These notes refer to the Regulation of Investigatory Powers Act 2000 (c.23) which received Royal Assent on 28 July 2000

REGULATION OF INVESTIGATORY POWERS ACT 2000

EXPLANATORY NOTES

OTHER AUTHORISATIONS

229. Sections 41 and 42 also relate to intrusive surveillance authorisations, but deal with those granted by the Secretary of State.

Section 41: Secretary of State authorisations

230. *Subsection (*1) provides that the Secretary of State shall not grant such authorisations unless an application is made by a member of the intelligence agencies (Security Service, Secret Intelligence Service and GCHQ), an official of the Ministry of Defence, the Armed Forces, or a specified individual within a public authority designated for this purpose by order of the Secretary of State (*subsection (3)*). Such an order would be subject to the affirmative procedure. For these purposes, the three service police forces are not treated as members of the armed forces (*subsection (7)*); instead, their use of intrusive surveillance is regulated, in the same way as other police forces, by sections 33 to 40.

231. The effect of *subsection (2)* is that authorisations will only be granted to an official of the Ministry of Defence or a member of the Armed Forces, where it is necessary in the interests of national security or for preventing or detecting serious crime.

232. This section also provides the power for the Secretary of State to impose, by order, restrictions on designated public authorities for the carrying out of intrusive surveillance, on the circumstances in which, or the purposes for which, such authorisations may be granted, and on the persons who can make such an application.

Section 42: Intelligence services authorisations

233. Where the Secretary of State grants an authorisation to one of the intelligence services under this Part (which will be for intrusive surveillance, or intrusive surveillance combined with directed surveillance), the authorisation will take the form of a warrant. This is consistent with section 5 of the Intelligence Services Act 1994.

234. *Subsection (2)* provides that a single warrant may combine an authorisation for intrusive surveillance with an intelligence services warrant (defined in subsection (6): a property warrant under section 5 of the Intelligence Services Act 1994).

235. In addition to the requirements in section 32, *subsection (3)* limits SIS and GCHQ to obtaining a warrant for intrusive surveillance in the British Islands to investigations carried out in the interests of national security or the economic well-being of the UK. *Subsections (4) and (5)* enable the Security Service to act on behalf of SIS and GCHQ in applying for and granting any authorisation in connection with a function of SIS or GCHQ, provided that SIS or GCHQ would have the power to act in that way, and provided that it does not relate to the functions of SIS or GCHQ in support of the prevention or detection of serious crime.

Grant, renewal and duration of authorisations

Section 43: General rules about grant, renewal and duration

236. This section sets out the general rules for authorisations, including their granting, renewal, and duration.

237. *Subsection (1)* provides that, in urgent cases, an authorising officer may give an oral authorisation. All other authorisations must be in writing.

238. A single authorisation may be given, combining two or more authorisations under this part. When this occurs, the provisions of this Part which relate to one type of activity only shall apply to those parts of the authorisation which authorises that type of activity. Further provisions for combined authorisations are in section 33(5), 42(2) and 44(7).

239. Oral authorisations and those granted by officers entitled to act in urgent cases in the absence of the authorising officer or his designated deputy will expire after 72 hours, beginning with the time when the grant or renewal of an authorisation takes effect.

240. Except where granted or renewed orally or by an officer entitled to act in urgent cases, authorisations for the conduct or the use of covert human intelligence sources will last for 12 months, beginning with the day on which the grant or renewal takes effect.

241. In all other cases (except those made under the special provisions for the intelligence services contained in section 44), the authorisation will last for 3 months, beginning with the day on which the grant or renewal takes effect.

242. *Subsection (4)* provides that an authorisation may be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation of the same type. The same conditions attach to a renewal of surveillance as to the original authorisation. However, before renewal of an authorisation for the use or conduct of a covert human intelligence source, *subsection (6)* requires there to be a review of the use made of that source, the tasks given to that source and the information so obtained.

243. *Subsection (8)* enables the Secretary of State, by order, to provide that certain authorisations will cease to have effect after a shorter period of time than is otherwise provided for.

244. *Subsection (9)* clarifies the time from which a grant or renewal of an authorisation takes effect. It synchronises the duration of authorisations with those given for interference with property.

Section 44: Special rules for intelligence services authorisations

245. This section sets out special provisions in relation to authorisations granted to or by the intelligence services.

246. Under *subsection (1)*, a warrant for intrusive surveillance or a renewal of such a warrant will not be issued except under the hand of the Secretary of State. However, in an urgent case, where the Secretary of State has personally authorised it, a warrant can be signed (but not renewed) by a senior official. This is the same urgency procedure as is provided in section 7(2)(a) for interception. Where this has happened, such a warrant will cease to have effect at the end of the second working day following its issue, unless renewed under the hand of the Secretary of State.

247. *Subsections (4) and (5)* relate to the authorisation of warrants for the intelligence services and for the authorisations and renewal of authorisations for directed surveillance where the authorisation is necessary in the interests of national security or in the interests of the economic well-being of the UK. Such warrants or authorisations last for a period of six months. Where this is a renewal, the period will start on the day when the previous authorisation or warrant would have expired. This is consistent with the provisions of the Intelligence Service Act 1994.

248. *Subsection (6)* enables the Secretary of State, by order, to provide that certain authorisations will cease to have effect after a shorter period of time than is otherwise provided for.

