INFORMATION AND SECURITY TECHNOLOGY – DEVELOPMENTS AFFECTING PERSONAL FREEDOMS

Professor John Pethica,
Chief Scientist, National Physical Laboratory (NPL)

Information and security technology is advancing rapidly, and each new development brings with it a new set of issues relating to the freedom and privacy of individuals. This in turn creates significant responsibilities for those involved in the use of personal data for security or commercial reasons. Both the public and the private sectors need to be aware of how the landscape is changing and the risks and responsibilities that arise from the access they have to large amounts of information.

The fall in cost of data storage, especially flash memory, has made it practical to keep vast banks of information which can be speedily accessed and copied. People leave an ever-growing set of digital fingerprints and an accumulating personal digital history. Phones track calls and locations to within a few metres, browsing history and timings can be monitored, and travel, health, and financial transaction information are all readily stored on databases. These can be called up almost instantaneously for analysis and correlation, all of which is very handy for advertising, efficient service delivery, or security.

The consequences of all this are far reaching. Data accumulates over time and users' history becomes more powerful and accessible. Once online, information is permanently public. Information on Facebook, for example, provides new links to a previously anonymous past. The people with privileged access to this data have a duty to act responsibly.

This all sounds a bit 'Big Brother', yet it has been accepted by many because of the conveniences that ready data access brings. We can now do our car tax online, medical databases speed up research and access to treatment, and the ability to carry out national and international trade without leaving your desk has a positive impact on the environment.

For the most part, it is where we are and who we talk to that is being monitored, not (yet) so much the content of what we say. As long as such databases provide tangible benefits which clearly outweigh the risks and disadvantages, and do not have direct, unacceptable consequences for our personal privacy, most people will tolerate them.

However, using such data for security purposes or for commercial gain raises issues which need to be addressed if organisations are to avoid further damage to public confidence in IT systems. One such problem is that of human error, and however often we hear 'this won't happen again', it will. Actions inevitably lead to errors. The laws of thermodynamics can be paraphrased as 'you can't win; and in practice you can't break even'. More prosaically, Murphy's Law states: anything that can go wrong, will go wrong.

Take car insurance data for example, as used for on-line taxing of vehicles. It is estimated that roughly one entry in every 1000 is in error. That means problems for 0.1% (some 25,000 people) not least because their cars appear uninsured when caught on an ANPR (Automatic Number Plate Recognition) camera. However, it also means the other 24.975 million are potentially satisfied customers.

. . . Both the public and the private sectors need to be aware of how the landscape is changing . . .

It is probably reasonable for an insurance company or bank to do a cost/benefit analysis, and conclude that it is cheaper to fix and compensate a few errors than to spend vast amounts trying to get a 'perfect' system. If it works for 999 out of 1000, that might be OK.

It is much less reasonable for security organisations to do so. Someone who has been wrongly detained as a terrorist due to incorrect data will rightly be much less forgiving than someone with a minor car insurance error, especially if the data cannot be readily erased. False positives and negatives can make data useless when looking for 1 in 100,000. Security is quite different from general customer convenience. We need to be very clear about the purpose of data collection *before* aggregating it and our policies need to be appropriate to how we plan to use the data.

Data used for security requirements must stand up to a certain level of scrutiny, but E-commerce and IT are too important for government data policy to be dominated by security services. It is important that policies relating to data storage are formed based on clear information about what the data will be used for and the risks associated with it.

However brilliant IT systems may be, it is impossible to eliminate human effects and errors. Wrong information might be entered. More serious, and regrettably common, is that data can be accessed or misused by insiders. *'Quis custodiet ipsos custodes?'* applies – who guards the guardians? Once leaked, all control is lost and risk of misuse aggravated. The more personal or irrevocable the data, especially DNA, the greater the potential harm that could result from error or misuse. Either we should not accumulate the data, or if there is real cost-benefit or security value (and this must be rigorously tested) then stringent regulations and segregation, and meaningfully serious penalties for abuse should be put in place.

In the USA, the National Institute of Standards and Technology (NIST), an independent and fully open state laboratory similar to NPL, draws up open security standards for government information technology. A recent example is their guidelines for electronic voting. Britain has no such system. Instead, government agencies must rely on standards produced by the intelligence services or private companies, organisations which are confidential and cannot be openly tested for weaknesses, and are therefore less trusted by IT experts. Openness is the essential basis of scientific confidence.

