

Information Overload

Issue 60, August 2007

Welcome:

Welcome to the August edition of Information Overload. We live in a very connected society. Just do a quick search on one of the many Internet search engines for your name and you will be both amazed and a little concerned what information is stored about you – in a very public forum.

The questions I would like to pose today are: Is Big Brother inevitable? Who has access to the material? And is that a good thing? We will look in particular at the problems we face when incorrect labels are attached to our metadata, and ask – can we do anything about it?

We would like to thank you in advance for forwarding this edition onto friends, colleagues and other interested readers. Please note that all back issues of this edition, as well as our registrant resources edition can be read and/or downloaded from our web site – <http://www.iea.com.au/web/Publications> should any of the topics be of interest and use.

Lorraine Bradshaw
Marketing Coordinator and Projects Officer

In this Issue we will be looking at:

- Big Brother is watching you. And you, and you, and you!
- Growth of surveillance
- Sharing services and resources.
- The digital concerns
- A Thought to ponder

Big Brother is watching you. And you, and you, and you!

I had to go to the doctor's the other week, the usual round of colds and flu had struck the office, and I needed to make sure that what I had, hadn't turned into something that needed something a little stronger than the over the counter prescription medication that I was taking. When the receptionist looked at my record on the screen, she commented that I didn't look like a veteran.... Now I don't know whether she had incorrectly input the information into their particular system or whether that information was imported from elsewhere, but it did get me thinking.

Whilst this particular "problem" was easily fixed, can you imagine what would happen if that information was stored in a central database, linked to social services, the armed forces and the many hospitals that cover our planet. Would I have been given more money for being a "veteran", then have to pay it back when they found out I wasn't. Would I be getting a visit from the forces, because I was AWOL from barracks, and would I be administered the right

kind of treatment and drugs – or should those treatments and drugs have been administered to someone else? And what impact would those drugs I should not have had in the first place would have on those drugs I was already taking?

Given the latest round of debates regarding a National Database to house the information on the proposed National ID Scheme (more later) it does pose some interesting thoughts and questions regarding the quality of the information that we store.

Growth of Surveillance:

In the United Kingdom, more than 4.2 million closed circuit televisions monitor people's movements. It has been estimated that the normal London dweller gets captured on camera approximately 300 times per day. Whilst it can be argued that these cameras will also capture the criminal activities, are we legislating for the minority?

Also in the UK, the national DNA Database contains information on approximately 6% of the UK's current population, and this will increase as the Government insists that every person who holds a passport submit to having 52 pieces of additional information held – including finger prints and Iris Scan's when those passports need replacing.

It is also interesting to note that there is also talk of introducing a National ID Card. The reason being, that the Government believes that it is important to prevent ID Theft, Crime and Terrorism and that the public must be willing to give up some personal liberty. Opponents are worried that the new super computers will be a one-stop shop for these same groups to hack into in order to steal information from.

The timeline for the growth of surveillance:

- 1984: DNA fingerprinting method discovered by accident by Sir Alec Jeffreys
- 1985: Outdoor CCTV camera erected in Bournemouth
- 1995: The world's first National DNA Database established in England and Wales.
- 2001: Sir Alec Jeffreys calls for profiles of entire UK population to be held
- 2004: Number of DNA profiles hits the two million mark
- 2004: Information Commissioner Richard Thomas warns that Britain is 'sleepwalking into a surveillance society'
- 2005: MPs vote to introduce identity cards
- 2006: National Black Police Association call for inquiry into why black people are over represented on DNA database
- 2006: Identity Cards Act becomes law
- 2007: Data-sharing by Whitehall departments likely to be introduced
- 2008: Foreign nationals will have to start supplying fingerprints, eye or facial scans added to a National Identity register
- 2008: Children's database, covering all under-16s in England and Wales, will be launched
- 2009: The first biometric identity cards will be issued to British citizens when they renew their passport
- 2010: NHS Database will store the records of 50 million patients providing details over the internet
- 2012?: ID cards compulsory
- <http://news.independent.co.uk/uk/politics/article2154844.ece>