Section 45: Cancellation of authorisations

249. *Subsection (1)* sets out when the person who granted or renewed an authorisation must cancel it.

250. *Subsection (2)* sets out who else is responsible for cancelling the authorisation eg the person who would have granted it if it had not been an urgent case or been granted by a deputy. However, an authorising officer's deputy (defined in *subsections (6) and (7))* is also under a duty to cancel an authorisation in those cases where he would have had the power to grant the authorisation on the authorising officer's behalf.

251. *Subsections (4)* and (*5)* provide for the Secretary of State to make regulations setting out how the duty for cancelling authorisations should be performed where the authorising officer is no longer available, and on whom such a duty should fall.

Section 46: Restrictions on authorisations extending to Scotland

252. This section prevents the granting or renewal of an authorisation under this Part for activity by a public authority in Scotland if all the conduct authorised is likely to take place in Scotland, unless the authorisation is one for which the Act is (under subsection (2)) the relevant statutory provision. Thus it does not prevent:

- those seeking authorisation on the grounds of it being in the interests of national security or the economic well-being of the UK;
- the intelligence agencies;
- the Ministry of Defence, the Ministry of Defence Police or HM Armed Forces;
- Customs and Excise;
- the British Transport Police; or
- any other public authority named by order as having authority for all parts of the UK;

from obtaining an authorisation under this Act notwithstanding that all the conduct might take place in Scotland.

Supplemental provision for Part II

Section 47: Power to extend or modify authorisation provisions

253. The Secretary of State may, by order, change the types of activities which fall within the category of directed surveillance by providing that a type of directed surveillance will be treated as intrusive surveillance. Furthermore, he may, by order, provide that additional types of surveillance, which are not at present defined as directed or intrusive surveillance in section 26, will be covered by the Act and become capable of being authorised under Part II.

Section 48: Interpretation of Part II

254. This section gives interpretations for the terms used in this Part. Amongst other things, it gives an interpretation for "surveillance" and clarifies that this does not include references to:

- the use of a recording device by a covert human intelligence source to record any information obtained in the presence of the source (*subsection (3)(a) and (b)*);

- activity involving interference with property or wireless telegraphy which requires authorisation or warrant under section 5 of the Intelligence Services Act 1994 or Part III of the Police Act 1997 (subsection (3)(c).

Part Iii: Investigation of Electronic Data Protected by Encryption Etc

Section 49: Notices requiring disclosure

255. This section introduces a power to enable properly authorised persons (such as members of the law enforcement, security and intelligence agencies) to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information which they lawfully hold, or are likely to, in an intelligible form.

Intelligible is defined in section 56(3)

256. *Subsection (1)* limits the information to which this power to serve notices applies. It does so by defining the various means by which the protected information in question has been, or is likely to be, lawfully obtained. By way of illustration, this could be material:

- seized under a judicial warrant (e.g. under the Police and Criminal Evidence Act 1984 (PACE));
- intercepted under a warrant personally authorised by the Secretary of State under Chapter I of Part I of this Act;
- lawfully obtained under an authorisation given under Chapter II of Part I or Part II of this Act;
- lawfully obtained by an agency under their statutory functions but not under a warrant (e.g. under the Customs and Excise Management Act 1979); or
- which has lawfully come into the possession of an agency but not by use of statutory functions (e.g. material which has been voluntarily handed over).

257. *Subsection (2)* states that persons with the "appropriate permission" (see Schedule 2) may serve a notice imposing a disclosure requirement in respect of the protected information in question if there are reasonable grounds for believing:

- that the key to the relevant protected information is in the possession of the person on whom the notice is being served;
- that serving a notice imposing a disclosure requirement is necessary for the reasons set out in subsection (3), or necessary for securing the effective exercise or proper performance of any statutory power or duty of a public authority;
- that imposing a disclosure requirement is proportionate to what is sought to be achieved by doing so; and
- that an intelligible version of the relevant protected information cannot be obtained by any other reasonable means.

key is defined in section 56(1)

possession of a key is defined in section 56(2)

258. *Subsection (4)* explains the format which notices must take.

259. The effect of *subsections (5) and (6)* is that, where applicable, notices must be served on a senior officer within a corporate body or firm.

Senior officer is defined in section 49(10)

260. *Subsection (7)* states that the requirement in subsections (5) and (6) does not apply where there are special circumstances to the case which mean that the purposes for which a notice is given would be defeated if it was served on a senior officer in an organisation (e.g. where that senior officer is a suspect in a criminal investigation).

261. *Subsection (8)* specifies the persons to whom a disclosure may be made by the recipient of a notice.

262. *Subsection (9)* ensures that a key which has been used solely for the purpose of generating electronic signatures does not have to be disclosed in response to a notice.

electronic signature is defined in section 56(1)

263. The effect of Schedule 2, which is introduced by s*ubsection (11)*, is to set authorisation levels (described in Schedule 2) for permission to serve a notice under section 49. The level of authority required will vary depending on the power under which the protected information was, or is likely to be, lawfully obtained.

Section 50: Effect of notice imposing disclosure requirement

264. This section explains the effect of serving a notice imposing a disclosure requirement in various circumstances.

265. *Subsection (1)* applies where a person has, at the time a notice is served, possession of the relevant protected information and a means of accessing it and of disclosing it in an intelligible form. This means that they have the password, in the case of material protected by a password; or the decryption key in the case of encrypted material; or both, in the case of material protected in both ways. In these circumstances, the effect of imposing a disclosure requirement is, first, that the recipient of a notice may use any key in their possession to access the information or to put it into intelligible form; and, second, that they must disclose it in accordance with the terms of the notice.

