

Information Governance – Just Say No!

Eur Ing Andrew Hardie

BSc, C.Eng, CITP, FBCS, FIMIS
<http://www.ashardie.com>

V1.2, 2008-10-01

Abstract

The spate of recent and ongoing high-profile public sector data losses and leakages have elevated the question of Information Management, in its widest sense, to high visibility and high priority. With public sector databases proliferating and data sharing and matching increasing exponentially, all in the name of efficiency and security, the risks also proliferate. With the prospect of the National Identity Register the risk of fundamental identity compromise as a result of information leakage or theft cannot and must not be ignored. The new field of ‘Information Governance’, encompassing identity management, information sharing, privacy and data retention, has become a hot topic.

Following the high-profile incidents, numerous reports have been published and many recommendations made. However, the changes recommended, as with all changes, bring new risks including the risk of introducing more complexity into situations and structures already criticised for being too complex.

Proposed solutions based on greater system integration and complexity ignore research indicating that the results can also be the opposite of that intended because of the increasing incidence and impact of unexpected and uncontrollable side effects.

The political-level alarm brings the risk of hasty legislation and more bureaucracy. Management fears bring the risk of unworkable procedures and ill-judged technology-based solutions, all in the name of satisfying compliance, but ignoring the significant human dimension of the problems.

Complexity and people are the main causes of the problems and seeking to manage information securely by creating a climate of personal liability and punishment without clear and simple solutions is unlikely to succeed. Recruitment advertisements for ‘Information Governance Officers’ have already started appearing. Right now, that job feels like ‘Chief Blame Officer’. Would you want the job? Just say no!

New name, old problem

“Information governance” is a new term, apparently UK-only (there is no Wikipedia entry for it), which seems to have originated in the NHS Connecting for Health project, used to describe the requirements, standards and best practice that apply to the handling of information. This sounds a lot like newly fashionable Corporate Governance meets old-fashioned Information Management. But, whatever you call it and however new the name, large-scale aggregated personal information handling is not a new concern. Consider this quote from 1992:

“Every time you make a telephone call, purchase goods using a credit card, subscribe to a magazine or pay your taxes, that information goes into a data base somewhere. Furthermore, all these records can be linked so that they constitute in effect a single dossier on your life not only your medical and financial history but also what you buy, where you travel and whom you communicate with. It is almost impossible to learn the full extent of the files that various organizations keep on you, much less to assure their accuracy or to control who may gain access to them.” (David Chaum, Scientific American, 1992)

That quote (in fact from an article promoting a privacy-enhancing anonymous digital cash idea) is from an era when few people used the Internet and the Web was only a few months old (the first site at CERN went live in August 1991). The situation now is far worse. Data sharing, matching and resale in the commercial world are routine and now Governments are doing or want to do the same both for financial reasons (“efficiency”) and, increasingly, for national security. Communication and commerce may have been made easier than ever by email and the Web but so has mass surveillance by governments – and mass data harvesting by criminals.

Not only will government have all the identification, registration and transaction-based information we will want or will have to supply, there is the prospect of recording all email, Internet telephony and Web browsing history. With that, and pervasive public CCTV recording, Big Brother in the form of the ‘Surveillance Society’ has unquestionably arrived. Apart from the social questions of whether this is desirable or acceptable, there are also the policy questions of how well it will be used, managed and guarded. The recent information leaks have brought this question into very sharp focus.

The warnings

Concerns over government information management have been growing in recent years. Amongst those concerns, this one stands out:

“Like all technologies, those used to collect, process or protect personal data are at risk of failure. Because many of these technologies are new or have only recently been deployed on a large scale, the potential for failure is high.”
(RAE Report: “Dilemmas of Privacy and Surveillance”, March 2007)

And then, a few months later, the failure happened – the Information Privacy “Event Horizon”:

HMRC, 18 October 2007.

