

High anxiety

Wendy R London

Introduction

All we talk about is "new technology". After all, isn't that what makes our personal lives easier and our employers more competitive? Isn't that what gives television the opportunity to show us programmes like "Beyond 2000"? And isn't that what gives people like us who are interested in security something to talk about over pints at the pub? Well, it isn't quite time to go to the pub yet, so let's talk about it here for a few minutes.

We are in a time when we simply cannot monitor and control all the new technology, applications, variations and changes that occur day-by-day. The more powerful the technology, the greater the potential for building on itself - computerised computerisation. But unless we *tell* the computer to do it, it won't try to secure itself. So we have to do it. We have to learn how to monitor, control and log the security aspects of the new technology without sacrificing its potential, spending disproportionate time or money doing it or, as a consequence, causing other problems. Also, while any given technology may look secure and non-threatening on its own, it may be terribly insecure when working in tandem with other technology, or interconnected with it.

And the issues aren't just technological ones. They are also legal ones - thereby re-opening the age old debate of: Is Technology Pushing Law, or Is Law Pushing Technology? Beats me.

I am not going to go into any detail, but I am going to tell you about some of the problems.

Examples

Neutral networks

These are the boxes that *can* reprogram themselves, so what happens if New Scotland Yard uses a neutral network for its investigation into the latest teenage biscuit snatcher and decides that the criminal is a 10 year old, 5 foot tall, fair-haired boy called "Sam" ... but the network decides that Sam is a girl's name (that's short for Samantha) and nicks all the girls of that description in the neighbourhood. Would the old-fashioned cop walking the beat make the same mistake? Did the neutral network simply get it wrong - but ended up violating the rights of young girls because there was no reasonable cause to arrest them?

Credit reporting

Similar issue. Computers can crunch numbers in a way that we can't. They are so good at it that certain businesses rely on them to make decisions for them. Like credit reporting organisations. Well, what if they get it wrong and the mortgage for your A-Frame ski chalet at Mt Buller gets buried in an avalanche of wrong data - e.g. you were never the occupant of 100 M-A-I-N Street, but of 100 M-A-I-N-E Street and accordingly, *you* get tagged as the deadbeat? At least with the relatively new phenomenon of data protection legislation there is an obligation to make sure that data gets corrected, but what about the average person who has no knowledge of the law or lives in a country where there are no such laws?

Telephone bills

Here's a famous one. In the beginning, I really don't know what the fuss was about since in the United States we have *always* had telephone numbers printed on bills. But then again, our fathers didn't *usually* have French mistresses ...

Road pricing chips

Another similar example. Road pricing chips are terrific as an efficient means for assessing tolls and road use taxes. But:

What happens when you inadvertently leave your itemised statement in full view on the kitchen table at home; or

Your movements just happen to match those of the neighbourhood's infamous Don Juan.

Wheelie bins

I like this one. I just heard that three city councils in Greater Melbourne are implanting the same road pricing chips in peoples' wheelie bins so that if one escapes, it can be traced. Good one. Richard Nixon would have had trouble explaining away the gap in his rubbish.

Phone numbers for life

Constantly at the mercy of the automatic diallers trying to sell double-glazing?

Hand scanners at the immigration queue?

Perhaps only a toe in the door, but clearly a move to a personal identity card: the hand print has to match the print embedded in the identity card ... which may have been corrupted (it's been ages since the swipe strip on my Amex card has worked properly), or the card has been inadvertently (or purposely) switched, or the data entry for that card might have been done inaccurately so that your name is now Rupert Murdoch but your hand print isn't (nor are you, for that matter).

A mighty web we weave

One wrong piece of data entered and the entire lattice gets blown away. A wrong assumption can make for a cultural-social-organisational-political

Nightmare. Take for example the poor guy who made lots of phone calls to Waco, Texas on his American Express card and just happened to buy a Bible in Omaha, Nebraska. The FBI thought it was kind of weird ...

GSM

GSM can be considered the beacon of the encryption movement. To be frank, I'm not too keen on driving around Parliament at 7.00 in the evening carrying on a conversation with a friend on my (hands-free) car phone ... only to have two other people waft in, talking about their secret rendezvous in some Greek island. Nothing illegal (as far as I know), but I don't ordinarily correspond on postcards either (unless I am on a Greek island). If I wanted the world to know what I am doing, I would use postcards, but I prefer to 'encrypt' my letters by using self-sealing envelopes. So why should telephones be different? Yes, I accept the argument about making sure that they are not being used for nefarious purposes, especially after learning that the number of organised crime organisations in the Netherlands has grown from *one* when I lived there in 1982-1983 to 79 today, but *what price crime detection?*

Trap doors

Invariably, the subject of trap doors comes up. The FBI, GCHQ, MI5 and even the telcos themselves - all being in the communications industry (one way or another) - can't even begin to comprehend life without snooping. All in the name of crime detection. (After all, what would they do all day?) I am all for putting the drug barons and the car thieves and the money launderers out of business, but I'm not too sure that I want my legitimate conversations being intercepted by a listening device that a twelve year old could crack by reading instructions which are less complicated than the ones for my new videotape recorder. It may be a conversation about my next secret rendezvous at Noosa, or about some multi-million dollar deal I am cutting for new technology.

