*Below are excerpts (in black) from the current CD Codes of Practice which, within the introduction, details the circumstances where it is possible to acquire CD. The proposed changes to text are in red. Reference to paragraph numbers have been removed until the paragraphs are settled.*

Introduction

This code of practice relates to the exercise of functions conferred by virtue of Parts 3 and 4 of the Investigatory Powers Act 2016 (‘the Act’). Section 2 of this code provides guidance on the procedures to be followed when acquisition of communications data takes place under the provisions in Part 3 of the Act (‘Part 3’). Section 3 of this code provides guidance on the procedures to be followed when communications data is retained under Part 4 of the Act (‘Part 4’).

Sections 1, 2 and 4 of this code are relevant to relevant public authorities within the

meaning of the Act and to telecommunications operators and postal operators. The

relevant public authorities are those public authorities that can acquire communications data. They are set out in Schedule 4 to the Act. Section 12 of the Act (with Schedule 2) limits the use of other information gathering powers in law which provide for access to communications data without a Part 3 authorisation.

Relevant public authorities, for the purposes of Part 3, should not use other statutory powers to obtain targeted communications data from a postal or telecommunications operator unless that power:

* is authorised by a warrant or order issued by a person holding judicial office;
* is a general information gathering power, which is a regulatory or supervisory power, and which is exercised otherwise than in the course of a criminal investigation;

In all other cases a Part 3 authorisation should be sought.

A ‘criminal investigation’ means an investigation of any alleged or suspected criminal conduct or to establish whether such conduct has taken place.

A general information gathering power, which is a regulatory or supervisory power, will be treated as not being ‘in the course of a criminal investigation’ if, at the time of the exercise of the power the investigation is not being conducted with a view to seeking a criminal prosecution.

A regulatory or supervisory power is a power to obtain information or documents exercised in connection with:

1. the regulation of persons or activities,

(ii) the checking or monitoring of compliance with

requirements, prohibitions or standards imposed

by or under an enactment, or

(iii) enforcement of any requirement or prohibition

imposed by or under an enactment.

This definition of a regulatory or supervisory power is to permit organisations such as the Financial Conduct Authority and His Majesty’s Revenue and Customs with the regulation of the Financial Sector and/or Money Laundering Regulations to acquire communications data. It is also designed to permit Border Force communications data acquisition powers in the management of activities to ensure illegal substances are not being transported across borders, and in the management of persons subject to immigration restrictions.

CD acquired using a general information gathering power, which is a regulatory or supervisory power, and which at the time was exercised otherwise than in the course of a criminal investigation can only later be used in support of a criminal prosecution where the public authority can show a clear, auditable and tangible escalation of the circumstances leading to a decision that criminal prosecution was more appropriate.

Public authorities who straddle both civil and criminal investigations and who need to move from a civil to criminal resolution, should have in place clear policy and operating procedures for managing such circumstances to give practical effect to the above paragraph.

It is recognised that the point at which a decision is made to move from civil to criminal process may come after the original CD has been deleted by the TO. The only relevant CD still available to investigators may be that obtained using regulatory or supervisory information gathering powers. It is therefore not intended to prevent the use of CD, acquired using such general information gathering powers, from being later used in support of a criminal prosecution.

That policy, and those procedures, however, must ensure sufficient record keeping enabling an independent reviewer, with no prior knowledge of the case, to follow the developing circumstances and reach a similar conclusion at broadly the same point in the enquiry.

Matters moving from an initial civil remedy to a criminal prosecution will be of particular interest to the Investigatory Powers Commissioners Office, during inspection of organisations which straddle both civil and criminal outcomes. This will provide the necessary independent oversight to ensure the use of regulatory or supervisory related information gathering powers are both lawful and proportionate in all circumstances.

Where a criminal prosecution is sought from the outset such regulatory or supervisory bodies, granted IP Act powers by virtue of Schedule 4, must continue to use a Part 3 IP Act authority to gather CD in that case.

Relevant public authorities should not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to restrictions on disclosing personal data under relevant data protection

legislation.

Sections 1, 3 and 4 of this code are relevant to telecommunications operators and

postal operators who have been given a data retention notice under Part 4.

This code should be readily available to members of a relevant public authority involved in the acquisition of communications data under the Act, and to telecommunications operators and postal operators involved in the retention of communications data and/or its disclosure to public authorities under the Act.

The Act provides that persons exercising any functions to which this code relates must have regard to the contents of the code in the exercise of those functions.

The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any

court or tribunal hearing any such proceedings, or to the Investigatory Powers

Tribunal (‘IPT’) or to the Investigatory Powers Commissioner (‘IPC’) or the

Information Commissioner when overseeing the powers conferred by the Act, it may

be taken into account.

The Interception of Communications Code of Practice, Bulk Acquisition Code of

Practice and Equipment Interference Code of Practice provide guidance on

procedures to be followed in relation to those Parts of the Act.

The exercise of powers and duties under Parts 3 and 4 of the Act and this code are

kept under review by the IPC appointed under section 227 of the Act and by his

Judicial Commissioners and inspectors. Duties under Part 4 of the Act and this

code in relation to the security, integrity and destruction of data retained under a

retention notice are subject to audit by the Information Commissioner. Telecommunications operators and postal operators must comply with reasonable

requests from the Information Commissioner in relation to his audit role.

The Home Office may issue further advice directly to public authorities, telecommunications operators and postal operators as necessary.

This code extends to the United Kingdom. For the avoidance of doubt, the guidance in this code takes precedence over any contrary content of a public authority’s internal advice or guidance.