Interception of Communications Ordinance 2022

ANDREW MITCHELL KC

QUINN HAWKINS

INTERCEPTION OF COMMUNICATIONS ORDINANCE [ICO] 2022

Raison D'Etre

The telecommunications infrastructure can be used to plan and carry out unlawful activity.

The law previously only permitted a court to authorise telecommunications providers to provide details of phone calls made and received and their locations.

A more comprehensive, transparent and modern legalised interception of communications is now established to permit the gathering of intelligence through the telecommunications and postal network.

The use of such interception is now supervised, transparent and accountable.

INTRODUCTION

The Interception of Communications Ordinance 2022 [ICO] is 78 Sections in 7 Parts

It provides a one stop legal framework for law enforcement and intelligence agencies to use investigative powers to obtain access to communications, communications data and postal material.

These powers cover the interception of communications, the retention and acquisition of communications data, and the use of equipment interference for obtaining communications and other data.

IOC is based on UK
- Investigatory Powers Act (IPA) 2016 and
- Regulation of Investigatory Powers Act (RIPA) 2000

Purpose

The Ordinance provides for the lawful interception of communications.

It is now unlawful to intentionally intercept, in the Turks and Caicos Islands, a communication in the course of its transmission without lawful authority.

This applies to all communications in the course of transmission via a public telecommunications system, a private telecommunications system or a public postal service (which includes any service whose purpose is the collection, sorting etc of postal packages and also means a courier service.

Scheduled Offences

1. Murder or treason

2. Kidnapping or abduction

3. Rape

4. Sexual exploitation of children

5. Money laundering offence contrary to the Proceeds of Crime Ordinance

6. An offence contrary to the Prevention of Terrorism Ordinance

7. Trafficking in persons contrary to the Trafficking in Persons (Prevention) Ordinance

8. Assisting illegal entry contrary to the ImmigrationOrdinance

Scheduled Offences - Continued

9. Producing, manufacture, supplying or otherwise dealing in any controlled drug in contravention of the Control of Drugs Ordinance

10. Importing or exporting a controlled drug specified in Parts I, II or III of the First Schedule of the Control of Drugs Ordinance in contravention of that Ordinance

11. Importation or exportation of firearm in contravention of the Customs Ordinance

12. An offence contrary to the Anti-Gang Ordinance

13. An offence contrary to the to the Firearms Ordinance

14. An offence contrary to the Integrity Commission Ordinance

15. An offence contrary to the applicable International Convention on hijacking, terrorist offences or people trafficking

16. Attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding paragraphs.

IOC - Part 1

Part I of the Ordinance provides the preliminary/explanatory provisions, which includes the commencement and interpretation clauses.

Section 3 defines “interception” and sets out when interception is regarded as taking place in the Turks and Caicos Islands. This clause set out what constitutes intercepting a communication in the course of its transmission by a telecommunications system. There are three elements.

Firstly, the person must perform a “relevant act”, which is defined in subsection (5) and includes modifying or interfering with the system.

Secondly, the consequence of the relevant act must be to make the content of the communication available to a person who is not the sender or intended recipient.

Thirdly, the content must be made available at a “relevant time”, which means a time while the communication is being transmitted or any time when the communication is stored in or by the system. The definition of a relevant time makes it clear that interception includes obtaining stored communications, such as messages stored on phones, tablets and other individual devices whether before or after they are sent.

OFFENCES

- **Part II – creates the Offenes of intentional interception of communications – without lawful authority – prosecutions only with the consent of the DPP**

S7

Interception: Public or Private telecommunucations and “public” postal service – carries a penalty of unlimited fine, 7 years imprisonment (or both) - following conviction on indictment.

S8

A relevant person – (any person holding office under the Crown, any person employed by RTCIPF or any person working for the relevant communications company) knowingly or reckelssly obtaining communications data is liable to imprisonment for 4 years a find of $50,000 of both

Exclusions – Section 4

Section 4 sets out conduct which does not constitute interception.

4(1) makes clear that interception of a communication broadcast for general reception is not interception for the purposes of the Ordinance. That means that watching television is not interception nor is listening to the radio.

4(2) excludes certain conduct in relation to postal data attached to the communication, e.g. reading the address on the outside of a letter in order to ensure it is delivered to the appropriate location.

Litigation restrictions - inquiries

By section 44

No evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which, in any manner—

(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—(i) any content of an intercepted communication; or

(ii) any secondary data obtained from a communication; or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

Disclosure of communications

- Section 45

- Disclosure of the existence of intercept is however permitted for the purposes of
  - a prosecution under ICO or related legislation,
  - to ensure fairness in any proceedings – disclsoure to a prosecutor
  - Disclosure to a judge – where the judge so orders –
  - And then if the judge orders disclsoure in the interests of justice - although it looks like there is a typo in 44 (8) and (9)

Lawful Authority to carry out interception

- Section 9

- A person has lawful authority to carry out an interception if AND ONLY IF
  - Warrant under ICO
  - In relation to stored communications such as voice messages, text and other messages or emails
    - Targeted equipment interference warrant, or
    - Exercise of any statutory power – such as a search and seizure warrant under POCO, or
    - Any Court order made for that purposes -

UK Authorities - “Interception”

R v Hardy and Another [2003] 1 Cr.App.R. 30

Authorised undercover police officers tape recorded meetings and telephone conversations. The defendants failed in an abuse of process argument which included that the authority for surveillance (undercover officers) did not cover the tape recording.