Two CDs, containing the records of around 25 million people from the Child Benefit Office, were lost and have never been found. It was a defining moment, the Government & ICT equivalent of the ‘sub-prime’ mortgage crisis in the financial world.

Like that crisis, it will have knock-on effects much wider than initially apparent – we have not seen the end of it yet! Also, like the sub-prime fiasco, complexity was a crucial factor.

The Fallout

Pre-HMRC:

“The government does not agree with the implication that the public has lost confidence in using the internet.”

(Govt response in October 2007 to House of Lords Science & Technology committee report on Personal Internet Security, August 2007)

Post-HMRC:

“Public confidence is evaporating” (Data Sharing Review, Thomas/Walport, July 2008)

There is strong evidence that the current downturn in online transaction activity is not only due to the recession but also to that loss of confidence in the online world. The proposed Internet Crime Reduction Partnership is a welcome development but one which will be judged not by its membership or its words but by its actions.

Action this day?

“We acknowledge that, following the Government’s disappointing response to our Report, they have reflected further and, with regard to some of the issues we raised, there has been some progress towards meeting our concerns. What progress there is, however, appears to be slow.”

(House of Lords Science & Technology Committee – Personal Internet Security Follow-up report, July 2008)

Slow progress is hardly surprising since, post-HMRC, not only does nobody in government want to own this problem, nobody wants to own the policy or even the solutions in case they are wrong, wrongly-implemented or just ignored. Identity Management, Privacy, etc – everything that might fall under the new heading of ‘Information Governance’ – are now seen as the new ‘must avoid’ career-limiting post, carrying all of the blame and none of the reward.

The Blizzard of Reports

Also, post-HMRC, we have had reports, lots of reports – mostly predictable, but with some more interesting points.

HMRC – The Poynter Review (June 2008)

- No senior Civil Servant was to blame (or, even, involved, it seems...)
- Loss was “entirely avoidable”...
- Result of: serious institutional deficiencies, information security not being a core objective, misunderstandings between departments, lack of information governance, lack of awareness, lack of training, etc...
- HMRC should: Enhance... Strengthen... Engage... Take this great opportunity to... etc.

Most competent consultants could have drafted the outline, conclusions and recommendations for that going home on the train. And, depressingly, like the numerous reports in the past few years

about why large government ICT-based projects fail, it could have been written at almost any time about almost any department with just the names, dates and numbers changed.

It was an accident waiting to happen, made more likely by the complexity of the organizational design and policies of HMRC – both strongly criticised in the Poynter review which went on to point out that much of that complexity was the direct result of business change within HMRC and noted the low morale of staff “weary of change”.

ICT-enabled business change (all too often, in fact, ICT being used as a tool to force business change) has become a ‘holy grail’, to be followed in spite of failures and warnings, as the only possible way to achieve goals. Similarly, the notion of ‘ICT infrastructure and business strategy alignment’ has been elevated to near mythical status, with ever more complex and highly integrated systems being developed.

However, complexity and change are not only both risky individually but are also interdependent – “reflexive” to use the term Giddens applied to modernization.

HMRC – The IPCC report (June 2008)

The Police Complaints Commission report was primarily to determine if any criminal or disciplinary offences had been committed but also examined questions of policy and practice. On these topics, their report was as scathing as the Poynter Review:

- “[...] *the failings identified by our investigation are significant.*”
- “*Our investigation found no visible management of data security at any level.*”
- “*Our investigation revealed the absence of a coherent strategy for mass data handling and, generally speaking, practices and procedures were less than effective: there was a complete lack of any meaningful system; a lack of understanding of the importance of data handling; a ‘muddle through’ ethos.*”

Both reports put the root causes of the HMRC incident down to people problems, not technology. There is also the nagging suspicion that the reports did not reach the real truth – human behaviour cannot be extracted and analyzed as easily as a computer log file.

