

Report of the Intelligence Services Commissioner for 2014

The Rt Hon Sir Mark Waller

Presented to Parliament pursuant to
section 60(4) of the Regulation of
Investigatory Powers Act 2000

Ordered by the House of Commons to
be printed on 25 June 2015

Laid before the Scottish Parliament by
the Scottish Ministers 25 June 2015

HC 225
SG/2015/74

inappropriate to give details of the way the monitoring works in a public document. Queries arising from these audits were primarily "false positives"; that is although they initially met a search term designed to catch misuse there is, on investigation, a fully justified explanation for their use in each case.

Misuse of Bulk Data

The agencies take any deliberate misuse of the system seriously and sanctions include dismissal, revocation of security clearance and possible criminal prosecution. Any breach of the system may result in a breach notice being issued. When a breach notice is served it remains on a person's personnel file (HR record) and is taken into account in the event of any subsequent breach.

When I first began monitoring misuse of data there were two serious breaches where officers had undertaken unnecessary queries of bulk data with no proper business justification. Both were contractors and in both cases, following investigation they were escorted from the premises and their contract revoked. Fortunately such action is rare but I am very clear that the agencies accept that any inappropriate use is unacceptable and will be treated very seriously.

Unacceptable uses are in fact few in number and not as serious as the cases referred to. For example well intentioned work-related instances such as failure to properly limit the parameters of a search are treated as serious breaches and I have made it clear that this is absolutely right that that should be so.

In MIS a note has been circulated to all users informing them of my recommendation endorsing MIS's policy to tighten up its procedures so that data on staff remains properly protected. The note introduced an automatic security breach if the procedures were not followed. There has not been a single breach in MIS for access to BPD since that note was circulated.

In one recent instance of misuse in SIS an officer accessed the BPD system despite having moved to another role which did not require access. The access was for a legitimate work purpose but still unacceptable and a breach notice was issued. However, I informed SIS that the corporate failure which allowed the officer to retain access to the system was a more serious breach.

BPD systems hold highly personal data and it is vital that staff only have access if they have a business need. The officer should not have been able to retain access to the system after moving post so I have asked SIS:

- to investigate if any more staff have access bulk data when they do not have a business need and to update me on this investigation;
- to inform me what has been done to ensure people are removed from the bulk data register when they move post.

Report of the Intelligence Services Commissioner for 2015

The Rt Hon Sir Mark Waller

Presented to Parliament pursuant to
section 60(4) of the Regulation of
Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed 8 September 2016

Laid before the Scottish Parliament by
the Scottish Ministers 7 September 2016

HC 459
SG/2016/96

Summary by agency

MIS

When I inspect protective monitoring at MIS this extends beyond the use of BPD and I look at protective monitoring measures in place across the organisation. This provides me with reassurance that the system as a whole works. I saw the results of all of the protective monitoring mechanisms in place, including the "false positives" where potential misuse has been flagged but on investigation a valid business justification was provided for the search.

In relation to non-BPD investigations a large proportion of the breaches issued were for searches of operational data which fell outside of the officer's specific remit of work. Throughout the year there were six instances where unauthorised devices had been inserted into MIS systems, for example charging a mobile phone. I take these breaches very seriously and I wanted to know what actions had been taken to prevent reoccurrence. MIS explained that a notice has been circulated re-emphasising that phones cannot be charged at computer terminals. I was also concerned to see that a number of the breaches issued in relation to these non-BPD misuse investigations, as well as one BPD breach, were by individuals who were not permanent MIS staff. It is very important that the parent organisations treat breaches as seriously as MIS do when a breach is issued to a member of their own staff. MIS explained that they had written to the organisations concerned stressing the gravity of the issue and expressed their displeasure at the situation.

I was also keen to understand why the number of breaches had significantly increased in relation to one particular non-BPD database. MIS explained that this was due to a change in the policy which governs what staff are permitted to search for on this database. Staff were not applying the new policy when they ran their searches. I recommended that a warning could be added to the system, or if this was not possible, then a notice should be circulated to remind staff of the new policy and inform them that I am very concerned about the high number of breaches. At my next inspection I do not expect to see such a high number of breaches.