It is important to understand that just because data appears to be anonymous does not mean it is secure. Anonymity is becoming increasingly hard for the average person to maintain. People have various identifiers which can all be correlated, from online names, IP addresses and phone numbers, to bank accounts, medical records and DNA. Some identities, and DNA in particular, provide a unique, irrevocable means of identification, and therefore a serious single point of failure. The risks are much greater for irrevocable data, and so their use and propagation require very great care. This is a particular problem for government IT, which has recently seen the consequences of carelessness when accumulating and handling sensitive data.

Even where personal information is not available, names and other details can be deduced from metadata and structured searches. This becomes vastly more powerful if large multiple datasets can be searched and cross-correlated. Though known for some time in censuses, awareness of this issue has been raised by the Netflix/AOL case, where the companies in question released supposedly anonymised data, which researchers quickly managed to use to identify specific individuals.

. . . It is important to understand that just because data appears to be anonymous does not mean it is secure. . .

It is disingenuous to say, as do some Governments and companies, that the content of messages is not monitored, and therefore that anonymity is respected. Traffic analysis and network structure are often all that is needed to establish comprehensive surveillance information about data subjects.

These rapid developments in technology do not look set to slow down. More and more data will be recorded and will become easier to access and correlate. New services are developing all the time which throw up new privacy issues. We are not far off ubiquitous internet access, widespread location services through mobile phones and extensive data-mining – the process of extracting hidden patterns from sets of data. We can also expect machine learning in the near future, whereby computers will hone their performance as they acquire new data, and this could lead to decisions being taken without human intervention. This too raises a whole host of issues around whether a computer can, or should, do the job of a human and what the consequences could be when something goes wrong.

The technical developments, as long as they are used properly, will continue to lead to improvements in a very wide range of areas of life, from personal convenience, the efficiency of e-commerce and reduced carbon emissions, to medical research, and to understanding and tolerance of others across the world.

It is easy to get carried away by the benefits of comprehensive data collection both to security and commerce, but those using data need to remember that they are in a privileged position. It is essential to be honest and open with customers and citizens about the purposes to which data can, and also might, be put. Secrecy doesn't help. Regulation must be informed by independent, open research and testing, to give a level of confidence appropriate to the sensitivity of the data.

John Pethica *is Chief Scientist at the National Physical Laboratory, the UK's National Measurement Institute. NPL has a strong heritage in computing; it is where the groundwork for today's computer and internet world was achieved through the pioneering work of scientists such as Alan Turing and Donald Davies, and it continues to be active in areas of computing which support measurement science.*

DOES SECURITY TECHNOLOGY RESTRICT PERSONAL FREEDOM?

SECURITY TECHNOLOGIES, FREEDOM AND PRIVACY

Dr David Murakami Wood
ESRC Research Fellow,
Newcastle University

Do real 'risks' mean that safety and security must be prioritised and must freedoms be reduced in doing so? Or do the freedoms that we are supposed to be defending constitute our security and cannot therefore be infringed? These debates are as old as modern politics: Benjamin Franklin made the latter argument in the early days of the US state. However, many things have changed and in this short piece I will concentrate on the challenges for policy-makers from new security technologies and from the deterministic 'logics' that they produce: that more information is always necessary for security, and that if technological capabilities exist then they must be used.

The usefulness of information depends on the architectures used to collect, store, process and share it. In these computer databases and the connections between them reside many key political questions concerning information, age, security and liberty. Digitisation of information allows not just vast storage capacity, but also sorting. Links and patterns can be recognised in superficially disparate data through data-mining or dataveillance. This can be used to create profiles of people, places, and things, which are categorised by risk or profit. Contemporary marketing, policing, health and social welfare all increasingly depend on these 'actuarial' judgements.

Thus, when we consider the National DNA Database, for example, there are not just traditional questions of justice and liberty (legal compliance, discrimination against black men or the poor, retaining the DNA of the innocent and children etc) but also what is done with the data and why. These questions are inevitably international: we may establish security around national databases, but when government signs an agreement on data-sharing with the USA, for example, such questions become moot after our data is stored and processed in the FBI's Investigative Data Warehouse.

At the same time, the methods of data collection grow more sophisticated. The world is increasingly transparent, with the use of surveillance technologies from scanners in airports, through CCTV cameras in cities to global satellite mapping and location technologies. Access to and use of these systems is no longer the preserve of the military or the intelligence services, but they are far from equal and democratic. Whilst both risks and profits are unequally distributed, some are more likely to be subjected to surveillance, and some to use it.

