Nostrum remedium - or Government quackery

MADELEINE WESTROP on the frightening extent and incompetence of e-Government

IT IS FUNNY that at the turn of a century something new often becomes all the rage and is seen as having miraculous qualities that will solve all our problems, only for us bitterly to regret the application of it a few years later.

Take radium which was sold in many patent tonics. Radium was considered healthy because after Marie Curie identified it in 1898, it was discovered to be 'naturally occurring' in spa-waters. Natural things must be good for you, surely? Advertisements promised this or that elixir contained genuine doses of radioactivity. Trading Standards penalised companies who sold phoney, instead of real, radium.

One playboy industrialist, who drank copious doses of Radithor (Certified Radium Water) as a tonic, became so ill that his jaw had to be cut away and then he died. The Radium Girls who painted clock faces with luminous figures ended up with luminous faces themselves. Of course, we know now how toxic the stuff is. In 1934, Madame Curie herself died from years of repeated exposure.

We have done the same thing with Information Technology (IT). I am an IT security professional in the public sector. In public affairs, IT is as toxic as Radithor. And, because it is the turn of a century, or possibly because New Labour was gullible about anything shiny and new, we have embraced IT in public life as enthusiastically and fatally as we embraced Radium, lead piping and asbestos in days gone by.

New Labour calls this eGov and it cannot work because it is too big. The biggest project is a £12.4 billion National Health Service (NHS) system that does not work. There is also the Identity (ID) card system, the pensioner system, the failed trainee doctor system and Contact Point for children.

By 31 March this year all local authorities must connect to a Government system, Government Connect, so that welfare information will be shared between local and central government.

There is so much wrong with this from the point of view of democracy, civil liberty and privacy. But, for brevity, I just want to say what is wrong with just one aspect of the security of this: the danger to the individual because his identity will always be lost, mislaid or deliberately misused. When we tell Government things about ourselves, it has a duty of trust to look after the information securely. This duty is just as important as their duty to defend the realm or the duty not to squander our money. The threat to individual liberty when identities are subverted is manifold and I shall try to explain why with just a few examples.

Take the latest plan. Some councils want to open shops up in an imaginary world called 'Second Life'. This is a game played on the Internet by millions of people around the world. One person can make his own mini-me digital character (or even a whole load of them) and these characters can meet and play together in a computer-generated world, on the Internet. Some six million people around the world choose their appearance, meet others, act out fantasies, gamble and run real businesses, buy property and meet friends, have PC-screen sex and spend money.

. . . because New Labour was gullible about anything shiny and new, we have embraced IT in public life as enthusiastically and fatally as we embraced Radium, lead piping and asbestos in days gone by.

It is a mostly licentious, unmoderated world where you cannot know the true identity of anyone; or even know if many different digital people are the same real person. Because there is gaming and real money, some of the digital people are in fact Federal Bureau of Information (FBI) agents spying on the activities of others. Computing and the sex trade feature largely. Some people pay their college fees by being a 'virtual prostitute' on Second Life.

The law still applies in this world (although jurisdiction is complicated). There have already been divorces when adultery is discovered in Second Life and law suits for breach of copyright there. The biggest problem is proving who anyone actually is (that is to say, who made and controls which digital character).

Sky News discovered an area called "Wonderland", which is a playground where paedophiles can pick up digital children - the digital children may be the *alter egos* of real adults pretending to be children. This is a crime in some countries, even though the 'children' are not real.

Where it is not possible to know who people really are there is always mischief. I have noticed how much more exaggerated and angry normally polite people become when they are sealed in their car. A supermarket trolley prang is usually, in my experience, followed by profuse apologies by all parties. A near miss in a car is usually followed by language that would make a sailor blush. I wonder if the virtual world has the same effect as the car, in that behaviour is more sordid and unrestrained precisely because identity is lost? I have the same feeling about cyber-society that I do about groups of men in hoodies: it is hard to judge the character if the face and manner are not open.

The dangers are complicated. One might well argue that the paedophiles in Wonderland are doing no harm to real children and to prosecute them is to persecute people for thought crime, surely something that would concern The Freedom Association, because, even though the fantasies are evil, they are not real. (Although, I am sceptical that any organisation can control their identity management in such a way that we can be sure the real players are over eighteen.)

There can be real victims of real crime in Second Life. Hackers have already broken into this world and have stolen vast numbers of real identities from records of credit card transactions, for use in fraud. A Pandora's box of wickedness has been emptied into the Second Life world.