MOD – The Burton Review (April 2008)

On 9 Jan 2008, an MOD laptop computer containing the unencrypted personal records of 600,000 people was stolen from a parked car. In the post-HMRC climate, a big fuss ensued, with disciplinary proceedings and the Burton review but, pre-HMRC, three other similar laptops had been stolen under almost identical circumstances with no big fuss, no disciplinary action and no change in security procedures or better enforcement of the ones that existed.

The headline findings of the report are very similar to those of the HMRC incident:

- MOD not treating information as key asset...
- Lack of training...
- Failure of supervision...
- A major security incident had been "inevitable"...

Like the HMRC reviews, the Burton review also criticized the “little awareness” of the importance of data security but this is a far more surprising revelation in the defence

environment. Whatever happened to the famous military and intelligence community principle of ‘need to know’? To quote from the preface to the review, *“During the Cold War, awareness of real security was ingrained in individuals and organizations. Audit, inspection, and compliance regimes were rigorously underpinned by codes of discipline. These well developed processes and procedures have not been translated, effectively, into the information age.”*

Then comes the first interesting observation: the “Facebook generation” casual handling of information, as on the Facebook social networking site where the widespread, one might almost say promiscuous, sharing of personal information and activities is the norm – the “need to share” instead of the “need to know”.

The new generation of MOD staff, with no memory of the cold war era, bring completely different cultural and social values to their work. *“The Department recruits from, and exists within, a culture where the rapid and often uninhibited exchange of information is the norm. At work, this behaviour must be tempered by common sense and sound judgement [...]”*. Ironic, then, that MI6 is now seeking to recruit new staff via Facebook.

The Legislative and Parliamentary View

Post-HMRC, various expert bodies have expressed grave reservations about the whole way in which the UK Government is going about public information gathering and management and warned of the consequences of failures in safeguarding that information.

“The Committee fundamentally disagrees with the Government’s approach of including very broad enabling provisions in primary legislation and leaving data protection safeguards to secondary legislation. Mere compliance with the HRA and DPA is not enough.”

“...recent lapses in data protection are not unfortunate “one-off” events but are symptomatic of the Government’s failure to take safeguards sufficiently seriously”
(Data Protection and Human Rights, Joint Committee on Human Rights, March 2008)

“The Data Protection Act 1998 was written in an age of ‘data silos’. While it covers several of these points [...], it does not cover all aspects of data guardianship in the ‘data sharing’ age adequately, nor does it cover information governance.”
(BCS Position Statement on Data Guardianship, Jan 2008)

It is worth remarking at this point that the solution to the numerous ‘data silos’ problem is not one big data silo. That just multiplies the risks of system failure (both in development and in operation) and the scale and consequences of any information leakage.

The term ‘silo’ is usually used to mean a separate system that cannot communicate readily with other systems, presenting this as the justification for increased integration. However, there is a demonstrably proven third way – separate systems that can communicate with other compatible systems, as wonderfully demonstrated by the Internet and the Web. Commonality is not necessary (or possible), loose coupling and compatibility are enough. Gateways turn out to be far more flexible, efficient and controllable than tightly integrated systems.

“Mistakes in or misuse of databases can cause substantial practical harm to individuals—particularly those who have little awareness of or control over how their information is used.”
(“A Surveillance Society?” Home Affairs Select Committee Report, May 2008)

With the widespread use and sharing of personal data, how is it feasible for users to track and correct information on them?

Intentional data sharing

The recent high-profile incidents were about unintentional loss or leakage of information not intended to be shared. But, what about the intentional data sharing government wants to do in the name of improved efficiency and security?