266. *Subsection (2)* allows a person who is required to disclosure information in an intelligible form to instead disclose a relevant key if they so choose to do so.

267. The effect of*Subsection (3)* is that where a notice is served on a person who does not have the relevant protected information in their possession; or cannot access the information without use of a key which is not in their possession; or the notice contains a direction that a key must be disclosed (as to which, see section 51), that person must disclose any key to the information that is in their possession at a relevant time. But this duty is qualified by subsections (4) to (6).

268. The Act does not prevent the person giving a section 49 notice from giving the recipient access to the protected information, in order to allow then to produce plain text rather than disclose a key.

Relevant time is defined in section 50(10)

269. The effect of *Subsections (4) and (5)* is that where a person served with a notice is entitled or obliged to disclose a key, they need only provide those keys which are sufficient to access the relevant information and to put it into intelligible form. And *Subsection (6)* further provides that such a person may choose which keys to provide, so long as they suffice to access the information and render it intelligible.

270. *Subsection (7)* requires a person served with a notice to disclose every key to the relevant protected information that is in their possession, subject to the provisions in subsections (5) and (6). It means that a person need only provide those keys which suffice to access the information and render it intelligible, and that they may choose which keys to provide to achieve that end.

271. The effect of Subsection (8) is that where a person served with a notice no longer possesses a key to the relevant protected information, they are to disclose all information that is in their possession that would facilitate the discovery of the key.

Section 51: Cases in which key required

272. This section sets out the extra tests to be fulfilled if a key is required to be disclosed rather than the disclosure of protected information in an intelligible form.

273. *Subsection (1)* states that a notice may not contain a statement that it can be complied with only by disclosing a key unless a direction to this effect has been given by the person giving permission for the notice to be served.

274. The effect of *Subsections (2) and (3)* is that a direction that a key must be disclosed given by the police, HM Customs and HM Forces must be given expressly by a person of the rank set out in this subsection (namely, Chief Officer of police or equivalent).

275. *Subsection (4)* provides that a person may only give a direction requiring the disclosure of a key if he believes that there are special circumstances to the case making this necessary; and that giving such a direction is proportionate to what is sought to be achieved by doing so.

276. *Subsection (5)* specifies that in deciding whether it is proportionate to require that a key be disclosed, consideration must be given to the sort of other information also protected by the key in question and any potential adverse impact on a business that might result from requiring that a key be disclosed.

277. The effect of *Subsections (6) and (7)* is that any direction to disclose a key given internally by the police, HM Customs or HM Forces must be notified, within 7 days, to the Intelligence Services Commissioner or the Chief Surveillance Commissioner, as appropriate.

Section 52: Arrangements for payments for disclosure

278. This section allows for payment arrangements to be made in order to compensate persons required to disclose information following service of a notice under section 49.

279.

Section 53: Failure to comply with a notice

280. This section creates an offence of failing to comply with the terms of a notice served under section 49.

281. *Subsection (1)* states that a person served with a notice is guilty of an offence if he knowingly fails to comply with the disclosure requirement contained in that notice.

282. The effect of *Subsections (2) and (3)* is that in proceedings against a person for an offence under this section, where it is shown that a person has been in possession of a key, that can lead to a conviction, but only if the person fails to raise some doubt as to whether he still had the key when the notice was given.

283. *Subsection (4)* allows a defence to a person who shows that it was not practicable to comply with the disclosure requirement placed upon him by the time he was required to do so but that he did what was required as soon as was reasonably practicable.

284. *Subsection (5)* specifies the maximum sentence for the offence of failing to comply with a notice. As regards financial penalties, there is no upper limit to fines set in the Crown Court (on conviction on indictment). In a Magistrates Court (on summary conviction) the maximum fine is £5,000.

Section 54: Tipping-off

285. This section creates an offence where the recipient of a notice (but only one which explicitly contains a secrecy requirement), or a person that becomes aware of it, tips off another that a notice has been served, or reveals its contents. This is designed to preserve, where necessary, the covert nature of an investigation by, for example, a law enforcement agency. It outlines various statutory defences.

286. *Subsection (1)* limits this offence to occasions where the notice served explicitly demands secrecy.

287. *Subsection (2)* specifies that the inclusion of a secrecy requirement in a notice must be authorised by the person giving permission for such a notice to be served (or where such a person has himself permission to serve a notice - e.g. a Superintendent in certain cases).

288. *Subsection (3)* places restrictions on the instances when such a requirement may be imposed.

289. *Subsection (4)* specifies the maximum sentence for the tipping-off offence. On conviction in the Crown Court, the maximum term of imprisonment is five years. The financial penalties are as for the offence set out in section 53.

290. *Subsection (5)* provides a defence where the tipping-off occurred entirely as a result of software designed to give an automatic warning that a key had been compromised and where, in addition, the defendant was unable to stop this from taking place after receiving the notice.

291. *Subsections (6)* and *(7)* provide a defence where a disclosure is made to or by a professional legal adviser as part of advice about the effect of the provisions of this part of the Act given to a client or his representative; or where a disclosure was made by a legal adviser in connection with any proceedings before a court or tribunal.

