Ref: DPO/COMP/17

This is a summary of the Decision of the Commissioner.

I received a complaint from three trade unions concerning the use of fingerprint for attendance of employees without their consent against two respondents. The complainants would like to stop this process as they consider it to be unlawful.

My office opened an inquiry and the respondents were required to explain about their fingerprint attendance systems. A notice was served to both respondents to obtain the consent of employees before processing their fingerprint data or else to provide an alternative means of taking attendance for employees who did not consent. Respondent no.1 complied with the notice while respondent no. 2 did not.

By definition, any biometric collection of personal information has implications for privacy. These initiatives can also affect privacy in other ways, including affecting people's human dignity or expectations of anonymity. Therefore, before deploying a new biometric system with implications for privacy, an organisation should be able to clearly justify the prospective privacy intrusions. Many countries have rejected the imposition of fingerprint technology as a mandatory means to secure attendance. To guide this analysis, our office applies a four part test which represents the international standards applicable at European level and is also reflected in a 1986 Supreme Court of Canada decision, *R. v. Oakes.* The test weighs the appropriateness of a potentially privacy-invasive measure in light of four questions:

"1. Is the measure demonstrably necessary to meet a specific need?

2.Is it likely to be effective in meeting that need?

3.Would the loss of privacy be proportionate to the benefit gained?

4.Is there a less privacy-invasive way of achieving the same end?"

Necessity:-
Because there are privacy issues associated with all biometric systems, a proposed system should not be adopted *simply* because it appears to be the most convenient or cost-effective option. Instead, organisations proposing a biometric solution have to determine what specific problem they hope to solve, and whether the proposed system is essential for satisfying the need.

Effectiveness:-
A second consideration is whether the proposed biometric system is likely to be effective in meeting the identified need. Different biometric characteristics have attributes that can make them more or less appropriate for specific purposes. For

example, facial recognition systems are popular, in part because of the wide availability of passport photos and other facial images in databases - not to mention pictures that can be captured covertly. And yet, because facial features are neither permanent nor unique, facial recognition systems cannot be counted on to identify people with a high degree of certainty.

Proportionality :-

All biometric systems involve some loss of privacy because personal information is stored and used for authentication. In analysing the appropriateness of a proposed biometrics measure, a third consideration is whether the resulting loss of privacy would be proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy may not be appropriate.

In testing for proportionality, organisations should bear in mind that certain biometric characteristics are more privacy-sensitive than others. Fingerprints, for example, are especially sensitive because they can be collected covertly, linked across applications and databases, and used in law enforcement. Any proposal to use fingerprints in a biometric initiative would, therefore, have to promise *extraordinary benefits.*

It is thus proven beyond reasonable doubt by complainants, applying the above principles that the use of fingerprints for attendance purposes by Respondent No.2 regarding those who have not expressly consented to it cannot be deemed to be in strict compliance of the letter of section 22 of the Data Protection Act and cannot fall within the purview of the employment contract as provided either under section 24 or 25 of the Data Protection Act.

The fact that many public and/or private organisations are using fingerprinting technology for attendance purposes because it represents a cost-effective and convenient means to record attendance should not potentially and materially undermine in any way whatsoever the right of the data subject not to consent to this method and further be prejudiced or discriminated for not conforming to it. This case illustrates the modern flow of sacrificing privacy rights at the altar of technology without understanding and measuring the negative consequences which technology can also give rise to. Technology is certainly to be used but not abused. The matter is thus referred to the police under section 20 of the Data Protection Act for prosecution against the Chief Executive Officer of Respondent No.2.

Date :17.07.2013.