Data Sharing Review (Thomas – Walport)

This report was commissioned by the Prime Minister to review the operation of the Data Protection Act and the Information Commissioner’s Office and “*to provide recommendations on how data-sharing policy should be developed to ensure proper transparency, scrutiny and accountability.*”

Much of the report and its conclusions concentrate on the legal and regulatory environment, recommending that the ICO needs more powers and resources but what bureaucracy does not plead for more money and bureaucrats? However, the question of culture is also addressed, concluding that change is necessary “*to transform the culture that influences how personal information is viewed and handled*”. The report goes on to state:

- “*It is clear to us that data sharing is shrouded in confusion.*”
- “*[...] the culture of indecision that surrounds data sharing is problematic and needs to change, particularly in the public sector.*”
- “*Our most important recommendation calls for a significant improvement in the personal and organizational culture of those who collect, manage and share personal data.*”
- “*We recommend that rigorous training of those responsible and accountable for the handling of personal information, backed-up by enhanced professional development, accountability, reporting and audit, will effect a major improvement in the handling and sharing of data.*”

And, echoing the Burton review of the MOD laptop incident:

- “*None of this is a substitute for good judgement and common sense, which are key to making wise decisions about whether or not to share personal data.*”

The extra-procedural problem

However, just training the staff is not sufficient. The HMRC event and several of the other recent events have involved “extra-procedural” activities, i.e. not only the staff routinely involved in handling the data, but outsiders, such as auditors or consultants. To make matters worse, these outsiders had access to entire data sets, not the just individual records the staff normally see and handle. The checks and balances on their information access and activities should have been greater, not less.

The IPCC report describes the NAO request for the data that was lost from HMRC as “*a key departure from protocol*”, adding that “*It is not clear what, if any, authority was given for the two CDs to be given to the NAO.*”

It's the people, stupid!

As usual in security, it mostly comes down to the people. The whole issue of information management and security is beset with people problems at all levels:

- Management don't want the problem – seen as an albatross round their neck
- Staff don't want the solutions (complex procedures, rules, technology)
- Suppliers don't understand the people problems or don't care – technology push alone will not solve this!

People are not predictable – they are lazy, they lie, their work is affected by mood and situation. Change and new technology are both threatening and staff seldom react to them as management might hope. Staff, under pressure from management to improve performance, just want to Get The Job Done and right now – not so much “The power of now”, as a recent mobile phone network advert said, but “The weakness of now” – people won't wait for anything. We have turned into the instant satisfaction society, the “download generation”, where a result in 10 seconds = happy, no result in 20 seconds = bored and no result by 30 seconds = lost interest / angry / gone elsewhere.

For security or privacy to become effective, it must become invisible, i.e. part of the infrastructure. But, as infrastructure, the more widespread it becomes, the more it will be used by junior staff less interested in policy and more interested in getting their work done quickly and easily. The more it comes into conflict with getting the job done, the more ways will be found to get round it. If you give people conflicting goals, don't be surprised if they chose the one that benefits them. It will be every bit as vulnerable to the "OFI" principle as paper-based security but with potentially far more damaging consequences.

The more identity is demanded, used and shared, the greater the risks to privacy and the greater the consequences of any identity compromise. The attitude must NOT be: “it's not likely to happen”. The attitude must be: “when it happens, how do we fix it”.

It's a re-run of the business continuity issue – it takes a big incident before people sit up, take notice & do something about it. “*It should not take a train crash [...] but we have had a train crash*” (Richard Thomas, in evidence to JHCR). Well, we've had several and there seems to be no sign of them stopping.

Here's the rub – well, three, in fact:

- The more you rely on technology, the more you abolish human suspicion and common sense – turning people into robots.
- The more you seek to blame and punish, the more people will suspend their judgement, become robots and just hide behind the rules, if they can understand them!
- Seeking to make people responsible cannot alone solve the problem, *especially until the problem is perceived as being solvable*. Otherwise, nobody will volunteer and those ‘appointed’ will just look for transfer or early retirement. We've seen it before – whatever happened to ‘Information Age Champions’?

It's a people problem, so you must start with the people. Security must include ethnographic and social factors, not just rules, procedures and technology. Solutions must take into account human weaknesses. The attackers already understand this – remember the 'I love you' virus?