292. The effect of *Subsection (8)* is that the protection in Subsections (6) and (7) will not apply where a professional legal adviser tips off a client with a view to furthering any criminal purpose.

293. *Subsection (9)* provides a statutory defence where the disclosure is made to a Commissioner or authorised by:

- a Commissioner;
- the terms of the notice;
- the person who gave the notice, or someone on his behalf; or
- a person who is in possession of the data to which the notice relates, as described in section 49.

294. The effect of Subsection (9) is to ensure that, for example, persons within an organisation may be informed about a notice in order to give effect to the notice (e.g. accessing a key or plain text) without this falling foul of the tipping off offence.

295. *Subsection (10)* provides a statutory defence for a person told about a notice but not about the fact that there was a requirement for secrecy.

Section 55: General duties of specified authorities

296. This section describes the safeguards that must be in place for the protection of any material (e.g. a decryption key) handed over in response to the serving of a notice under this Act.

297. *Subsection (1)* ensures that the safeguard requirements apply to all those who may have responsibility for organisations that will handle material provided in response to a written notice. In the case of the security and intelligence agencies for example, this will mean the Secretary of State.

298. *Subsection (2)* places an onus on those identified to ensure that:

- any material disclosed is used only for a purpose for which it may be required;
- the uses to which the material is put are reasonable;
- the use and any retention of the material are proportionate;
- the requirements of subsection (3) are complied with;
- that keys are stored in a secure manner; and
- the material is destroyed as soon as it is no longer needed.

299. *Subsection (3)* specifies that the material is shared with the minimum number of people possible.

300. *Subsection (4)* imposes a civil liability in instances where seized keys are compromised by a failure of the safeguards arrangements in this section. There are two elements to this. Subsection (4)(a) is in respect of a person who fails to ensure that adequate arrangements are in place for the protection of keys. Subsection (4)(b) applies to where a person does not comply with those arrangements properly and compromises a key.

301. *Subsection (5)* describes the persons who may bring an action under the terms of this section. These are limited to persons who have made a disclosure in pursuance of a notice under section 49 or those whose protected information or key has been disclosed by some other person in pursuance of a notice.

Section 56: Interpretation of Part III

302. This section provides for the interpretation of various terms used in Part III of the Act.

Part Iv: Scrutiny Etc of Investigatory Powers and of the Functions of the Intelligence Services

Commissioners

Section 57: Interception of Communications Commissioner

303. This Section provides for the appointment of an Interception of Communications Commissioner to replace the Commissioner appointed under the Interception of Communications Act 1985. This is currently Lord Justice Swinton Thomas.

304. *Subsection (2)* details the remit of the Interception Commissioner. This will involve reviewing:

- the Secretary of State's role in interception warrantry;
- the operation of the regime for acquiring communications data;
- any notices for requiring the decryption of data authorised by the Secretary of State which relate to intercepted material or communications data;
- the adequacy of the arrangements made by the Secretary of State for the protection of intercepted material and by those persons listed in Section 55 for the protection of encryption keys for intercepted material and communications data.

305. *Subsection (7)* requires the Secretary of State to provide the Interception Commissioner with sufficient technical facilities and staff, after consultation with him. The provision

itself places no limitation on the number of staff and (subject to Treasury approval as to numbers) allows flexibility over the numbers, grades and individuals.

306. *Subsection (8)* is a transitional provision allowing the existing Interception Commissioner to take office as the new Interception Commissioner on the coming into force of this section.

Section 58: Cooperation with and reports by s. 57 Commissioner

307. *Subsection (1)* requires that all those who may be involved in requesting, authorising, or carrying out, interception should cooperate with the Interception Commissioner as he reviews the operation of the regime.

308. *Subsection (3)* provides that the Interception Commissioner should report to the Prime Minister if he believes that arrangements made by the Secretary of State are inadequate for the protection of either intercepted material or decryption keys.

Section 59: Intelligence Services Commissioner

309. This Section provides for the appointment of an Intelligence Services Commissioner to replace the Commissioners appointed under the Security Service Act 1989 and the Intelligence Services Act 1994. Both posts are currently held by Lord Justice Simon Brown.

310. *Subsection (2)* details the remit of the Intelligence Services Commissioner.

311. *Subsection (7)* requires the Secretary of State to provide the Intelligence Services Commissioner with staff, after consultation with him. The provision itself places no limitation on the number of staff and (subject to Treasury approval as to numbers) allows flexibility over the numbers, grades and individuals.

312. *Subsection (9)* is a transitional provision allowing the existing Intelligence Service Act Commissioner to take office as the new Intelligence Services Commissioner on the coming into force of this section.

Section 61: Investigatory powers Commissioner for Northern Ireland

313. This section provides for the appointment of an Investigatory Powers Commissioner for Northern Ireland.

314. *Subsection (2)* details the remit of this Commissioner

Section 62: Additional functions of Chief Surveillance Commissioner

315. This Section allocates oversight of certain powers in this Act to the existing Chief Surveillance Commissioner established under the Police Act 1997.

316. It adds to the existing remit of the Chief Surveillance Commissioner the functions of reviewing the use of surveillance, agents, informants, undercover officers and decryption notices, and the arrangements for protecting decryption keys, so far as these are not required to be kept under review by any of the other Commissioners mentioned in this Act.

