POL00121550

CONFIDENTIAL: SECURITY, LEGAL

ROYAL MAIL CORPORATE SECURITY
INVESTIGATION COMMUNICATION

6th August 2004

Contents:

1. The meaning of 'Intrusive Surveillance'
2. Livescan Fingerprinting
3. Antecedents
4. Investigation Policy Review Group
5. Safe Working Practices

1. The meaning of 'Intrusive Surveillance'

Some feedback indicates that there is confusion over the definition of 'Intrusive Surveillance' and that this may limit some of the potentially useful surveillance activities of investigators. Corporate Security policy on surveillance states:

'Intrusive' Surveillance *- Surveillance is intrusive only if it is covert surveillance that -*

- *Is carried out in relation to anything taking place on* ***any residential premises or in any private vehicle and***

- *Involves the* ***presence of any individual on the premises or in the vehicle or is carried out by means of a surveillance device***

Royal Mail Group (including Post Office Limited) has no authority under RIPA to perform 'Intrusive' surveillance under any circumstances.

Some investigators have interpreted this to mean that they cannot perform surveillance on suspects who are using their personal vehicle for traveling to/from work or for mail delivery purposes. The key words in the above policy (which are copied from the Codes of Practice) are whether investigators or surveillance devices are ON and/or IN the residential premises or private vehicle.

This means that with the appropriate authority for Directed Surveillance or as an immediate response to an event investigators may observe a private house or vehicle. Investigators will need to ensure that they:

- do not put watching or listening devices inside any private residence or private vehicle;
- do not enter any private residence or private vehicle without the provisions of PACE;
- do not peep through windows or letter box apertures of any private residence unless it is a matter of any person's health and safety;
- do not examine the contents of any private vehicle through the window although a cursory glance to determine whether mail is present for a vehicle which has been used as a conveyance to and from a delivery is acceptable.

Any privacy aspects about looking AT a private house or vehicle should be assessed at the surveillance application stage with particular consideration given to minimising collateral intrusion and the avoidance of using zoom lenses and binoculars to see in. Clearly the intrusive nature of surveilling a vehicle should be less than a house as expectation of privacy by the subject (or any other 3rd party present) will be less.

2. Livescan Fingerprinting

POL00121550

Most custody suites in Police stations are now equipped with Livescan technology allowing the main set of fingerprints, the 'Tenprint' to be taken and stored electronically and be placed on the National Automated Fingerprint Identification System (run by PITO who run the PNC). It also allows marks from crime scenes to be stored.

Currently, the national databases held on the system consist of more than five million sets of prints and over half a million crime scene marks. Later this year, the system will be capable of holding 8.2 million sets of prints and 1.2 million marks from crime scenes.

These databases can be used to make searches in a number of ways:

- 'tenprint' sets from suspects can be searched against the 'tenprint' database to establish if a criminal history is present;
- marks captured from crime scenes can be searched against the national database of tenprints from offenders;
- tenprints from someone in custody can be run through the database of crime scene marks to establish a match; and
- marks taken from a crime scene can be searched against the database of crime scene marks to help link crimes.

There are currently some operational problems in respect of the memory capacity of the Livescan machines themselves. Some machines only have a memory of 100 such applications, some have 1000. One Royal Mail investigator who had a suspect bailed for several weeks at a custody suite where the machine held 300 prints, was told that his prints had "dropped off the memory" when 300 subsequent scans had taken place. This is NOT the case. Scans do not drop of the system, they must be MANUALLY removed.

Investigators are advised then when having marks or 'tenprints' scanned that they ensure (i) that the authorised user of the system clearly understands the purpose of the scanning and (ii) that the facility for adding notes to the scan is employed to ensure that there are instructions such as 'DO NOT DELETE' or 'BAILED FOR 6 WEEKS please contact XXX' etc etc.

3. Antecedents

There was a minor formatting change to the Antecedents form in May (CS033). Any copies printed off before then are not affected. Please replace any electronic versions that may be kept in separate folders or directories.

4. Investigation Policy Review Group (IPRG)

The Investigation Policy Review Group IPRG met on 5th August 2004. The purpose of the group is to review and improve existing investigation policies and guidelines and to identify areas required for clarification and update. Ongoing work is as follows.

- A revised Serious Complaints process has been drafted and will replace the current policy and the Rules and Standards policy. The draft is to be circulated within the group for comment.
- The IPRG is reviewing and comparing the alternatives for accessing the Human Resources Database. While this is taking place:
    i. whichever method is employed, CS219s (or photocopies) must always be sent to Criminal Intelligence to maintain a comprehensive community record of HR access;
    ii. external requests for HR data **must** be forwarded for Criminal Intelligence to deal with;
    iii. Investigation Operation Managers must not authorise AND acquire their own HR data disclosures.

POL00121550

- A safety working party to revise the Safe Working Practices policy and guidelines is to be formed (see below).

Members of the group are Conrad Critchley, Danny Boles, Ray Pratt, Garth McCarron, Ian Diffley, Marcus Copper, Tony Utting, Alan Bartholomew and Steve Pusey. Please provide feedback to them or myself over any issues raised or any other matters of investigatory interest.

5. Safe Working Practices

The IPRG has set up a working party to examine and revise the Safe Working Practices policy, process and guidelines. This will comprise Conrad Critchley, Danny Boles, Steve Pusey, Alan Bartholomew and several nominees at different levels within the investigation operation whose identities will be revealed once they have been consulted. Most teams will be consulted as part of the ensuing exercise to identify, assess and control safety risks on investigation work.

For further information or queries about anything contained in this communication please contact: Conrad Critchley - Tel: GRO, P/L GRO Mobex GRO GRO Mobile GRO