The best way to get users to do the right thing is to make it the easiest thing – any other way is doomed to failure or evasion. Security has to be as near invisible as possible. System designers, suppliers and management have to get their heads around this, and *fast*...

But, staff also have to be more responsible –

- Not bringing the “Facebook generation” attitude into the workplace
- Not abandoning their judgement and common sense
- Not being afraid to question policies and procedures they don't understand
- Not selling equipment containing confidential information on e-Bay!

Management must implement *simple, practical* procedures – complexity is the enemy of both compliance and reliability. The same is true of the systems themselves. Everything keeps coming back to those same two key factors: **people and complexity**. In fact, this is true throughout information systems development, deployment and operation but is all-too-often forgotten.

Flexibility vs Security

The flexibility of today's systems is both their strength and their weakness – the systems become infrastructure. Dumb terminals were inherently secure and proprietary closed systems were inherently restrictive. Now, it's USB, VOIP, Ajax, Java, Bluetooth, WiFi, WiMax, laptops, memory sticks, email, IM, browsing, forums, etc. Blogs & Wikis bring the new Web 2.0 world inside the enterprise. With companies, politicians and public sector bodies deliberately establishing presences on Social Networking sites like Facebook, MySpace and Second Life to appeal to the 'Facebook generation', where does the work and play divide lie and how can it be enforced?

Monitoring and auditing all this is now a lot harder than just recording all email and browsing history. There is the problem of the shift to visuals – Flickr, YouTube and the OCR-resistant images of the 'pump and dump' email scammers – it's a lot harder to search visual content. Then, there are the problems of those deliberately intent on trying to bypass the controls and audit, using techniques such as Steganography (the hiding of one type of content in another) both in images and now in VOIP traffic, DNS piggy-backing, encrypted proxy tunnels, etc.

What software vendors might call 'productivity enhancing', security professionals would probably call 'insecure'. There are now simply too many ways of doing the wrong thing. With most users now having faster and better computing facilities at home than in the office, upward pressure on management and restrictive procedures is inevitable. “Why can't I do...? It's much faster and really, really easy...”

Organizations under threat

Privacy issues are a time-bomb under information-based organizations, lurking to destroy their reputation and assets. They are:

- More damaging than system errors & failures – people have become used to ‘computer errors’ or ‘the system’s down’...
- Much harder to recover from – you can’t restore customer trust from a backup tape
- Impossible to ‘news manage’ – there is no way to put a positive spin on privacy breaches
- No longer a back-office technical problem - it's a top-level, high-profile issue, threatening your brand

Furthermore, the problem is getting more difficult, as noted in the O’Donnell report:

“Managing information risk in the public sector is likely to become harder in the future rather than easier. Technology and external threats both continue to change quickly...”

(Data Handling Procedures in Government: Final Report – Gus O’Donnell, June 2008)

Users under attack

Privacy is also a new battlefield being conducted inside every user’s PC. The threat has shifted from intrusion and disruption to organized crime identity theft and fraud – it’s much easier to target users than organisations with good security systems. This mirrors what has happened with car theft – with car security systems now so good, the car-jackers simply target the owners to get the keys. Botnets (collections of compromised ‘Zombie’ computers that can be remotely programmed to run malicious code or send spam) are so widespread that the rental price is now about 50c per PC. Phishing attacks are at epidemic proportions.

These and other threats are becoming ever more sophisticated. The latest is so-called ‘click-jacking’ where an invisible submit button, tracking and hovering under the mouse pointer, is activated when the user clicks on anything else. Users are under siege from more than a million existing malware code threats, growing by around a thousand every day...

“Something must be done!”