Smart cards

Here's a good one. In my firm, you have to exert yourself physically to rummage through your briefcase or handbag or pockets to find your security pass to use the shortcut through the middle of the building or enter the building after hours. However, I've been to firms where you don't need to produce it at all, but merely walk through airport-type security gates which will 'read' your smart card through layers of briefcases and handbags and pockets. I suppose that this is reasonable if there is only one checkpoint in the building (i.e. at the entrance) but where there is more than one checkpoint, for example to expedite building evacuation procedures, then I get a little twitchy. Some security officer somewhere in the basement of the building need only read through the daily movements log to find out that I was with the Managing Director for 16.5 minutes, that I stopped by Fred's room for a three hour chat, and that I nipped out of the building for 46 unexplained minutes in the middle of the afternoon.

The Legal Bulletin Board

The *American Bar Association Journal* reported a story a couple of years ago about a New Jersey lawyer (coincidence, I assure you) who gives legal advice over a bulletin board. Can the bulletin board owner provide hermetically sealed security to prevent someone from tampering with that advice to prevent Aunt Daisy from leaving her \$16 million estate to her Cat ... rather than Cath?

TV monitor cameras in city centres

Again, we must balance our need for greater security with our right to privacy. TV monitor cameras are being installed in city centres for the very appropriate reason of safeguarding the public safety, but who or what is safeguarding our privacy? What controls have been put into place? I'm afraid our technology isn't so clever yet that cameras will turn themselves on only when a criminal walks by.

Safeguards

I think you get the picture. But what can we do, or what is being done? I think it is worth having a quick look at the November 1992 *Guidelines for the Security of Information Systems* issued by the OECD, not so much for analysing what they say (because that is not within the scope of this talk) but for beginning to gain a sense of how these problems are beginning to be tackled.

The stated purpose of the Guidelines, which apply to all information systems, emphasises the need to engender co-operation between the private and public sectors in the development and use of information systems, the development and implementation of security measures for those information systems and the promotion of confidence in their use. The objective of the *Guidelines* is "the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality and integrity". And in nine brief principles, the *Guidelines* set out what I believe should be our creed for ensuring that our information systems are no more threatening than books, nor more vulnerable than libraries. These principles are:

1. Accountability principle

Individuals who own, provide and use information systems should have their responsibilities made explicit.

2. Awareness principle

In order for confidence in information systems to be acquired, everybody who comes in contact with them should acquire "appropriate" knowledge of and be informed about the security measures, practices and procedures in force.

3. Ethics principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

High anxiety

4. Multidisciplinary principle

Measures, practices and procedures for security should take into account and address *all* relevant viewpoints: technical, administrative, organisational, operational, commercial, educational and legal.

5. Proportionality principle

The cost and level of security should be proportionate to the reliance on the information systems, the potential for harm and the actual requirements for security in that given information system.

6. Integration principle

A coherent regime should be adopted through the integration of all measures, practices and procedures available in the organisation.

7. Timeliness principle

Breaches in information systems security should be addressed in a timely and co-ordinated manner by national and international public and private bodies.

8. Reassessment principle

Because security requirements will vary over time, security measures, practices and procedures should be reassessed periodically.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

Summing up

Information systems are everywhere and they govern everything that we do. They exist as stand-alone, discrete desktop PCs and as mainframes connected to vast networks by satellites and telephone lines and fibre optic links. They contribute to the quality of life, but they also have the potential of degrading it. Unless and until we take a balanced and realistic view of how to *manage* them, they will manage us.


Wendy London is Head of the Information Media and Communication Group of Price Brent (Solicitors) Melbourne office. Wendy is an American-qualified lawyer and librarian who was the IT Director for City of London firm, Cameron Markby Hewitt for five years and a lawyer in the firm's Technology Group for two. Prior to joining Price Brent in August 1995, Wendy was a Visiting Fellow at the London School of Economics where she lectured on the legal and organisational aspects of information security and a Senior Principal Consultant with Oracle Corporation (UK) Limited where she headed up the Legal and Regulatory Group. Wendy is a Fellow-Elect of the College of Law Practice Management, Vice-Chair of Committee 10 (Professional Development and Technology) of the International Bar Association (IBA) and a committee officer of Committee R (Computer Law) of the IBA. She is past Managing Editor of *Computers and Law* published by the UK Society of Computers and Law, is on the editorial panel of several computer security publications and frequently writes and speaks internationally on computer law and computers in the law. This is an edited version of a presentation made by Wendy at a 1995 Victorian Society for Computers and the Law seminar.

IN OUR NEXT ISSUE...

Our next issue looks at

THE INTERNET

Contributions from members of all Societies are welcome. Although this is the central theme of the issue, contributions can be on any topic relating to computers and law and can take the form of an article, product or book review, abstract or press release.

 Please send your contributions to the Editors no later than 15 April 1996.