Section 63: Assistant Surveillance Commissioners

317. This section allows for the appointment of Assistant Surveillance Commissioners to help the Chief Surveillance Commissioner fulfil his duties. Assistant Surveillance Commissioners can be circuit judges or equivalent.

Section 64: Delegation of Commissioners' functions

318. This Section allows Commissioners to delegate statutory powers or duties to members of staff.

Section 65: The Tribunal

319. This Section establishes a Tribunal, sets out its jurisdiction and gives effect to Schedule 3, which provides for its constitution and functioning.

320. *Subsections (2) to (8)* set out the key elements of the Tribunal's jurisdiction. It is to be the appropriate forum for complaints or proceedings in relation to the following categories:

- any proceedings for actions incompatible with Convention rights which are proceedings against any of the intelligence services or people acting on their behalf; or which concern the use of investigatory powers under this Act, any entry on or interference with property, any interference with wireless telegraphy; where any of these take place in relation to conduct by any of the public authorities listed in subsection (6);
- any complaint by a person who believes that he has been subject to any use of investigatory powers under this Act, any entry on or interference with property, any interference with wireless telegraphy which he believes to have been carried out by or on behalf of any of the intelligence services or in the challengeable circumstances described in subsection (7);
- any complaint by a person that he has suffered detriment as a result of any prohibition or restriction in Section 17 on his relying on any civil proceedings (Section 17 imposes various restrictions and prohibitions on the disclosure in court of intercepted material and related information); and
- any other proceedings against any of the intelligence services or people acting on their behalf, or which concern the use of investigatory powers under this Act, any entry on or interference with property, any interference with wireless telegraphy where any of these take place in relation to conduct by any of the public authorities listed in subsection (6). This category only applies to proceedings allocated to the Tribunal by the Secretary of State. Section 66 makes further provision concerning such orders.

321. *Subsection (6)* limits the Tribunal's jurisdiction in respect of Human Rights Act cases and proceedings allocated to the Tribunal by the Secretary of State. The jurisdiction will only apply to conduct by or on behalf of the police, Customs or intelligence services.

322. *Subsection (7)* qualifies the first and second categories and some elements of the fourth categories of the Tribunal's jurisdiction.

Section 66: Orders allocating proceedings to the Tribunal

323. This Section makes further provision concerning the orders (by affirmative resolution, see Section 78) that the Secretary of State may make to provide for the Tribunal to exercise jurisdiction over certain types of case. It ensures that:

- the Tribunal is given the power to remit proceedings to the court or tribunal which would have had jurisdiction but for the order;
- proceedings before the Tribunal are properly heard and considered;
- information is not disclosed where this might be damaging or prejudicial as described in subsection (2)(b).

Section 67: Exercise of the Tribunal's jurisdiction

324. This Section makes further provision concerning the exercise of the Tribunal's jurisdiction under Section 65. It describes how the Tribunal is to hear, consider and investigate complaints and proceedings, confers on the Tribunal the power to award compensation, quash or cancel any warrant or authorisation and require the destruction of records of information.

325. *Subsection (7)* confers powers on the Tribunal. An order to quash or cancel any warrant or authorisation would overturn the decision of the person who authorised such an instrument, and any continued conduct under the terms of the quashed authorisation or examination of information obtained under its authority would not be lawful.

Section 68: Tribunal procedure

326. This Section provides for the Tribunal to determine their own procedure (subject to any rules made by the Secretary of State under Section 69), and requires it to inform certain persons of proceedings, complaints and their determinations, and empowers it to require the cooperation of certain persons in exercising their powers and duties.

327. *Subsection (2)* empowers the Tribunal to require any Commissioner listed in subsection (8) to advise it on any matters falling within his knowledge which are relevant to the Tribunal's functions.

Section 69: Tribunal rules

328. This Section describes those rules which the Secretary of State may make subject to the affirmative resolution procedure to regulate the Tribunal's exercise of its powers, and any matters related to them.

329. *Subsections (2) to (5)* describe rules the Secretary of State may make, without limiting his power to make rules only to those matters listed.

330. *Subsection (6)* requires the Secretary of State, in making any rules, to ensure:

- that proceedings before the Tribunal are properly heard and considered; and
- that information is not disclosed where this might be damaging or prejudicial as described in subsection (2)(b).

331. *Subsection (7)* enables any rules to incorporate, for example, Civil Procedure Rules which have already been made. This avoids the need to create such rules from scratch for the Tribunal where they already exist elsewhere.

332. *Subsections (9) to (11)* provide that where rules governing the conduct of the Tribunal are made for the first time, they be made under a special 40 day procedure. This will ensure that the Tribunal is operational as soon as the substantive provisions in the Act are brought into force. For all subsequent rules, the affirmative resolution procedure will apply.

Section 70: Abolition of jurisdiction in relation to complaints

333. This Section repeals those provisions listed in subsection (2), which provide for the jurisdiction of Tribunals established by other Acts of Parliament to investigate complaints concerning conduct which is in future to be investigated by the Tribunal established in this Act. Those Tribunals may, however, finish their investigation of those cases which they begin to consider before the Act comes into force.

Section 71: Issue and revision of Codes of Practice

334. This Section deals with the issuing of Codes of Practice to explain in greater detail the practical arrangements relating to the use of the provisions of this Act.

