BACKGROUND ON BIOMETRICS

Biometrics is the technique of automatically identifying an individual according to their physical or behavioral characteristics. Examples of biometrics which you may be familiar with are iris and retina scanning, fingerprint identification and face and hand recognition geometry.

The development of new biometric technology for identity cards, passports and counter terrorist surveillance have received a huge amount of media coverage in recent years. But some employers are also starting to introduce biometrics in the workplace as a way of monitoring their staff. This development raises a number of concerns for UNISON members who may be concerned at the prospect of biometric information being lost or misused.

Practices such as finger-printing employees as a way of monitoring their time-keeping and sickness absence also raises serious questions about personal privacy and intrusive employment practices. This factsheet seeks to clarify the legal position on biometrics in the workplace and suggests some ways in which your branch might organise around this issue if it becomes relevant locally.

UNISON'S POSITION

UNISON believes that workers should not be subject to unnecessary or intrusive monitoring at work. A “surveillance culture” in the workplace can lead to increased stress, sickness absence and staff turnover. Biometric monitoring, particularly for the purposes of checking on time-keeping, clearly qualifies as an over-the-top and unnecessary measure.

There is also the question of the kind of relationship that employers want to have with their staff. The process of finger-printing is understandably associated with criminality in the public mind. So when employers start fingerprinting their own staff it sends out a very negative and confrontational message. UNISON believes that employers should aim to develop a relationship with staff based on trust – not excessive monitoring.

UNISON is not against all biometric monitoring in all situations. There may be circumstances in which biometric monitoring of staff could be justified on the grounds of security. Each case should be judged on its own merits with the need to avoid excessive monitoring balanced against security concerns. For example, there could be a case for introducing biometric monitoring for staff accessing hazardous materials or extremely sensitive information.

Nevertheless, an exceptional case would need to be made for any new system using biometrics. This should be focused on security rather than monitoring staff and should only be introduced after full and comprehensive consultation with staff and their trade unions.

THE LAW ON BIOMETRICS

Several pieces of legislation are relevant to the issue of biometrics, but of these the Data Protection Act 1998 is the most important. The Act provides a framework to ensure...
that personal information is handled properly and provides individuals with rights, such as the right to find out what personal information is held on them. The Act stipulates that anyone processing personal information must comply with eight principles. They are:

1. **Fair and lawful processing of data**
2. **Processing for limited purposes**
3. Adequate, relevant and non excessive storage of data
4. Keeping data accurate and up to date
5. **Ensuring data is not kept for longer than is necessary**
6. Ensuring data is processed in line with other rights
7. **Keeping data secure**
8. Ensuring data is not transferred to other countries without adequate protection

The first, second, fifth and seventh principles (highlighted) are the most relevant to this issue. The protections they provide are as follows:

- Fair and lawful processing of data requires that employers ensure that staff are informed about and understand the purpose for which their personal data is being processed.
- Holding biometric data for limited purposes means that it should not be used for any purpose not directly related to that for which it was collected.
- The fifth principle requires that personal data is not kept for longer than it is needed. This means that biometric data on staff should be destroyed as soon as they cease to be employed by that employer.
- The security principle means that biometric data should be protected against unauthorised processing and accidental loss, destruction or damage.

The Office of Information Commissioner (The organisation responsible for enforcing the Data Protection Act) has highlighted the issue of “interoperability”. This means that care should be taken to prevent the use of information across different systems. According to the ICO:

> “Even where systems were developed locally, interoperable technologies could allow them to be linked. This could enable the construction of de facto fingerprint databases of large parts of the population. In our view such an enterprise should only be introduced when explicitly authorised by the Government and subject to public debate and appropriate legislation.”

Your employer therefore has a responsibility to make sure the biometric data they keep on staff cannot be easily transferred. Ultimately though, there is nothing in law to stop employers introducing biometric monitoring in the workplace if they satisfy the conditions set out above. Nevertheless, these conditions are intended to set a high standard of data security and so should not be treated lightly.

**BRANCH BEST PRACTICE: WESTMINSTER COUNCIL UNISON**

In August 2008, Westminster Council’s Community Protection Management team installed finger print recognition machines in various workplaces across the borough. This was done without consultation or even notification of staff representatives. About 200 employees in the street management services department were to be asked to provide their fingerprints. A source at the authority said staff would have to swipe a
finger across a wall-mounted box linked to a computer system. The prints would then be logged and matched against staff records.