“Public confidence is evaporating” (Thomas/Walport), just when Government wants us to do everything online to save money, improve security, etc, etc. It’s not just trust in Government and corporate brands that is under threat – online transactions of all kinds are under threat. So is the Internet itself

Child porn, chat-rooms, paedophiles, etc are all legitimate, but often over-used, concerns that have to be set against the great benefits of the Internet, including for children – read the Byron report: *“For [children], new technologies are a seamless part of the world into which they were born. The challenge of empowering children to stay safe in this digital world is significant, but I firmly believe that it is achievable.”*

This, the recent data losses and the fear of e-Crime, which is now a political-level issue, bring the risk of a classic ‘legislate in haste, regret at leisure’ outcome here at home, in the EU and at the IGF (Internet Governance Forum). Add in the pressure from the copyright protection lobby and there is the real danger of a ‘slippery slope’ down into routine Internet censorship, monitoring and control. It is hard for one country to defend censoring the Internet against one perceived social evil and argue against other countries censoring the Internet for political reasons.

The great good that the Internet has brought over the years is being obscured and forgotten. In the public mind, the ‘evils of the computer age’ converge on ‘The Internet’ and it is being blamed for information incidents that were nothing to do with it. Not only was the HMRC incident nothing to do with the Internet but the data would have been far safer if it had been sent over the Internet! Laptops left in cars or mislaid memory sticks are also nothing to do with the Internet and the data would not have been lost if it had been accessed via a secure remote connection instead of being copied onto the laptop or memory stick.

For those of us whose careers developed as the Internet grew and who benefitted enormously from the freedom (in many senses) that the Internet brought, this is a very sad state of affairs. For the new generation who have grown up taking the Internet for granted, ‘freedom’ means sharing music without paying for it; to that older generation of Internet pioneers and users, it meant something very different. The Internet dream is fading. If you think this is wrong, please consider supporting the If4g initiative: *Internet: Force for Good* (www.if4g.org)

The System View

Systems are being developed and commissioned with no clear ideas about how privacy is to be implemented, monitored or controlled. As with security, it is very difficult to add-in privacy late on in a project. (How often has this happened before in the industry, e.g. ISO 7-layer model?) Information is ‘atomic’ – you have to think like you are building a nuclear power station:

- Fail-safe design
- Commissioning costs
- Running, guarding and monitoring costs
- Training costs
- Update costs
- Information disposal costs
- System decommissioning costs (equipment disposal, etc)
- Minimize ‘Critical Mass’ risks – don’t give people access to entire data sets!

What about government systems?

The Cabinet Office ‘Coleman Report’ on protecting government information (Cabinet Office, June 2008) paints a worrying picture. The language may be diplomatic, but the meaning is clear:

“Government going forward needs to be able to demonstrate a comprehensive understanding of the risks it is facing.” [Translation: it hasn’t]

“Government must do more to deliver confidence in its information infrastructure” [Translation: it hasn’t]

The British Computer Society put it rather more bluntly:

“I think the Government is being really blinkered in what it's doing. They don't understand the technology and how difficult it is to do the things they are saying.” [No translation required!] (Louise Bennett, BCS Security Forum, SC Magazine Interview, June 2008)

The Technology

Maybe the technology can save us after all, or so the suppliers keep trying to persuade us, but what are the expert views on this?

"A good solution to a cybersecurity problem is one that is effective, resilient against a variety of attacks, inexpensive, cost effective and easy to deploy, is easy to use, and does not significantly interfere with the function of the system of which it interacts."

(ESRC - The Economics of Information Security Seminar, April 2008)

"Engineering ingenuity should be exploited to explore new ways of protecting privacy."

(RAE report "Dilemmas of Privacy & Surveillance", March 2007)

It's hard not to interpret both of those as saying that we don't have any good solutions yet...

The hidden risks of complexity and people

The similarity, suggested above, between the US 'sub-prime' mortgage crisis and the HMRC event was more than a passing observation. There are significant similarities and the common factors are complexity and people. However, an appreciation of this requires a brief departure from technology into the worlds of ethnography and philosophy.

