars, etc; the covert use of informants and undercover officers; powers for a wide variety of agencies and government departments to undertake covert surveillance; and the interception of communications. The Bill is fundamentally flawed, because it does not contain sufficient safeguards against misuse, and does not take human rights or civil liberties sufficiently into account. The Bill has four main parts. The first deals with the interception of communications; the second covers surveillance and covert human intelligence sources; and the third deals with encryption. The fourth part outlines a

regulatory mechanism for scrutiny of investigatory powers and of the functions of the intelligence services.

According to the Bill, the interception of communications is restricted to investigations in the interests of national security, for safeguarding the economic well-being of the UK, or for preventing or detecting serious crime. Amnesty International is concerned that the Bill does not provide a definition of national security and that therefore it can be open to abuse. In addition, the definition of serious crime includes "conduct by a large number of persons in pursuit of a common purpose", which means that surveillance could be extended indiscriminately to participants in legitimate collective activity. Amnesty International is concerned that these provisions could lead to the targeting of people for exercising their rights to freedom of association and expression.

PART I

Part I, which is entitled "Interception of Communications", gives the Home Secretary -- rather than a court -- the power to authorise a warrant requiring the interception of any form of communication, including e-mails, faxes and pagers, and which could also include interceptions of private telecommunications systems. It also deals with communications data. The Bill also provides for interception -- without judicial supervision and without warrant -- in relation to covert investigations, prisons and secure hospitals, among others.

Amnesty International considers that the power of authorisation should not be in the hands of the executive, but rather that such power should be in the hands of the judiciary: "it is argued that a member of the executive lacks the necessary independence to authorise interception by a state agency ... a senior judge would be a more appropriate arbiter of the balance between the rights of the individual and the interests of the state". (Justice, Second Reading Briefing) The European Court of Human Rights, as in the case of Klass v Germany, has stressed the importance of judicial oversight as a safeguard for surveillance operations.

Under this legislation, Internet Service Providers (ISPs) will have to build "interception capabilities" into their systems, so that when served with a warrant they will be forced to intercept private e-mail messages and convey the contents to police or intelligence officers; refusal to comply with this warrant could lead to a term of imprisonment of up to two years. The person at the ISP, in whose name the warrant is issued to place an intercept, is liable to five years' imprisonment for "tipping off" the client or any third party about the intercept.

Internet service providers and other telecommunications providers could also be required to disclose "communications data" (which means data indicating all addresses of a person's Internet communication). Designated officials in any public authority may also authorise themselves to obtain such data directly. Once the RIP Bill becomes law, ISPs will be required to install a black box -- which would be linked to a central monitoring facility currently being installed in MI5's headquarters -- and which would allow the security services to monitor all Internet traffic. This new mass surveillance facility is called the Government Technical Assistance Centre (GTAC). This would enable MI5 to identify the pattern of individuals' Internet connections by monitoring logs of the websites accessed, which would provide knowledge of the pages downloaded, the addresses of email contacts, the discussion groups accessed, etc.

Under law currently in force in the UK, evidence obtained through interception of communications is prohibited from being used in criminal proceedings. The RIP Bill, however, if enacted, will allow for the disclosure of this material by the prosecution but only to the trial judge. There is no provision for the disclosure of this evidence to the defence. This provision undermines an individual's right to a fair trial under Article 6 of the European Convention because it undermines the right to present a defence and the principle of the equality of arms. This material should be the subject of ordinary disclosure rules in criminal proceedings.

Another of the provisions of great concern is the exchange, with foreign governments' agencies, of the fruits of interception. Information passed on by British police authorities could be used by governments to target people engaged in the peaceful exercise of fundamental internationally recognized human rights of freedom of speech and association, including human rights defenders. This bill allows for interception from the UK of "communications of subjects on the territory of another country according to the law of that country" at the request of the "competent authority" in that country. No limits are placed on the use of such intercepted material. It also covers intercepting communications (post and telecommunications) at the request of a non-UK state or agency under an international mutual assistance agreement. Amnesty International is concerned that these provisions could potentially violate the rights to life and to liberty of people for exercising their human rights, including human rights defenders and prisoners of conscience.

