INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

IOCCO Response to Operation Alice

It has been reported in the media that the Metropolitan Police Service (MPS) has used their powers within Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 ("the Act") to acquire communications data to investigate the circumstances surrounding an incident in Downing Street in September 2012 involving the Rt. Hon Andrew Mitchell MP and police officers from the MPS. Operation Alice was the investigation into what has been referred to in the media as "Plebgate."

MPS has disclosed information that confirms communications data was acquired from communication service providers (CSPs) as part of that investigation using their powers within Chapter 2 of Part 1 of the Act.[1]

The media reports have made several references about the use of those powers to acquire communications data and the appropriateness of their use in relation to journalistic privilege. We have received several enquiries about the reports and this response seeks to provide further information in relation to the legislative framework governing the acquisition of communications data.

The law

Parliament has enabled a range of public authorities, in addition to law enforcement and the intelligence agencies, to be able to use powers within Chapter 2 of Part 1 of the Act to acquire communications data as they have statutory requirements to investigate particular areas of criminal activity (for example the Gambling Commission in relation to illegal online gaming). It is therefore unhelpful when media reports cite the Act as a terrorist law and infer that its use for non terrorist related matters is inappropriate.

There are strict rules governing who can obtain communications data and the circumstances in which they can access the data retained by CSPs and they are defined in Chapter 2 of Part 1 of the Act and the code of practice[2] accompanying it. The rules in the code were approved by Parliament and implemented in October of 2007 and include -

- the statutory purposes for which public authorities may obtain data;
- the type of data public authorities may obtain;
- which senior officials within public authorities may exercise the power to obtain data; and
- which individuals within public authorities undertake the work to obtain data.

The code relates to the powers and duties conferred or imposed under the Act relating to the acquisition of communications data by public authorities and its disclosure by CSPs. It provides guidance on the procedures to be followed for the acquisition of communications data and describes communications data. It sets out rules for the acquisition and disclosure of data and the keeping of records.

Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed (see section 81(5) of the Act). Where an investigation relates to an allegation of criminal conduct by a member of a police force, that police force (or another public authority appointed to investigate the complaint) may use their powers under Chapter 2 to obtain communications data for the purpose of preventing and detecting the alleged or

[1] http://www.met.police.uk/pressbureau/Bur01/Operation%20Alice%20Closing%20Report.pdf
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97961/code-of-practice-acquisition.pdf

suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. That means the police cannot use their powers within the Act to acquire communications data to obtain evidence to then merely make an officer or member of their staff subject to an internal discipline hearing. So, should it be determined there are insufficient grounds to continue the criminal investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate for the police force to obtain communications data under the Act.

Communications data generated and processed by CSPs are business records. They do not contain any details of what was said or written by the sender or the recipient of the communication. As such, the communications data retained by CSPs do not contain any material that may be said to be of professional or legal privilege – the fact that a communication took place does not provide what was discussed or considered or advised.

However, it may be possible to infer an issue of sensitivity is under consideration because a person has regular contact with, for example a lawyer, doctor, journalist, Member of Parliament, or minister of religion. Thus the degree of interference with the person's privacy and their correspondence may be said to be higher when a person is in regular contact by telephone with, for example, a medial practitioner known to specialise with a particular condition or illness or with a journalist noted for specialising in a particular topic. Such situations do not preclude the acquisition of communications data within a criminal investigation but the senior officer considering authorising an application in such circumstances must have the facts set out in the application they are considering so they may properly assess necessity, proportionality and collateral intrusion matters. The senior officer can only approve the acquisition of data where they believe it is necessary and proportionate in the specific circumstances and they must record their considerations at the time. There is case law relating to various rulings regarding freedom of expression[3] when intertwined and balanced against, for example, the prevention or detection of crime or matters relating to national security. The communications data code of practice puts an onus on the senior officers who undertake the role of a designated person to have a current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

The Government Note on the European Court of Justice Judgment[4] outlines the Government's intention to amend the communications data code of practice, ensuring that where there may be concerns relating to professions that handle privileged information (for example, lawyers or journalists), public authorities give additional consideration to the level of intrusion. Section 71(3) of the Act requires the Secretary of State to prepare and publish a draft of the code and consider any representations made to him about that draft prior to issuing the code.

Clearly the legality and considerations are different in matters relating to the interception of communications (Chapter 1 of Part 1 of the Act) or in circumstances where the police use their powers to undertake surveillance (Part 2 of the Act). It is recognised that the use of these powers, could in certain circumstances, result in access to confidential personal information or confidential journalistic material. It is for this reason the rules approved by Parliament relating to the interception of communications and those relating to surveillance have within their respective codes of practice clear guidance –

- see Interception of Communications - Code of Practice - paragraphs 3.9 to 3.11[5] and
- see Covert Surveillance and Property Interference - Code of Practice - Chapter 4[6].

[3] https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-10-freedom-expression
[4] www.gov.uk/government/uploads/system/uploads/attachment_data/file/331106/DRIPgovernmentNoteECJjudgment.pdf
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf
[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf

Oversight

The Interception of Communication Commissioner and his Inspectors scrutinise public authorities conduct to obtain communications data. Within each public authority a senior responsible officer must be appointed (within the police the minimum rank is superintendent) to ensure the full provisions of the communications data code of practice are complied with, in particular the integrity of the process to acquire communications data, and;

- compliance with the code;
- oversight of the reporting of errors to the Commissioner, identifying their causes;
- taking appropriate action to minimise the repetition of errors;
- engagement with the Commissioner's Inspectors and ensuring that all relevant records are produced for the inspection.
- oversight of the implementation of recommendations, approved by the Commissioner.

IOCCO is not a "public authority" for the purpose of the Freedom of Information Act (FOIA). We do publish the statistical information that we hold in relation to public authorities use of communications data in our Annual Report (see Pages 22-25 and Annex B of our 2013 Annual Report[7]). We do not hold any additional statistical information to that which is published. We also do not hold information concerning the detail of individual applications submitted by public authorities.

The communications data code makes clear that anyone who believes their data has been wrongly acquired has the right to approach the Investigatory Powers Tribunal[8] established under the Act to consider complaints about unauthorised conduct. The communications data code of practice makes clear that if the Commissioner establishes an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority to comply with the Act he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role and should enable that person to effectively engage the Tribunal.

NOTES:

- IOCCO is an independent oversight body – independent of Government and Parliament – The Commissioner is required to have held high judicial office and complete independence is a hallmark of any judge.

- We are committed to openness and transparency. We report on our work in an Annual Report to the Prime Minister which is laid before Parliament for all to read.

- We conduct thorough and robust inspections of public authorities which have powers to intercept communications and acquire communications data. We have full and unrestricted access to all of the information we require to carry out our statutory oversight function.

- We carried out 140 inspections in 2013, and made 350 recommendations to ensure compliance or to improve systems and procedures. Detailed information on our inspections and findings can be found in our latest Annual Report.

- We are in the process of carrying out an Inquiry into whether there might be institutional overuse by police forces and law enforcement agencies of authorisations to acquire communications data. We will report on this inquiry when the investigation is complete.

[7] http://www.iocco-uk.info/sections.asp?sectionID=1&type=top
[8] http://www.ipt-uk.com/