A key factor in the 'sub-prime' financial crisis was the mis-pricing, i.e. mis-appreciation, of the unsuspected – or hidden – risks involved. Risk that was presented as securitized and diversified turned out to be far less diversified and far more risky than it appeared. Off-balance sheet activities, conduits and other increasingly creative financial instruments increased the complexity, further reducing the ability for objective assessment whether tacitly or intentionally. Accordingly, unexpected events can hardly have been surprising. Even without the help of human greed or deceit, the complexity and inter-dependence ('integration' in system terms) alone meant high-impact or catastrophic events were almost inevitable.

Management responses to what are seen as man-made problems are typically to seek increased control, either on the basis of the management maxim of "you cannot control what you cannot measure" or by formulating more strategies or by increasingly futile attempts to enforce conformance with existing strategies or project plans. These views are based on a theory that turns out to be a practical house of cards – the myth of increased control minimising risks, especially when attempting to achieve 'alignment' between business re-engineering and the ICT that supports it. An increasing body of evidence points to the opposite conclusion: that increased control actually magnifies the risks.

The late Professor Claudio Ciborra wrote (e.g. in his books "The Labyrinths of Information" and "From Control to Drift") about how staff can interact unpredictably with systems and the way in which increased system complexity and integration increase the risk of and the damage caused by unexpected side effects. He was writing on the specific topic of highly-integrated ICT systems, such as Enterprise Resource Planning (ERP) systems, widely used in the commercial and financial world, but he was influenced in his thinking by the work of other thinkers concerned with more general risks, such as Ulrich Beck, with his concept of the "Risk Society" (a society organised as a result of risks) and Anthony Giddens and his concept of "Reflexive Modernity" (where modernisation is constantly affected by more information appearing about the modernisation process itself). Ciborra therefore concluded that not only was 'drift' an inevitable

part of the ICT systems development process but also that an unavoidable effect of globalisation (i.e. integration on the grandest scale) was the globalisation of side effects, i.e. higher risks and higher-impact consequences, as well demonstrated by the ‘sub-prime’ mortgage affair.

Furthermore, all too often, even when system failures are analysed, only single-loop learning is applied – ‘the plan was right, but we didn’t enforce it rigorously enough’ – and the need for double-loop learning, questioning the plan or the project itself, is ignored. Those seeking to solve the current ‘crisis’ by legislation or more bureaucracy should consider this and the consequences of recent financial and intellectual property legislation – more unintended side-effects.

There is a saying in politics, “*Laws seldom prevent what they forbid*” – perhaps we should add “*...but they can prevent what they did not intend to forbid*” or “*... but they can inhibit those they were not intended to deter*”.

Conclusions

The public and, by extension, their political representatives are right to be worried by the recent government information leakages. But, it is important not to over-react, legislate in haste or introduce more bureaucracy and complexity into an area that needs clear and simple solutions.

The weakest link is, and will always be, the people not only because they are often unpredictable, careless and irrational, reacting in unexpected ways to management control and new technology, but also because they are victims themselves. Solving the unintentional leakages does not solve the problem of criminal activity. The better the security technology, the more those intent on wrong-doing will target the people directly to get what they want.

The numerous reports on the recent events tell us that:

- The legal environment is not right
- The policy environment is not right or not properly applied
- The organizational environment is not right
- The technology is not right or not properly used
- The staff mental attitude is not right

In addition, the media and public pressure on legislators is not creating the political environment in which to formulate good decisions on possible legislation. Data sharing can have beneficial uses but the public perception now is of the all-pervasive surveillance society, permeated with incompetence and criminals, threatening our financial and personal security.

In this confused and increasingly risky environment, someone in every organization is expected to step in and sort it all out. Recruitment advertisements for ‘Information Governance Officers’ have already started appearing. One, for a local authority says “*you will ensure the Council discharges its legal responsibilities regarding Freedom of Information, Data Protection and the Environmental Information Regulations*”. Right now, that feels like ‘Chief Blame Officer’. Would you want the job? Just say no!