335. *Subsections (1) and (2)* require the Secretary of State to issue one or more Codes of Practice covering the powers and duties in this Act and those relating to interference with property or wireless telegraphy in either the Intelligence Services Act 1994 or Part III of the Police Act 1997.

336. *Subsections (3), (4) and (5)* require the Secretary of State to consult on any Codes of Practice, lay the drafts before Parliament and bring them into force through an Order (by affirmative resolution, see Section 78).

Section 72: Effect of Codes of Practice

337. *Subsection (1)* requires any person to take account of any applicable Code of Practice issued under Section 71 while exercising or performing any power or duty under this Act.

338. *Subsection (2)* explains that a failure to comply with a Code of Practice issued under Section 71 will not of itself constitute a criminal offence or civil tort.

339. *Subsection (3)* allows the evidential use of a Code of Practice in court.

340. *Subsection (4)* requires that, where relevant, the statutory bodies described in this subsection must take into account the provisions of a Code of Practice.

Part V: Miscellaneous and Supplemental

Section 73: Conduct in relation to Wireless Telegraphy

341. This section amends Section 5 of the Wireless Telegraphy Act 1949 and is intended to ensure that the interception provisions of that Act comply with the Human Rights Act 1998.

342. *Subsection (1)* transfers the words of the existing section 5 of the Wireless Telegraphy Act to a new subsection 5(1). It also has the effect of removing the general authority to intercept wireless telegraphy which existed for persons acting in their duty as a servant of the Crown, and of changing the authority level which is required to authorise interception of wireless telegraphy from "under the authority of the Secretary of State" to "under the authority of a designated person".

"Designated person" is defined in the inserted section 5(12)

343. *Subsection (2)* creates new subsections 5(2) to 5(12) to the Wireless Telegraphy Act 1949 as follows:

- 5(2) restricts the ability of a designated person to authorise interception of wireless telegraphy to activity which cannot be warranted or authorised under this Act;
- 5(3) requires that where the an authorisation is granted under the Wireless Telegraphy Act 1949, consideration must be given to both the necessity and proportionality of the interception in the context of what is sought to be achieved through it;
- 5(4) explains the purposes for which an authorisation under the Wireless Telegraphy Act 1949 may be granted;
- 5(5) requires that where a requirement exists to intercept wireless telegraphy which would not meet one of the tests in 5(4) above but would fit within the criteria of this subsection, a separate authority must be sought;
- 5(6) requires a designated person to consider whether that which is sought to be achieved through the interception could be done in another way;

- 5(10) follows on from subsection (2) and explains that where interception of wireless telegraphy is required to be authorised under the Regulation of Investigatory Powers Act, the fact that the applicant cannot be authorised in this way because he is not mentioned as one of the bodies to which the Act applies does not mean that he can rely upon section 5 to obtain authorisation;
- 5(11) explains the meaning of "separate authority".

Section 74: Warrants under the Intelligence Services Act 1994

344. This section changes the test which must be satisfied before a warrant is issued under section 5 of the Intelligence Services Act 1994. Instead of "likely to be of substantial value", the test is now that the Secretary of State must be satisfied that:
    - the action is necessary for the purpose of a function of the intelligence agency;
    - the action is proportionate to what it seeks to achieve;
    - the action authorised by the warrant could not reasonably be achieved by other means.

345. *Subsection (3)* amends the urgent provisions so that a senior official of any department may sign an urgent warrant issued on the oral authority of the Secretary of State. Such a senior official will be a member of the Senior Civil Service or its equivalent in the Diplomatic Service.

Section 75: Authorisations under Part III of the Police Act 1997

346. This Section makes amendments to Part III of the Police Act 1997.

347. *Subsections (2) and (3)* amend section 93 of the Police Act to allow a police authorising officer to authorise interference with property outside his force area solely for the purpose of maintenance or retrieval of equipment. This will allow a chief constable to authorise action to maintain or retrieve a tracking device from a vehicle that has travelled outside the force area, without having to seek authorisation from the chief constable into whose area the vehicle has travelled. In addition it removes the restriction on where a customs officer may act.

348. In the same way that Section 74 amends the Intelligence Services Act 1994, s*ubsections (4) and (5)* introduce the new tests in the Part III authorisation process. These again require that the action authorised must be necessary and proportionate to what it seeks to achieve and that the action could not reasonably be achieved by other means.

349. *Subsection (5)* provides for an authorising officer of the Royal Ulster Constabulary to authorise interference with property or wireless telegraphy where it is necessary in the interests of national security as well as for the prevention or detection of serious crime. This is required because of the particular responsibilities of the Chief Constable of the RUC in relation to counter-terrorism.

350. *Subsections (6), (7) and (8)* extend the provisions of Part III to allow the chief constables of the British Transport Police and the Ministry of Defence Police and the Provost Marshals of the three service police forces to be authorising officers and to authorise interference with property or wireless telegraphy within their own jurisdictions. It also allows the Deputy Director General of the National Crime Squad to be an authorising officer in his own right and for the Commissioners of Customs & Excise to designate more than one customs officer to act as an authorising officer.

351. *Subsection (7)* makes an amendment to section 93(6) to provide that "relevant area" for the MOD police means the places described in section 2 of the Ministry of Defence Police Act 1987.

352. *Subsection (8)* makes provision about where the Service Police forces may exercise powers under the 1997 Act.