Dataveillance and surveillance processes are increasingly automated and algorithmic. Not only are links, profiles and categories often automatically detected and generated in databases, but simulation, anticipation and, the dream is, pre-emption, are possible. Biometric surveillance systems, like facial recognition, iris scanning and gait recognition as well as more esoteric areas like olfactory detection, are progressing rapidly. Facial recognition is being introduced in eight major UK airports this year; however it is less effective in open spaces... for now.

There are two more key developments. The first we already know: connection. The Internet is simply the biggest and most accessible of the many networks linking computers (and databases) together. It panics governments that are used to well defined national borders, and this has led to technologically and socially naïve attempts to 'control' it through regulation. But the Internet is already generating new trans-border knowledge communities; government has to learn to live with and use it.

The other issue is one of

. . . The usefulness of information depends on the architectures used to collect, store, process and share it. . .

scale. It is not simply that computers and sensors are both ever smaller and more powerful, but that potentially they can be distributed and embedded into everything from walls to living beings, or become part of mobile systems, connected by wireless. Ubiquitous computing means ubiquitous surveillance, because to function, the 'Internet of things' needs to locate, identify and address every element. How this new technological infrastructure is built, for what purpose, by whom and who can connect to which parts for what reason, matters. Again, it is not a question of restricting development, but it is easy to see how ubiquitous computing infrastructures could be both empowering, democratising and enriching but also a perfect tool for totalitarian rule, and any number of possibilities in between.

SO WHAT ARE THE CHALLENGES?

Difficult regulatory questions emerge simply from size. The smallest available sensors are the 'smart dust' 'motes' manufactured by Dust Networks of California, and these 4mm^2 platforms will seem large within a few years as micro- and nanotechnology progress. Such tiny sensor platforms and their larger mobile cousins (Unmanned Aerial Vehicles or UAVs) are also being programmed to imitate natural biological systems like swarms or flocks, which will operate independently rather than by traditional human remote-control. How do we regulate things which relate to security or privacy, that you cannot see or perhaps even detect, and which can be scattered and collected casually, and could have a virtually independent existence?

It is clear then that policy is lagging some way behind technological development. As current technological limits and problems cannot be a substitute for adequate foresight and regulation, we need to 'get ahead of the game.' We need not (and cannot) anticipate every technology, but we must establish systems and criteria by which we can judge proposed technological changes quickly, within and beyond government. Tools like Privacy Impact Assessment (PIA) are essential, but government also needs to regulate for human rights, like privacy, to be built-in to the architectures of systems. It should start with its own: as the Joseph Rowntree Reform Trust revealed, more than 25% of government databases (proposed and actual) contravene data protection and/or human rights law. Government can also help by facilitating recognised standards internationally: from the base architectures through languages, protocols, and to the specifics of media, identification systems and so on.

Current laws are also inadequate. Britain's regulations are better than the EU's on data protection, but they are still based on a rather 1980s conception of computing and the information society. Freedom of Information is likewise premised on paper files (on which much information remains, but will be less and less so). We need to bring these and other concepts together in a comprehensive new Information Act setting the ground rules for the information relationships between citizens, state and private sector. This needs to be premised on the citizen's ownership of data. The state must accept that data is not just information *about us*, that it can demand and use as it likes, as it increasingly determines our life chances: and it *is us*. At the same time, the state and private sector themselves need to be more transparent. Corporate confidentiality is not equivalent to personal privacy and should not be allowed to excuse secrecy. But privacy too is changing and has to change further. It is not dead – although anonymity might be – but privacy in a society where information flow is taken for granted cannot be the same as it was.

> . . . the Internet is already generating new trans-border knowledge communities; government has to learn to live with and use it. . .

Above all, we must refute 'security technology logic.' CCTV in Britain is a case in point. CCTV expanded both in location and use in the 1990s, becoming rapidly 'normalised', largely without public debate or parliamentary scrutiny. The 9/11 and 7/7 attacks merely intensified this; despite the fact that when we watched CCTV images of the attacks and the attackers, we were witnessing the failure of CCTV as the prophylactic we had been promised. For the Government and developers, CCTV is now essential 'infrastructure', written in to crime reduction strategies and contingency planning. Public objections now prompt a defensive reaction: armouring cameras and portraying 'interest' in CCTV as inherently suspicious. What is it that is being secured? Increasingly it seems that it is not just the state, but the security architecture itself! This is not conspiracy; it is simply the result of unchallenged security technology development logic. We need instead to consider how government can facilitate both the other positive logics of technologies (for example, the possibilities of freedom, empowerment, and expanded sensoria offered by the 'Internet of things') and the positive social effects of technologies, whilst accepting and enhancing the ability of people to change, adapt *and even refuse* new technologies.