Held: The tape recording by the undercover officers of their telephone conversations with the appellants was not an interception of a communication in the course of its transmission by a telecommunication system, within s. 2(2) of RIPA 2000, but was the same as the secret recording by the officer of a conversation whilst meeting the suspect face to face.

UK Authorities - “Interception”

R v E [2004] 2 Cr.App.R. 29

Police obtained permission under RIPA 2000 to place a covert listening device in the appellants car. The device recorded words spoken by the appellant to other people in the car, words spoken by those people to him and words spoken by the appellant when in the car and using a mobile telephone, although it did not record what was said by the other person on the other end of the telephone. On the appeal it was submitted that what had occurred amounted to an “interception” of the telephone calls which either authorised by the Sec. of State under s.5 RIPA, or, if not constituted an offence of unlawful interception and, either way, all the evidence was inadmissible as a consequence of s.17 RIPA 2000.

Held: Dismissing the appeal, the natural meaning of the expression “interception” denoted some interference or abstraction of the signal during the process of transmission. The recording of a persons voice did not become an interception because what was said was recorded and, by a separate process was transmitted by a telecommunications system. The recording was independent of the operation of the telecommunications system and were not recordings made in the course of transmission.

UK Authorities - “Interception”

R v A and Others [2021] 2 W.L.R. 1301

As part of the case as against the appellants the prosecution relied on material harvested from an EnchroChat communication system (handsets issued by the provider could only communicate with other handsets on the system). Any message sent was encrypted as it passed through its server between one handset and another, being decrypted at the receiving handset so that it could be read by the user. The defendants submitted that the material was inadmissible pursuant to section s.56(1) Investigatory Powers Act 2016 (s.44(1) ICO) because the material consisted of intercepted communications. The issue was whether the communications were “stored” in or by the telecommunications system or as the defendants submitted, whether they were “being transmitted”. The trial judge rejected the defendants argument finding the EnchroChat material was admissible. The defendants appealed.

Held: Dismissing the appeal, that the question whether an intercepted communication was “being transmitted”or “stored” at the relevant time did not require a minute examination of the inner workings of the relevant telecommunications system, since the statutory scheme, which used ordinary English words, had to be made to work whatever the technical features of the system in question and then to decide whether, as a matter of ordinary language, the communication was being transmitted or stored at the time of its inception … that having regard to the words used and the overall legislative purpose, the definition “stored” at the relevant time, within section 4(4)(b) IPA (s.3 ICO) extended to all communications stored on a telecommunications system, whether before, during of after transmission. Thus if the material is “stored in or by the system” within the meaning of s.4(4)(a) IPA (s.3 ICO)(as opposed to it being intercepted while it was “being transmitted” within the meaning of s.4(4)(a) and therefore inadmissible under s.56 IPA (s.44 ICO) and as such was admissible in evidence.

Part III - Warrants

The Ordinance sets out the circumstances in which an authorised person may be granted authority to carry out interception, so that the offence of unlawful interception is not committed.

An application for a warrant can only be made by the Director of Public Prosecutions, on behalf of an authorised officer.

An authorised officer is defined as the COP or the DCOP (or a person acting for such persons).

The Ordinance provides for (s.10) targeted interception warrants, mutual assistance warrants and (s.23) targeted equipment interference warrants.

Warrants - continued

Targeted interception warrant may authorise any activity for the interception, in the course of its transmission whether the postal service or telecommunications system in respect of communications described in the warrant.

A mutual assistance warrant gives effect to a request from a foreign authority, or authorises an outgoing request, for assistance in relation to the interception of communications. Such a request may be made in accordance with international mutual legal assistance agreements.

Warrants - continued

Section 14 sets out the grounds on which warrants may be issued by a Judge of the Supreme Court.

S.14(2) The grounds are: in the interests of internal security, for the purpose of preventing or detecting serious crime (defined in the schedule to the Ordinance), in the interests of the economic well-being of the Islands, or for giving effect to the provisions of a mutual assistance agreement.

S.14(4) An application for a warrant in the interests of the economic well-being of the Islands may only be considered necessary when it relates to the acts or intentions of persons outside the Islands.

S.14(5) specifies that a warrant cannot be considered necessary if the only purpose is gathering evidence for use in legal proceedings.

Warrants – limitation and procedure

A warrant lasts for **six months** (unless it is cancelled earlier).

If the warrant is not renewed it will cease to have effect after that period.

The application must be on oath and in writing.

The Ordinance provides for cancellation of warrants and modifications which may be made to a warrant.