Section 76: Surveillance operations beginning in Scotland

353. This section provides that surveillance operations which properly begin in Scotland under the Regulation of Investigatory Powers (Scotland) Act can be continued in England under the original authorisation should circumstances arise which make that necessary. But the section stipulates that such authorisations can only be valid for three weeks outside the Scottish jurisdiction.

Section 79: Criminal liability of directors etc

354. This Section provides for personal criminal liability on the part of certain individuals in companies and other bodies corporate.

Section 80: General saving for lawful conduct

355. Section 80 ensures that nothing in this Act makes any actions unlawful unless that is explicitly stated. The availability of an authorisation or a warrant does not mean that it is unlawful not to seek or obtain one. In this respect, the Act must be read with section 6 of the Human Rights Act, which makes it unlawful to act in a way which is incompatible with a Convention right.

Schedule 1: Relevant Public Authorities

356. Part I of Schedule 1 lists those public authorities entitled to use the powers of directed surveillance and covert human intelligence sources under sections 28 and 29 of this Act. Part II of Schedule 1 lists those public authorities entitled to use the power of directed surveillance only, under section 28 of this Act

Schedule 2: Persons Having the Appropriate Permission

357. Schedule 2 deals with the duration and types of appropriate permission which may empower a person to serve a notice under section 49 of this Act requiring disclosure of information. The authority required to grant such permission varies depending on the powers under which unintelligible information is or is likely to be obtained.

Paragraph 1: Requirement that appropriate permission is granted by a judge

358. This paragraph states that subject to the provisions of the paragraphs below, authority to serve a notice must be given by a judge as described in Sub-paragraph (1).

359. The effect of Sub-paragraph (2) is that where a judge's permission has been obtained under this paragraph, no further authority is required to serve a notice.

Paragraph 2: Data obtained under warrant etc

360. This paragraph deals with unintelligible information which is or is likely to be obtained under a statutory power exercised in accordance with:

- a warrant issued by the Secretary of State or a person holding judicial office; or
- an authorisation under Part III of the Police Act 1997.

Examples of legislation under which the Secretary of State may issue a warrant include Chapter I of Part I of this Act and the Intelligence Services Act 1994. Examples of legislation under which a person holding judicial office may issue a warrant include the Police and Criminal Evidence Act 1984 and the Drug Trafficking Act 1994.

361. *Sub-paragraph (2)* states that the warrant or authorisation may empower a person to serve a notice requiring disclosure if:

- the warrant or authorisation gave explicit permission for the notice to be given; or
- written permission has been given by the authority since the warrant or authorisation was issued.

362. *Sub-paragraphs (3) to (5)* describe those persons who are capable of having the appropriate permission to serve a notice in relation to material to which this paragraph applies. And *Sub-paragraphs (6) to (8)* describe those persons who may issue a warrant or authorisation in relation to such material.

363. The effect of this paragraph is that where, for example, protected material has been obtained under an interception warrant, the authorisation to serve a disclosure notice may be granted by the Secretary of State.

364. *Sub-paragraph (9)* excludes from this paragraph unintelligible information:

- which has been obtained under a statutory power without a warrant; but
- which has been obtained in the course of, or in connection with, an exercise of another power for which a warrant was required.

365. This might include, for example, cases where a constable has a right to enter premises under a warrant and while on the premises uncovers matter which he suspects to be evidence of a crime unrelated to the warrant itself, in accordance with e.g. section 19 of the Police and Criminal Evidence Act 1984 (PACE).

Paragraph 3: Data obtained by the intelligence services under statute but without a warrant

366. This paragraph deals with unintelligible information which is, or is likely to be, lawfully obtained by the intelligence services but not under a warrant issued by the Secretary of State. This might include, for example, material obtained under a directed surveillance authorisation given under Part II of this Act.

367. *Sub-paragraph (2)* enables the Secretary of State to give authority for a notice to be served in such instances.

Paragraph 4: Data obtained under statute by other persons but without a warrant

368. This paragraph deals with unintelligible information which is or is likely to be obtained by certain agencies (other than the intelligence services) under statutory powers but not under a warrant issued by the Secretary of State or judicial authority. This includes, for example, material obtained by the police under powers conferred by section 19 of PACE.

369. The effect of Sub-paragraph (2) is that senior officers of the police, customs and excise and armed forces (as described in Paragraph 6) may authorise the service of a written notice in relation to material to which this paragraph applies.

370. The effect of sub-paragraph (3) is that where material to which this paragraph applies is obtained by agencies other than those described in Sub-paragraph (2), authority to serve a written notice is to be given by a judge, provided that the stipulations set out in Sub-paragraph (4) are complied with.

Paragraph 5: Data obtained without the exercise of statutory powers

371. This paragraph deals with unintelligible information which is or is likely to come into the possession of an intelligence service, the police or customs and excise by any other lawful means not involving the exercise of statutory powers (e.g. material which has been voluntarily handed over).

372. The effect of Sub-paragraph (2) is to enable the Secretary of State to give his permission to serve a notice in relation to material, obtained by an intelligence service, falling under this paragraph.

Paragraph 6: General requirements relating to the appropriate permission

373. This paragraph makes some further stipulations about the categories of person who may be empowered to require disclosure. It also makes some stipulations about the permissions that may be given by members of the police, customs and excise and the armed forces.

