



**PRESS RELEASE: 23.08.11**

**IRM Reaction to 'Privacy Laws Fail to Stop Data Abuse' <sup>1</sup>by Aiden Radnedge**

**Written by Punam Tiwari, IRM Legal Counsel**



Metro's Aidan Radnedge has touched on one of the most important aspects of our lives - privacy.

The earliest definition of privacy under English law is "the right to be left alone". Because there is no right to privacy at common law, the Courts adopted various other methods of defending the privacy of an individual or that of an individual's data, including trespass of the person, and contractual and tortious breach of one's confidence. The problem with relying upon these methods of protection was that they were cumbersome and only available for the wealthy few.

Article 8 of the Human Rights Act 1998 tried to establish a positive right to privacy in English law both at home and in the workplace. Again this proved somewhat inaccessible.

Subsequently, the purpose behind the Data Protection Act 1998 ("the Act") was to protect individuals from the increasing computerisation of our community by protecting information recorded in a processed form by equipment operating automatically. The common complaint against the Act, as has been mentioned in the article, is that it is unnecessarily complicated and lacks common commerciality.

What with most of our data now being accessible in electronic form, be that in a polling station or in a library, it is imperative that the Act be revised so that it is more comprehensive for non-lawyers.

Having said that, the Act cannot be deemed completely negative. The writer of the article does not appreciate that the Act succeeds in defining a variety of data and whilst not prescriptive does succeed in establishing some sound principles, which prior to its existence, had not been set out for employers or government bodies.

There is a difference between "personal data" which is defined as "data that relates to a living individual who can be identified from that data" and "sensitive data" which includes, but is not limited to, racial origin, political opinions, religious beliefs, health conditions and one's sexuality.

The core difference between the two types of data is that with "personal data", provided always that the data protection principles set out in the Act are adhered to, namely that the data is processed fairly and lawfully and that it remains adequate, relevant and accurate, contrary to popular belief, a "data controller" (the party who decides on the purpose and manner in which the data is processed) may process information on a data subject how he sees fit.

Greater legal protection is granted to "sensitive data", namely that the data controller is required to obtain explicit consent rather than implied consent and enhanced security measures must be in place to protect such data.

This distinction between the two types of data enables the employer or government body to do their job, whilst respecting an individual's rights to privacy.

---

<sup>1</sup> Metro, 14/08/2011



Ultimately, the purpose behind the Act is to establish good practices, rather than a prescriptive methodology, that data controllers can adopt and comply with in order to protect the data that they are holding, reflecting both their interests and those of the data subjects. This is surely a positive thing.

There is a suggestion in the article that there is no recourse against those who are in breach of the Act, but in fact a breach of the Act is a criminal offence and an officer of a company which is found to be in breach of the Act could be personally liable not just to pay a fine but also to face the wrath of the criminal courts. This threat alone seems to me to be enough to ward off those who do not take the Act seriously.

Certainly better measures do need to be implemented into companies and government departments to make sure that the mistake that happened in 2007 with the 3 million learner drivers' details does not get lost again, but this can only happen with time and greater investment in security methods and training for employees.

**ENDS**

---

#### **Notes to Editors**

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy with 13 years experience working with large enterprises, helping our clients identify and mitigate the risks inherent in today's increasingly interconnected business environments.

Today our portfolio includes a wide range of technical assurance services, complemented with a wealth of security management and risk assessment options, covering the full spectrum of our clients' information security requirements.

For further information, please contact IRM on:

Tel: +44 (0)20 7808 6420

Email: [press@irmplc.com](mailto:press@irmplc.com)

Website: [www.irmplc.com](http://www.irmplc.com)

Twitter: #IRM\_tweet