FOI Reference: 617/2012

Request:

Could you please provide me with the following information under the terms of the Freedom of Information Act 2000?

1. Can you please tell me for the year 2011, how many RIPA applications were made by members of your Force in relation to Police Officers' use of Social Media or e-mail?

2. Can you please tell me for the year 2011 what were the relevant offences or Discipline Regulations for these applications?

3. For the year 2011 what was the result of these applications? How many officers were either prosecuted or disciplined?

4. For the year 2011, how many such applications (as above) were refused and on what grounds?

Responses 1-4:

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held.

Where exemptions are relied upon Section 17 of the Freedom of Information Act requires that we provide the applicant with a notice which: a) states that fact b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption applies.

The Dyfed Powys Police Service can neither confirm nor deny that it holds the information you requested as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply, by virtue of the following exemptions:

Section 23(5) Information supplied by, or concerning, certain Security bodies
Section 30(3) Investigations and Proceedings conducted by Public Authorities
Section 31(3) Law Enforcement
Section 40(5) Personal Information
Section 44(2) Information covered by Prohibitions on Disclosure

Sections 44(2), 23(5) and 40(5) are absolute exemptions, which means that the legislators have identified that harm would be caused by release and there is no requirement to consider the public interest test, (except for Section 40(5)).

Sections 30(3) and 31(3) are qualified exemptions and require us to carry out a public interest balancing test before they can be relied upon.

Overall Harm for the Neither Confirm nor Deny (NCND)

The Regulation of Investigatory Powers Act 2000 (RIPA) is often a complex piece of legislation to interpret. The RIPA Act is a regulatory framework around a range of investigatory powers to ensure the powers are used lawfully and in a way that is compatible with the European Conviction on Human Rights. It also requires, in particular, those authorising the use of covert techniques to give proper consideration to whether their use is necessary and proportionate. A legislative scrutiny framework already exists for RIPA activity: Police surveillance activity is subject to annual inspection by the Interception of Communications Commissioners Office (IOCCO) and Office of Surveillance Commissioners (OSC). These inspections assess each constabulary's compliance with the legislation and a full report is submitted to the Prime Minister containing statistical information.

In order to counter criminal activity it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the successful arrest and prosecution of those who commit criminal acts.

The prevention and detection of crime is the foundation upon which policing is built and the police have a clear responsibility to prevent crime and arrest those responsible for committing crime. To do this the police require evidence and that evidence can come from a number of sources, some of which is obtained through covert means.

To confirm or deny any of the police actions around RIPA would undermine on-going investigations, reveal policing techniques, risk the identification of individuals and the possibility of revealing involvement of any exempt bodies.

Revealing information that specific tactics are used in certain circumstances would help subjects avoid detection, and inhibit the prevention and detection of crime. This could either lead to the identification of specific cases or in providing this level of information at force level is likely to result in significantly small authorisation numbers being published and presents a real risk of identifying the resources available to individual departments to covertly monitor individuals likely to be committing offences under their remit. Disclosure would undermine the partnership approach to law enforcement but also, due to the legal constraints under Chapter 1 of Part 1 of the RIPA legislation, it may actually be a criminal offence to do so (Section 19).

To confirm or deny how many RIPA applications have been made relating to police officer's use of social media or email would compromise on-going investigations or identify individuals. If a force applied an exemption to the information this would reveal that these policing techniques and investigative activity had taken place. Conversely, by stating 'no information held' would highlight to an officer that his conduct is not being investigated and that he is free to continue.

It is important the Police Service discloses information regarding surveillance activity under RIPA where it is appropriate to do so, but an officer's conduct may be investigated covertly by the force Professional Standards Department (PSD) without the member of staff knowing of its existence. By confirming or denying that RIPA applications have been made would alert an officer that may or may not be involved in the misuse of social media or email, not only that PSD have the ability to ask for RIPA applications in these circumstances, but that they are aware of his misconduct. The officer would then cease his activity and perhaps make attempts to hide or delete the evidence.

Information compiled for the purposes of an investigation, be it a criminal investigation or internal misconduct hearing, may contain information obtained from individuals to assist with an investigation, which would be in confidence. To disclose investigative information could dissuade people from providing information to the police in future. The public, be they general members of the public or internal police officers or staff, must have confidence that their information is treated sensitively and appropriately. Confirming or denying the information is held could lead to 'trial by media' as it is likely to identify any officers that may or may not be involved.

Public Interest Test

Factors favouring confirmation or denial for Section 30

By confirming or denying that any information relevant to the request exists would enable the public to obtain satisfaction that all investigations are conducted appropriately and that their public money is well spent. Confirming or denying that RIPA is applied to police that misuse social media would increase public scrutiny of police actions and in turn hold the police service to account.

Factors against confirmation or denial for Section 30

By confirming or denying that RIPA applications have been made in instances of police use of social media or email would hinder the prevention or detection of crime and undermine the partnership approach to law enforcement.

Factors favouring confirmation or denial for Section 31

By confirming or denying that RIPA applications have been made in respect of police officers use of social media would enable the public to see where public funds are being spent. Better public awareness may reduce crime or lead to more information from the public.

Factors against confirmation or denial for Section 31

By confirming or denying that any information relevant to the request exists, law enforcement tactics could be compromised which could hinder the prevention and detection of crime and more crime could be committed.

Section 40(5) Personal Information

The duty to neither confirm or deny under this section of the Act arises where the disclosure of the information into the public domain would contravene any of the data protection principles or Section 10 of the Data Protection Act 1998 or would do so if the exemptions in Section 33A(1) of that Act were disregarded.

Disclosure under Freedom of Information is a release of information to the world in general and not an individual applicant. Therefore, simply confirming or not that such information were held would disclose personal information about individuals.

As such any disclosure that identifies an individual or identifies that an individual has had contact with Dyfed Powys Police or not is exempt and would be a clear breach of principle 1 of the Data Protection Act. Personal data is defined under Section 1(1)(e) of the Data Protection Act (1998) as:

"… *Data which relate to a living individual who can be identified-*

(a) from those data, or

(b) *from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual*."

In this case, the confirmation or denial of the existence of information (if any) would breach Principle One of the Data Protection Act (details of which are provided below).

Principle One:

"Personal data shall be processed fairly and lawfully and in particular shall not be processed unless

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data at least one of the conditions in Schedule 3 is also met."

Balance Test

The Police Service will not divulge whether information is or is not held if to do so would undermine on-going investigations or compromise law enforcement. Whilst there is a public interest in the transparency of policing operations and in this case providing assurance that the police service is appropriately and effectively managing the conduct of police officers, there is a very strong public interest in safeguarding the integrity of police investigations and operations.

There is also no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use. The force is already held to account by independent bodies such as The Office of the Surveillance Commissioner and The Interception of Communications Commissioners Office. These inspections assess each constabulary's compliance with the legislation and a full report is submitted to the Prime Minister containing statistical information. Our accountability is therefore not enhanced by confirming or denying that any other information is held.

As much as there is public interest in knowing that policing activity is appropriate and balanced in matters of police officer conduct, this will only be overridden in exceptional circumstances. The points above highlight the merits of neither confirming nor denying the requested data exists. It is appreciated that members of the public will naturally be interested in techniques employed for surveillance. Likewise, we also understand some people believe surveillance (in any form) is used too widely, and therefore an unnecessary intrusion into their privacy. However, taking into account the fact that the Police Service are already scrutinised as detailed above and effective operational law enforcement would be compromised by any disclosure, it is our opinion that for these issues the balance test for confirmation or denial is not made out.

None of the above can be viewed as an inference that any information does or does not exist.