374. *Sub-paragraph (3)* states that in the case of information which has come into the police's possession by means of powers to stop and search vehicles and pedestrians under the Terrorism Act 2000 or the Prevention of Terrorism (Temporary Provisions) Act 1989 (PTA), those able to authorise the serving of notice must be an officer of police of or above the rank specified in section 44 and section 13A of those Acts respectively.

Section 13A of the PTA, for example, specifies such ranks as:

- *commander of the metropolitan police, as respects the metropolitan police area;*
- *commander of the City of London police, as respects the City of London; or*
- *assistant chief constable for any other police area.*

Paragraph 7: Duration of permission

375. This paragraph provides for the duration of the validity of authorisations to serve a notice and prevents the issue of a notice after the authorisation has expired.

Paragraph 8: Formalities for permissions granted by the Secretary of State

376. This paragraph states that any permissions granted by the Secretary of State in accordance with Schedule 2 may only be granted:

- if signed by him personally; or
- if signed by a member of the Senior Civil Service (or Diplomatic Service equivalent) and expressly authorised by the Secretary of State. The express authorisation must be in relation to that particular warrant (i.e. there can be no standing authorisation).

Schedule 3: The Tribunal

377. This Schedule provides for the constitution of the Tribunal established under Section 65.

Paragraph 1: Membership of the Tribunal

378. This paragraph determines the membership of the Tribunal.

379. *Sub-paragraph (1)* ensures that members of the Tribunal may be drawn from the legal profession in all parts of the United Kingdom.

> *"High Judicial Office" is defined in Section 25 of the Appellate Jurisdiction Act 1876 as follows:*
>
> *"'High Judicial Office' means any of the following offices; that is to say*
>
> *The office of Lord Chancellor of Great Britain… or of Judge of one of Her Majesty's superior courts of Great Britain and Ireland:*
>
> *'Superior courts of Great Britain and Ireland' means and includes*

As to England, Her Majesty's High Court of Justice and Her Majesty's Court of Appeal; and

As to Northern Ireland, Her Majesty's High Court of Justice in Northern Ireland and Her Majesty's Court of Appeal in Northern Ireland; and

As to Scotland, the Court of Session."

The Appellate Jurisdiction Act of 1887 amended the term 'High Judicial Office' in Section 5 to include the office of a Lord of Appeal in Ordinary and the office of a member of the Judicial Committee of the Privy Council.

The requirement of ten years' standing means that only those eligible for appointment to the judiciary can serve.

The Courts and Legal Services Act 1990 states that a person has a "general qualification" if he has a right of audience in relation to any class of proceedings in any part of the Supreme Court, or all proceedings in county courts or magistrates' courts.

380. Sub-paragraph (3) limits the term of office to five years. A member whose term of office expires is eligible for reappointment. Were he to serve a second time he would have to be re-appointed by further Letters Patent. There is no retirement age.

381. Sub-paragraph (4) provides the means whereby a member may resign.

Paragraph 2: President and Vice-President

382. This paragraph establishes the positions of President and Vice-President who will be members of the Tribunal.

Paragraph 3: Members of the Tribunal with special responsibilities

383. This paragraph requires the President of the Tribunal:

- to give one or more members of the Tribunal special responsibility for matters involving the intelligence services; and
- to ensure that in the consideration or hearing of any complaints or proceedings considered by the Tribunal which relate to an allegation against any of the intelligence services or their members or to conduct by or on behalf of any of those services or their members, the Tribunal on that occasion includes one or more of the members with such special responsibility.

Paragraph 4: Salaries and expenses

384. This paragraph deals with the payments of the members of the Tribunal and of its expenses.

Paragraph 5: Officers

385. *Sub-paragraph (1)* provides for the appointment of officers of the Tribunal by the Secretary of State, after consultation with the Tribunal. The Secretary of State may not therefore proceed unilaterally to make appointments. The provision itself places no limitation on the number of officers and (subject to Treasury approval as numbers) allows flexibility over the numbers, grades and individuals.

386. *Sub-paragraph (2)* enables an officer who is so authorised by the Tribunal to obtain documents or information on the Tribunal's behalf.

Paragraph 6: Parliamentary disqualification

387. The parts of the Schedules referred to in this paragraph list the bodies whose members are disqualified from membership of the House of Commons and the Northern Ireland Assembly respectively. They include Tribunals and public Boards, Commissions and Councils. Members of this Tribunal (as people paid for adjudicating in a quasi-judicial capacity on the decisions of Ministers, and able to overturn those decisions) clearly fall within the category of those who are normally disqualified.

Schedule 4

Paragraph 8: The Police Act 1997 (c.50)

388. This makes necessary consequential changes in the light of the amendments to Part III of the Police Act 1997. These take account of the extension of authorising powers to the Ministry of Defence Police, the British Transport Police, the Service Police, the three service police forces, the Deputy Director General of the National Crime Squad and additional designated customs officers.

389. *Sub-paragraph (10*) extends the functions of the Chief Surveillance Commissioner so that he reports annually to the Prime Minister and at any other time on any matters arising from his functions in relation to Part III of the Police Act 1997 or Part II of this Act.

390. *Sub-paragraph (11)* imposes a duty on those exercising functions under these provisions to disclose or provide the Chief Surveillance Commissioner with any documents or information he requires to enable him to carry out his functions. It also imposes a duty on every Commissioner to give the Tribunal established under section 65 of this Act all such assistance as may be required.