Select Bibliography

Electronic Frontier Foundation (2009) *Report on the Investigative Data Warehouse*. EFF.

Foundation for Information Policy Research (2009) *Database State*. Joseph Rowntree Reform Trust.

House of Lords Constitution Committee (2009) *Surveillance: Citizens and the State*. UK Parliament.

SWAMI (2006) *Safeguards in a World of Ambient Intelligence,* EU Information Society program.

Surveillance Studies Network (2006) *A Report on the Surveillance Society*. Information Commissioner's Office.

DURING DISCUSSION THE FOLLOWING POINTS WERE RAISED:

Any Member of Parliament will tell you instantly that their constitutents do not want any security cameras applied to them, but to every other constituent! The growth in scale of mobility and the freedom to travel results in a desire for more information about the activities of the much larger, but much less well known, groups of people that we now interact with. The legal situation concerning photography in the street is not well understood. With regard to Government databases how can individuals find out what information is already on the database about themselves? Much of the technology and information used is obtained from third parties. In the case of the G20 demonstration in the City, office workers were requested to dress down so as to become indistinguishable from protesters and therefore able to go about their work undisturbed. Could this lead to subsequent misidentification of City employees as protesters by association? What protection, if any, do we have from misuse or misinterpretation of such data by potential employers or others? The order of magnitude of surveillance and analytical ability to interpret data have both increased, resulting in greater awareness and concern. The upcoming Olympic Games in London will pose a wide range of security issues, yet the public will expect this to be conducted in a non-intrusive manner. This increases personal freedom to move around, knowing that surveillance is providing protection but at the cost of privacy.

How do the police know about us? They don't, suspicion is categorical, if you are in a certain place at a certain time alongside people who are suspects, you are also a suspect. You are on a categorical database. This may affect you later in your life. There will be increasing concern in future at the growth and use of databases. You cannot be sure you are not on a database. Their power is greatly extended as the number and variety of databases increases. There are already a very large number of databases in existence providing information about individuals that cannot be deleted by those affected. There is already a hierarchy of quality of information so who do you trust? The chances of controlling personal data in the public domain are essentially zero. The National Institute of Standards and Technology (NIST) in the US have concluded that regulation is a waste of time as it is impossible to keep up with the growth in technology. It is better to establish benchmarks and legal expectations and obligations on those who hold the data, as there is no technical fix available. "City air makes you free" due to the anonymity which exists in cities which we are now losing. We never fully adjusted to the new freedoms and we have not adjusted yet to the new restrictions. These are big issues.

TAKING SCIENCE TO THE STREET

Meeting of the Parliamentary and Scientific Committee on Tuesday 19th May 2009

TAKING SCIENCE TO THE STREET

Professor Anthony J Ryan OBE
Pro Vice Chancellor,
Faculty of Science,
The University of Sheffield

In December 2008 BBC Radio 4 ran a week of programmes called 'Street Science'. The basic premise was that most scientists are passionate about what they do and believe that it's in a good cause. But the programmes asked the question "What happens when scientists are taken out of their comfort zone, to church or to the school gates, to try to explain what they do and why, to members of the public?"

I was one of those scientists and spent a couple of afternoons in Sheffield's Winter Gardens talking to the public, quite literally accosting people as they walked down the street, asking them their hopes and fears about nanotechnology. The technical level of the debate was somewhat variable but discussing the applications of carbon nanotubes with retired miners and giant magneto resistance with school kids obsessed with their iPods was, I hope, as entertaining for them as it was for me.

The potential dangers of nanotechnology have been in the media and fear of the world being overrun with "grey goo" was even highlighted by HRH Prince Charles. This fear comes from an unfortunate extrapolation of a reasonable argument. The idea that atom-by-atom construction could build fantastic devices that could reproduce themselves and take over the world has its proper place in the world of fiction, as exemplified by Michael Crichton's book '*Prey*'. But all the potential problems of nanotechnology, both real and imagined, have to be balanced against all the potential benefits it could bring to medicine and the environment, with nanomachines saving lives and cleaning up pollution. If one asks the question "What will a nanobot look like?" the answer won't be the shrunken submarine envisaged by Hollywood. Physics at the nanoscale mean that shrunken submarines won't work and nanobots will actually look more like bacteria or sperm and that soft nanotechnology, based on self-assembly and Brownian motion, is the way to go.

. . . What happens when scientists are taken out of their comfort zone. . .

The substance of my 'Street Science' programme surrounded the economic and ethical