Local UNISON representatives responded immediately. Branch Secretary Phil Vaughan wrote to the Leader of the Council demanding to know why the machines had been installed without any consultation. He also pointed out that finger printing staff was likely to lower morale, were contrary to Conservative Party Policy (Westminster is a Conservative run Local Authority) and that the machines did not represent value for money.

Local UNISON reps secured local and national media coverage for their campaign against finger printing staff on the BBC and LBC radio. The branch also produced a standard letter for employees to return if requested to give their prints. Management began to realise that they would have to start disciplining people if they wanted them to comply. The standard letter can be downloaded here: http://www.westminsterunison.org.uk/multiattachments/2505/DocumentName/FPrintLetter.doc

Phil Vaughan eventually met with Westminster’s Chief Executive to explain why the union opposed the policy, and that UNISON members would be refusing to provide their finger prints. Following the meeting the Chief Executive wrote to the Branch stating that Community Protection management “will remove the machinery from current locations” and “will not pursue the use of machines in the Community Protection service in the foreseeable future.”

Branch Secretary Phil Vaughan said in reaction: “We are obviously very pleased with this decision, and are now keen to engage with local managers on other ways in which time monitoring can be done without biometric technology.”

ORGANISING AND CAMPAIGNING

If your employer proposes introducing biometric monitoring in your work place your branch can make sure members voices are heard. Here are some tips on how to organise around this issue:

**Find out what is going on**
Before you campaign and organise around this issue, you need to get all the facts. Issues you may want to concentrate on are:

- Branch reps should find out why management is seeking to introduce biometric monitoring. Is it for particular security reasons? Or is it just to monitor staff?
- Will a full consultation be conducted before any biometric monitoring is introduced?
- Who is going to be monitored? Is it all staff, or just particular departments? Will a full equality impact assessment been carried out?
- How much will biometric monitoring cost to introduce? Does it represent value for money?
- Will the system guard against “interoperability”? (see above). What specific purpose is the data being kept for. Will it be destroyed when employees leave? If the answer is no to any of these question, your employers proposals may well breach data protection law.

**Consulting members**
It’s important to find out what members think about biometrics in their workplace. They may be extremely angry at the prospect of being finger-printed or, if there are Bargaining Support Group e-mail: bsg@unison.co.uk
particular security issues, they may understand the need for changes. Your branch should tailor its response to the views of members. You could:

- get out and talk to members face to face
- send around a brief survey on the issue (either by e-mail or hard copy)
- report back to members on the results of any branch consultation

Represent members
You could:
- write to managers setting out the views of members
- call for a face to face meeting with managers to put across members views
- Present managers with the results of your branch consultation

Campaign in the Media
Biometrics is an issue which may well be of interest to local or even national media. If members are opposed to its introduction, some steps you might like to take are:

- Speak to your region. They will have media contacts which can help highlight your cause.
- Draft a press release. Depending on your usual procedure, send it out directly or via your regional media contact
- Encourage concerned members to write to their local paper

Organise members

- Try to identify non-members who are concerned about this issue. You may be able to convince them to join UNISON
- You could produce a standard letter for UNISON members to respond to management requests to provide biometric information.
- Depending on circumstances and the views of members, you could inform managers that UNISON members will refuse to give any biometric data needed for monitoring to take place.
- If your branch has a website and e-mail list, make sure you use them to keep members updated.
- Talk to members wherever possible to find out what they think of the campaign

WORKING TOGETHER

If your branch has campaigned against biometrics or even if your employer is considering introducing it, let us know about it at Bargaining Support. By sharing information your branch can help the union to spread best practice, identify obstructive employers and monitor the implementation of employment rights. Please forward any information to the Bargaining Support Group at bsg@unison.co.uk or UNISON Centre, 130 Euston Road, London NW1 2AY.
FURTHER INFORMATION

The website of the Office of the Information Commissioner – http://www.ico.gov.uk/

Home Office Biometric website (mainly focused on anti-terror measures but does contain technical information)
http://www.dti.gov.uk/employment/workandfamilies/maternity-leave-pay

European Biometrics Forum http://www.eubiometricsforum.com/

The International Biometric Foundation website: http://www.ibfoundation.com/