



1st September 2014

Circular to all Senior Responsible Officers¹ under Chapter 2 of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA 2000) regarding Applicant Errors

Dear Senior Responsible Officer,

The proper application of RIPA 2000 and thorough procedures for operating its provisions, including the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities (for example the police, law enforcement agencies etc.) or by communication service providers² (CSP's).

It is of concern that in the first six month period of the reporting year (January to June 2014) there have been 195 applicant errors - of which 153 (78%) were, according to the reports submitted to IOCCO, caused by the applicant submitting the wrong communications address. In all cases the applicant error led to communications data being acquired relating to members of the public who had no connection to the investigation or operation being undertaken. The public authorities have been instructed to destroy the data that was wrongly acquired in these cases. Regrettably one of these errors led to executive action being taken against a member of the public who had no connection to the investigation being undertaken.

It is worthy to note that should the Interception of Communications Commissioner establish that a person has been adversely affected by any wilful or reckless failure by any person within a public authority exercising or complying with the powers and duties under RIPA 2000 in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected person of the of the existence of the Investigatory Powers Tribunal and its role³.

¹ See paragraph 3.22 of the code of practice accompanying Chapter 2 of Part 1 of RIPA 2000

² See paragraph 6.9 of the code of practice accompanying Chapter 2 of Part 1 of RIPA 2000

³ See sections 65 to 70 of RIPA 2000

Senior Responsible Officers (SROs) are responsible for oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.

It is unsatisfactory to note that the telephone numbers / email addresses / Internet Protocol (IP) addresses were, in the vast majority of cases, derived from records available to the applicant in electronic form and as such could have been electronically copied into the application to ensure accuracy. SROs must develop, implement and robustly enforce measures to require applicants to electronically copy communications addresses into applications when the source is in electronic form (for example forensic reports relating to mobile phones, call data records etc). Communications addresses acquired from other sources must be properly checked to reduce the scope for error. It is not acceptable for public authorities to simply state that applicants have been reminded to double check communications addresses to prevent recurrence.

IOCCO Inspectors will want to be assured during inspections that sufficient measures have been implemented by SROs to minimise the repetition of this type of error.

IOCCO is also in the process of investigating a number of CSP system errors which have resulted in incorrect data being disclosed to a number of public authorities. I thank you for your assistance with those investigations. We will report on the cause and impact of these errors in our 2014 Annual Report.

Joanna Cavan
Head of IOCCO