Part II

Part II provides the framework for authorising three forms of covert surveillance: directed surveillance, intrusive surveillance, and the use and conduct of covert human intelligence sources (informers, agents and undercover officers). Justice has raised concerns that some of the powers in direct and intrusive surveillance, because of how they are defined and

controlled, may be in contravention of Article 8 of the European Convention. These powers, once again, are not subject to any form of judicial authorization. The mechanism of a Covert Investigations Commissioner would appear to be nominal unless it were to be specified, within the legislation, that each agency, which has authorised surveillance, is required to report their activities to the Commissioner. No one can have effective oversight of activities of which they are unaware.

This part of the bill also places the use and conduct of informers and undercover officers under statutory control. However, Amnesty International is concerned that the safeguards to control and scrutinize the legality and necessity of the use of covert human intelligence sources are inadequate. Amnesty International has for years been concerned about the operations of undercover law enforcement officers in Northern Ireland because of evidence that such operations were not subject to any form of scrutiny and that officers who broke the law have not been brought to justice, including officers who may have colluded in murder. Therefore Amnesty International is concerned that the proposals in the bill for internal, executive authorisation (self-authorisation) do not provide an adequate safeguard to ensure that such activities are lawful and are being regularly monitored. Indeed the self-authorisation and the lack of judicial supervision perpetuates the existing lack of effective control and scrutiny.

Part III

Part III f the Bill gives the authorities unprecedented powers to compel the disclosure of keys to enable intelligence and law enforcement officials to read communications, which have been "encrypted" (i.e. coded) in order to maintain confidentiality. The interception of such confidential communications may be a serious invasion of privacy, under Article 8 of the European Convention, as well as a potential risk to the security of people who have been victims of human rights violations or who may be vulnerable because of their activities as human rights defenders. It may also deter people from transmitting information about human rights violations, including authorities' involvement in abuse. These provisions risk undermining the work of Amnesty International and other non-government organizations in working for the protection of human rights.

Under this provision, an individual within the service provider will be served with a written notice compelling that person to disclose the "encryption key". The notices can be served on "anyone there are reasonable grounds for believing" that they have the encryption key. If the person on whom the notice has been served refuses or is unable to reveal the key, that person faces two years' imprisonment. The onus is on the person, who was served with the notice, to prove that they do not have the key - this provision shifts the burden of proof from the prosecution to the defence by basing the proof of a criminal case on a fundamental element of the offence. Amnesty International considers

that this violates the rights to a fair trial and the presumption of innocence. In addition, people face five years' imprisonment for revealing that they have been required to supply an encryption key, even if their actions are based on conscientiously-held beliefs.

Part IV

This section deals with oversight and the complaints mechanism. The additional areas of covert surveillance will be added to the tasks of oversight of the four existing Commissioners (the Interception of Communications Commissioner, the Security and Intelligence Committee, the Surveillance Commissioner and the Covert Investigations Commissioner). However, the powers of the oversight Commissioners are not adequate to make them a real safeguard against abuse of power. For example, the Interception of Communications Commissioner cannot effectively oversee the working of the provisions concerning communications data if the Commissioner does not have to be notified of each authorisation. It is also difficult to see how the Interception of Communications Commissioner could supervise the operation of the "black-boxes".

The bill provides for a single Tribunal to hear all complaints in relation to surveillance conduct, including that of the intelligence services. A complaints mechanism cannot be effective, if a person is unaware that their communications have been intercepted or that they have been under any form of surveillance. According to Justice, legislation in other countries provides for some form of notification after the event, subject to police investigations not being prejudiced. Consideration should be given to providing some form of such notification. In addition, for the Tribunal to be effective, its functioning and procedures must be transparent and in accordance with Article 6 of the European Convention, which means that the complainant must have a hearing, must have access to relevant information and must be given reasons as to why their complaint has or has not been upheld. A Tribunal which does not have the above attributes does not inspire any confidence that it will ensure that the agencies, engaged in surveillance or interception, will be held accountable for their conduct.

In conclusion, Amnesty International is concerned at the implications of this legislation for the protection of human rights. The organization urges you to amend the legislation in order to ensure that it will incorporate effective safeguards, including judicial supervision of or authorisation of interception and surveillance operations, in order to protect people's fundamental rights to life, liberty, fair trial, freedom of expression, freedom of association, and privacy.

KEYWORDS: CONSTITUTIONAL CHANGE1 / FREEDOM OF EXPRESSION1 / FREEDOM OF ASSOCIATION / LEGISLATION / TELECOMMUNICATIONS / SURVEILLANCE / IMPUNITY / ECHR