SIS

The protective monitoring arrangements at SIS are highly classified, access to and knowledge of the techniques is highly controlled. Staff who work in this area are subject to additional security screenings before they gain access to the systems or understand the actual checks that are in operation to detect anomalies and misuse of BPD. The results of these checks are monitored by the team who seek additional information or launch investigations if there are any concerns of misuse. They also provide advice and answer any queries from officers in relation to their searches and the justifications required before a search can be run.

In the first half of the year there were no disciplinary cases, moderate or minor breaches at SIS in regards to their use of BPD. In the second half of the year protective monitoring tripwires led to two moderate breaches being issued. Across both periods SIS carried out regular random investigations. These investigations are not generated by protective monitoring tripwires but look at the justifications given for each search to ensure each search is necessary and proportionate. No breaches were issued as a result of these investigations.

Two breaches have occurred in SIS where users were able to use their previous access to BPD in a different role within the organisation. Use of BPD is job specific and BPD access restrictions must be manually updated each time users change roles. To try and prevent such breaches SIS have briefed the IT Access Management team to ensure they are following the correct procedures when users move roles and have updated their BPD Code of Practice and informed all BPD users to say: "If your role changes and you are required to do work that is different to the role described on your original BPD application form, you must consult the data compliance team".

I am particularly impressed at how rigorously the team monitor the use of BPD, the only point I will continue to repeat is that the disciplinary measures for misuse need to be consistent across all three agencies.

In relation to overseeing the use of protective monitoring across areas other than BPD, I was given a summary of the results of protective monitoring and investigations conducted across SIS' corporate network, which was very useful in showing how effective and comprehensive the protective monitoring checks in place are.

GCHQ

Similarly to SIS the protective monitoring arrangements at GCHQ are highly classified and subject to additional security clearance.

This year I was shown the protective monitoring checks that are in place at GCHQ and I was very pleased to see that the level of monitoring in place was exactly what I would want to see. These do not extend over all operational systems, but they do cover all of the key systems including BPD. Although I recognise my statutory oversight in respect to protective monitoring is limited to bulk personal data I would like access to protective monitoring of personal data across all operational systems at GCHQ. As I have discussed in relation to the other two agencies having sight of investigations and breaches detected in other areas outside of BPD helps to provide assurance that the system as a whole is robust. This year GCHQ have shared with me the results of protective monitoring across a number of their other operational systems

In the first half of the year there was no misuse of GCHQ's BPD holdings. There were however 14 investigations which were triggered as a result of the protective monitoring systems. Although GCHQ confirmed that on investigation all of these searches had a legitimate business reason and were both necessary and proportionate, I requested further information about these flagged searches as well as the investigations conducted.

In the second half of the year there was no misuse of GCHQ's BPD holdings, the results of protective monitoring on another operational system were brought to my attention for which there were four investigations, none of which resulted in a breach.

I raised the point as I also did at MIS and SIS that I am keen to see the agencies work together to ensure that misuse of data is sanctioned in the same way. In response to this the agencies have set up a working group to align SIA breach and disciplinary policies and I look forward to learning of its progress in 2016.

**Report of the
Intelligence Services
Commissioner for 2016**

The Rt Hon. Sir Mark Waller

PROTECTIVE MONITORING

In my 2015 Annual Report I provided details of my inspection of the internal controls in place at each intelligence agency. These controls are designed to prevent misuse of data by restricting staff access and ensuring all access to the data is necessary and proportionate, minimising the intrusion into privacy. Each agency proactively conducts protective monitoring to identify any misuse of data, and reports to me instances of misuse.

I am confident that this regime identified misuse of data by staff. The agencies have reported to me any instances of misuse and detailed their investigations into this activity. The breaches identified are typically minor, and I commend the approach taken by the agencies where they have any concerns about the individual involved.

I have been pleased that UKIC has worked to manage the risk of external individuals, such as contractors or secondees working with access to sensitive datasets. The agencies have demonstrated that access controls and safeguards are in place to prevent misuse by these individuals, but have suggested that this continues to be a vital piece of work. I have recommended that MI5 should make it plain to secondees and contractors that they are subject to MI5 rules of conduct regarding access to data and ensure all people working on MI5 premises know the consequences of misuse. This also applies to the other agencies.