The opponents of the scheme are not alone in their concerns. Back in October 2005, Jerry Fishenden a senior Microsoft Official said "the plans for a central national identity register could lead to "huge potential breaches" and a leakage of personal information." Fishenden

went onto state “no systems are ever completely secure” and warned that putting vast amounts of personal data and biometric information such as iris, fingerprint and facial scans into one central database could prove too tempting a target for hackers and other criminals. http://news.com.com/2100-7348_3-5900411.html

It is also interesting to note, that the current biometric system being proposed has trouble identifying groups of people. Apparently brown eyes cause the system problems, as does manual workers who wear down their fingerprints. http://news.com.com/2100-7348_3-5900411.html

One of the main reasons given for supporting some form of national ID card regime is the increased security demanded by the United States of America, especially after the terrorist attacks of September 11, 2001. The logic goes that if the U.S. and other countries demand a higher level of travel document security, or require biometric information in passports in order to be allowed into the country, the remaining countries will have no choice but to 'join the trend'.

It is interesting to note however, that the planned UK's mega database has been shelved for the time being, along with the requirement to have iris scan's as part of the identification process, the ID card programme will forge ahead in one form or another, especially if we have to comply with the United States requirements. For those of you who have not travelled into the US recently, IRIS scans and fingerprints are already obtained from visitors, along with information from passports.

http://news.com.com/U.K.+ditches+ID+card+megadatabase/2100-7348_3-6145027.html?tag=topicIndex

And before you think that it cannot happen here. Debate regarding the introduction of a national ID scheme has been raging for years. What is interesting to note is that the processes may have already begun!

Sharing Services and Resources: The First Step towards a National ID Card?

Here in Australia it has been proposed by the Federal Government that it introduces what has been termed “The Human Services Access Card Scheme”. The aim of the scheme is to get rid of the many different cards and replace it with a single card, incorporating data from the Medicare system, Veterans Affairs and Numerous other benefit cards issued by Centrelink, and storing the information in a central location. http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html

Given that it is estimated that Centrelink has 275Km of records and Medicare – 3 square kilometres of records you can see why the government would be interested in keeping it all electronically. It is also interesting to note, that it has also been estimated that it would take approx 100 TerraBytes of storage to hold the information if it is digitised. (Note: The Public Records Office of Victoria used 11TB of storage to store electronic copies of 44km worth of paper records). <http://www.australianit.news.com.au/story/0,24897,20752199-15306,00.html>

In Western Australia the government has created the Office of Shared Services whereby some of the functions normally handled by individual government agencies, are now amalgamated into one central point including Finance and Human Resources, as well as

payroll, procurement and project billing. The recently created Office now looks after approximately 100 government agencies, with further rollouts planned to include Workers Compensation, Occupational Health & Safety, Time and Labour and Reporting and Labour Relations added to the mix.

Whether the new card will go ahead or not, and at what cost, or whether the card will contain the biometric information or not, will be debated by many. As an information professional, I would like to look at this issue from another level.

The Digital Concerns:

Now is not the place to discuss the rights or wrongs of monitoring our movements, buying behaviours, television viewing habits, types of medication we take and where we have it administered – as can be currently determined through monitoring credit card payments and CCTV footage, rather as information professionals – the types and quality of the information we are being asked to store, classify and retrieve. Including:

1. **The quality of the data input.** If the wrong information is entered into the system then the wrong results / conclusions can be drawn from that information. Consider that the data entry operator was tired s/he typed in a wrong code into the wrong field that simply wasn't picked up. Consider also the global predilection to give very alternative names to their offspring, not to mention the various spellings of some of the more popular names, it can be a logistical nightmare to check the spelling variations against the spider scrawl most people use as their handwriting. Can we guarantee that the record you are looking at is actually the person standing in front of you?
 - a. By the way - did you know that the 3 of the most popular names given to boys in the UK last year was not in fact John, Fred or Justin, but Mohammed, Muhammad and Mohammed.
(http://www.statistics.gov.uk/specials/babiesnames_boys.asp).
2. **The quality of the data retrieval.** Imagine that your medical records were online, and you had a serious accident at work. Imagine then that your name is John Smith. The hospital staff noted that you were male, you had brown eyes, brown hair, weighed approximately 100 kilos and lived in Perth, Western Australia. But because they were busy, hadn't slept in 2 days and didn't bother to verify that your middle name was Eugene, or that your date of birth was correct, they administered the wrong treatment to you, and you died. Had they pulled up the correct record for John Eugene Smith, they would have seen you were in fact allergic to that particular drug, but because they assumed the data was correct and given that you in your pain were in fact delirious and didn't know what was being asked of them, or worse still you were unconscious when they started so couldn't answer their questions, begs the question – what safety checks are in place to ensure those errors cannot in fact occur.
3. **The system goes down.** We've all had instances whereby power failures, system failures, software crashes have occurred. How can you retrieve the information if it's only in electronic format?
4. **The organisation decides to upgrade their software and hardware capabilities.** But rather than test to see if the data transfers correctly, a global dump is done. Backs are slapped for a job well done – on time and under budget. Except there are actually gaps in the metadata as they forget to mention that the

two systems were not entirely compatible, and a few bits got missed off the transfer process.

5. **Someone installed the software without deleting the admin passwords supplied by the vendor.** Of course the hackers, crackers and opportunist thieves know about these and happily dive into the new system rifling through the content, changing information, removing information they don't want anyone to know about. And if you think I am being fanciful – consider the rather embarrassing news story regarding that world famous Encyclopaedia. It has been revealed that a host of blue chip companies, religious bodies and government organisations have been exposed for making heavily biased edits. <http://www.idm.net.au/story.asp?id=8731>
6. **How are we going to guarantee that we will be able to access the electronic information once it has been archived and no longer in the realm of day-to-day operations?** Or will everything remain live? Given the size of the planned programmes, we are talking bigger than terabytes of information. What's bigger than a terabyte? Actually – a Google !! but that's another story !!
7. **Will the new technology deliver what it says it will deliver?**
8. **Who will benefit from the rollout?** The companies creating the smart cards, the companies creating the software that drives it, the companies creating the mega databases (hardware and programming), or the government in saved duplication of services. Whilst we could talk about the numerous job losses that are likely as a result of the amalgamation in terms of fairness or not; consider what would happen if one (or more) of those laid off, disgruntled employees decided to delete some / all of the information, plant a virus, email details of passwords to known criminal groups as retaliation!

Whilst I am aware that there are inherent problems trying to maintain and store the mountains of trees that we have stuffed in boxes, the problems associated with rodent infestation, destruction through fire and water, shredding and mis-filing items notwithstanding, we can – assuming none of the above actually occurs, maintain access to our paper records for millennia. We still do not have those guarantees when it comes to our electronic records.

It's also interesting to note that it is a little harder to search for every instance of your name within the various legacy systems, and change them all in one go – as can be the case with a national database, for instance. And if we can delete the records of the people surely it can be argued that it is a small step away from deleting the people associated with the original records – especially if you are intent on infiltration, crime, terrorism, "sleepers" and all those other scarily portrayed instances throughout the fictional realm of movie producers and writers the world over.

As always we hope we have given you food for thought, let the debate continue.

A Thought to Ponder:

“What we call ‘progress’ is the exchange of one nuisance for another nuisance.”

Havelock Ellis (1859 - 1939)

Your comments and suggestions on the subject of this newsletter are most welcome. Or if you would like to see other issues covered in future editions, please email me at training@iea.com.au. Please feel free to pass on this newsletter to your colleagues' friends and associates. To subscribe they should send an e-mail to training@iea.com.au with “subscribe newsletter” in the subject line.

If you have any suggestions as to what should be included in future editions, then please send an email to training@iea.com.au. If you would prefer not to receive this newsletter, please send an email to training@iea.com.au with “unsubscribe newsletter” in the subject line.