There has even been a banking crisis in the Banks of Second Life. Second Life has a currency which can be converted to dollars. Apparently, the Second Life banking customers were getting the jitters about the Second Life banks' liquidity

and customers have been withdrawing their money. Stock exchanges in Second Life have been offering massive bubble-like returns: 250% per annum. Two banks recently went bust and real investors suffered real losses. There is worse: political agitation. The *Daily Mail* informed us that Peter Mandelson will be wandering around Second Life, spinning a line for Labour. Howshall we know it is he? I don't know. Perhaps someone should pretend to be him and spin a line for another party. In Cyberspace, the only certain thing is that there is never any certainty about who anybody really is; although you could add that if hackers find identities and steal real money, then the hackers are probably finding the real people to rob.

It is into this spun world of lies and cheats that Government wants to go next. Ever since the State of Missouri recruited IT staff from a 'virtual job fair' in Second Life, other public bodies around the world are neurotically worrying that if they don't join they will be left behind. I fear that it looks as if local councils will be setting up stalls in Second Life at huge expense and security risk to the ratepayer, so that you can pay your parking fines between the brothel and the casino or while chatting to a Party spin doctor. Is it far-fetched to imagine that you will do this while a police cyberspy watches your behaviour? I think it is only too likely.

However, this is just the latest wheeze. In the here and now, eGov means that thousands of people have access to details about just about all of us. It cannot be secure. It is simply impossible to keep such large system-networks secure. This is not for lack of trying. It is simply impossible to do.

Take the £33 million existing scheme called Contact Point, which will allow a modest 300,000 people to look at and change details of millions of under-18s. It is not just the social worker, teacher, policeman and probation officer who can look, but it includes the NGO extensions of modern government such as Barnardos. One of many problems is the identity of the persons using the IT.

Can Government control who looks at the personal information supplied to the Government? My experience is that out of 300,000 authorised users, the number correctly identified stabilises at about 240,000 looking at the children's details; and about 60,000 authorised "users" who, in reality, could be anyone, a temporary staff replacement, the cleaner, a replacement for a dead colleague, someone who has moved or been promoted but never given up his access or (horrors) the teenage daughter of someone working from home (mobile IT is part of eGov).

I used to find, in the private sector, that a far higher number of people were correctly identified - about 99% instead of 80% . But these were smaller databases and there was a commercial risk if the access was wrong. Moreover, this was before the days of the insidious service delivery model that takes our services and data to centralised call centres on a public sector scale.

Why does this matter? It matters because every day I deal with unauthorised people getting into systems and changing data, taking the details of children for nefarious purposes, putting mean, unfair and damaging accusations in public view or just selling lists of names and addresses to marketing companies or criminals. And because the unknown impostors are using other people's access, there is never any possiblity of catching them.

It matters because every day I deal with unauthorised people getting into systems and changing data, taking the details of children for nefarious purposes, putting mean, unfair and damaging accusations in public view or just selling lists of names and addresses to marketing companies or criminals.

There is also, far more dangerously than the merely unauthorised IT user, the army of disgruntled or angry IT administrators who statistically seem to be responsible for the worst security breaches and who have the advanced knowledge to bring the whole public service to a grinding halt. A month or two ago a man in San Francisco's town hall felt disillusioned with his job and changed all the administrator access to the IT system there, making Government grind to a halt.

The United Kingdom (UK) Government has adopted a range of strategies to control access to the eGov information. My experience is that these precautions never work. The bigger the project the more uncontrollable it becomes, the less accurate the data is and the more the individual and his identity is lost. For example, when HMRC lost all our details last year, the thorough Poynter review remarked that those involved in the loss did not always know the relevant security rules.

In my job I spend most of my time writing security rules for a public body. There are tons of rules. But nobody really knows them and I am expressly not allowed to spend time rectifying this. The reason is that the rules are written to target in order to gain targets and certifications, rather than to be useful. Security in public service is usually, as in the Her Majesty's Revenue and Customs (HMRC) case, relegated to a low priority because Government is so busy doing other things to us.

Security will always be breached. Passwords can be cracked. Data can be hacked. There is no such thing as absolute security in digital data. It cannot be carbon-dated, fingerprinted, smelt by a sniffer dog, its stratum or handwriting cannot be analysed and the brush strokes cannot be X-rayed. It is just a pattern of 0s and 1s passed about from one chip to another and across wires. It exists more in the idea than as a thing. When it is stolen or misused, this is less damaging to the individual when it is on a small scale.

Take one limited system recording the patients in a General Practitioner's (GP's) practice, or another localised system recording the prison guards in a particular place. If either system is compromised, the damage is limited to the information stored for the function served by that system. But the eGov drive for interconnected systems that do it all, is flawed and the biggest problem is going to be the fateful ID card scheme.

Richard Clayton, an industry expert, in an article in *The Economist* last February, said that personal information should be treated like plutonium pellets: "Kept in secure containers, handled as seldom as possible and escorted whenever it has to travel. Should it get out into the environment, it will be a danger for years to come. Putting it into one huge pile is really asking for trouble."

I couldn't agree more: IT is as poisonous as radioactivity.

Madeleine Westrop
westrop8@hotmail.com