



OECD International Academy for Tax Crime Investigation

Investigative Techniques for the Effective Use of Banking Information



OECD Anti-Money Laundering / Crypto Presentation

Mark Waldon – Senior Investigation Officer HMRC

Regulation Of Investigatory Powers Act 2000 (RIPA)

- Provides a framework to ensure investigatory techniques are used in a way that is compatible with Article 8 – right to respect for a private and family life enshrined in the European Convention of Human Rights (ECHR).
- Provides safeguards against abuse of powers by the state
- Use of covert tactics will only be authorized if considered legal, necessary and proportionate
- Complex act as we shall see.....

Necessity

- In the interests of national security;
- For the purpose of preventing & detecting crime or of preventing disorder;
- In the interests of the economic well-being of the UK;
- In the interests of public safety;
- For the purpose of protecting public health
- For the purpose of assessing or collecting any tax, duty or levy or other imposition, contribution or charge payable to a government department; or
- For any other purpose prescribed in an order made by the Secretary of State.

Proportionality

- Balancing the size & scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Collateral Intrusion

- **Inevitable intrusion** (such as into the privacy of intimate associates of the subject)
- **Foreseeable intrusion** (such as into the privacy of known associates)
- **General intrusion** (such as into the privacy of other members of the public who come into contact with the subject)

Applicants must detail how they will minimize the risk of collateral intrusion and how they will store/treat/handle any material which intrudes into the private lives of the subjects; their friends and families; and/or any members of the public

Interception, directed and intrusive

- Interception = the most sensitive kind of surveillance, obtained via a warrant signed off by the Home Secretary (inadmissible in a UK court)
- Directed (DSA) – information about a communication NOT its content. Also physical surveillance carried out ‘in such a manner as is likely to result in the obtaining of private information about a person’
- Intrusive (aka Police Act) – interfering with (entering, ‘bugging’, trespassing) on either a residential premises, a private vehicle, or any kind of surveillance device
- Investigatory Powers Act 2016 – TEI – provides the ability to obtain a variety of data from equipment (phones, laptops, tablets) remotely or physically

Targeted Electronic Interference

- The implementation of the Equipment Interference provisions of the Investigatory Powers Act (IPA) 2016 commences on 5th December 2018.
- Equipment interference describes a range of techniques that may be used to obtain communications, equipment data or other information from equipment. EI can be carried out either remotely or by physically interacting with the equipment.
- EI covers a range of techniques which vary hugely in complexity and sensitivity but includes:
 - Physically accessing and examining a device;
 - Accessing login credentials for an online account;
 - Deploying EI tools either physically or remotely;
 - Exploiting a device remotely through EI.

Legal Advice

- Advice was sought on whether employing a tool or device to interpret data from various Blockchains and openly distributed ledgers in order to map transactions required an authority (DSA) under RIPA 2000
- Legal counsel considered Blockchains ‘open source’ and therefore NOT requiring a DSA
- However it is thought both ‘best practice’ and prudent to align our department with other Law Enforcement agencies in erring on the side of caution and obtaining a DSA
- Defends us against legal argument and multiple surveillance attempts and data captures