The Ordinance requires that the authorising officer must ensure that arrangements are in force for securing that there is proper provision relating to retention and disclosure of material obtained under the warrant.

The number of persons who see the material, the extent of disclosure and the number of copies made of any material must be to the minimum necessary for the authorised purposes.

Urgent Warrant

S 15 provides for urgent warrants - they will only last for seventy-two hours.

The application for an urgent warrant may be made orally but needs to be backed up by a written application within 72 hours.

Protection of rights - Safeguards

Section 16 provides for safeguards to apply to the interception of items that might be subject to legal privilege. Items subject to legal privilege are communications between a lawyer and their client, or a person representing that client, in connection with legal advice or legal proceedings.

Where the purpose, or one of the purposes, of a warrant is to obtain communications subject to legal privilege, the warrant application must make that clear.

The Judge issuing the warrant must consider the public interest in obtaining the information that would be obtained by the warrant outweighs the public interest in the confidentiality of items subject to privilege.

The Judge must be satisfied that there are **exceptional and compelling circumstances which make the interception** or selection for examination of these items necessary, and that there are specific arrangements in place for how these items will be handled, retained, used and destroyed. This it is suggested would include where the communication is to further crime, but there are likely to be other circumstances

Section 17 provides for similar safeguards in respect of confidential journalistic material or to identify or confirm a journalist's source.

Part III – Chapter 2 – Equipment Interference

Sections 22 to 32

- Same processes and procedure as for an interception warrant
- Chapter 2 - provides for interference with “equipment” – being systems data or data that identifies people or events – and an interference warrant shall authorise the interfernce with any equipment for the purpose of obtaining communications, equipment data, any other information – by monitoring, observing, listening, recording.
- In respect of stored communications (s23(6))
- S30(6) lists the issues that might arise for the warrant application, such as why it is needed and sets out the details that need to be provided in the warrant in particualr cases

Progress

Section 35 provides for the judge who grants a warrant to seek updates on the progress of the investigation or on any matter which the judge deems necessary at such stages that the judge deems appropriate - failure to provide the update can result in the cancellation of the warrant. The judge cannot seek updates where the warrant applied for was following an urgent application.

Postal Articles

What to do with the post –

S39 – if perishable – with due regard to interests of persons concerned – dispose of the article as circmstances may require.

Retain it if not disposed of, unless no criminal or civil proceedings instituted – then it must be returned.

Part IV Disclosure Orders ICO ss49-55

Application for Disclosure Orders (s.49 - 55)

If there is “protected information” that is information that is passworded or secure (by whatever means) - the DPP may apply ex parte to a judge in chambers for a Disclosure Order - to enable the information to be obtained in an accessible form - in the interests of National Security, preventing or detecting crime; or in the economic well-being of the Islands.

Tipping off (s.53)

If a person is served with or becomes aware of a disclosure order and discloses the existence of such an order: liable to imprisonment for one year or a fine of $20,000 on summary conviction. It is a defence to a tipping off allegation that the disclosure was to an Attorney in contemplation of advice or proceedings.

Communications Data

By Section 5 communications data is defined in relation to a telecommunications operator which in the ordinary course of operation the Operator would have — call records, cell points, operation of the system - this is defined as entity data and events data - that is information about the contract between the operator and an entity, which describes the entity and/or describes when and where communication occurred.

The Governor's Powers

Part V ICO - Power to Grant Authorisations

Section 56 ICO gives the Governor power on application by an 'authorised officer' to grant authorisation to obtain communications data.

The Governor must consider:

(a) that it is necessary for a purpose falling within subsection (7) (interests of national security, applicable crime purpose etc);

(b) that it is necessary for the authorised officer to obtain the data for the purposes of a specific investigation or a specific operation; and

(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

Thus an 'appropriate officer' upon application should be able to assist the Governor in respect of the purpose for the application, why it is necessary and proportionate.

Authorised Officers Powers - Urgent

An authorised officer (The Commissioner or Deputy Commissioner of Police s.2 ICO) granted the authority by the Governor may engage in ‘authorised conduct’ (s56(4) ICO) by:

a. obtaining the communications data himself from any person or telecommunications system;

b. asking any person whom the officer believes is, or may be, in possession of the communications data or capable of obtaining it, to obtain or disclose the data; and

c. requiring by notice endorsed by or on behalf of the Governor a telecommunications operator whom the officer believes is, or may be, in possession of the communications data or capable of obtaining it, to obtain the data; and to disclose the data to a person identified by, or in accordance with, the authorisation.

Extension of application of Ordinance

The Ordinance provides that the Governor may by Order published in the Gazette, declare any electronic, electro-magnetic, acoustic, mechanical or other equipment or device, the design of which renders it primarily useful for the purposes of interception of communications, under circumstances specified in the notice, to be listed equipment.

It is unlawful to manufacture, assemble, possess, sell, purchase or advertise any equipment declared to be a listed equipment, unless an exemption order is in place.

The Ordinance provides for the forfeiture of listed equipment seized from a person convicted of an offence.