

Sharing is dead! Long live sharing!

What can we learn from the post-9/11 US Intelligence Community experience?

Eur Ing Andrew Hardie

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

V1.0, 2008-10-30

Introduction

Sometimes, when contemplating a problem, it can be helpful to turn it around and look at it from the opposite direction. In the UK and Europe, the focus of information governance is on the guarding and protection of data (“stewardship”, as the BCS calls it) so as to limit the sharing of that data. In the US following the events of 9/11, which was widely perceived as a major US intelligence and information sharing failure because of the “need to know” mindset, the entire intelligence community was re-organized and the whole way in which information is to be managed and shared has been revolutionized, with the emphasis on the “responsibility to provide”. Even though the thrust of these actions is within the US Intelligence Community, their work would clearly have relevance to wider considerations of government information sharing.

Far from creating a “Wild West” environment of careless information sharing, the strategy is heavily focussed on security – albeit as much from the perspective of protecting the information gathering techniques (“sources and methods”) as the information itself, but the approach could also be valuable in the European context where the same security principles and provisions can safeguard the information to meet data protection concerns as well as ensuring the integrity of the systems used to collect and process that information. Tightly controlled sharing can be seen as the counterpart to tightly controlled access. This summary of recent reports has been prepared to help illuminate and inform the discussions on information sharing currently taking place in the UK

DNI – The New Strategy

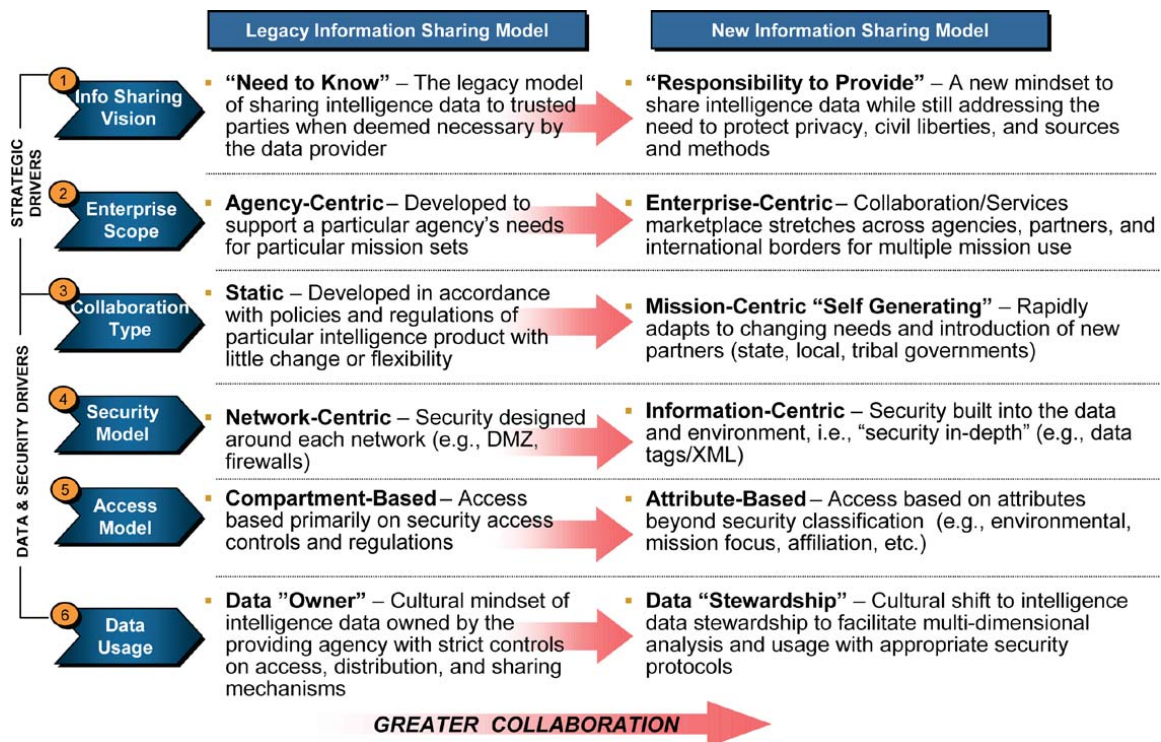
In February 2008, the Office of the Director of National Intelligence (ODNI, created in 2005) published their new Information Sharing Strategy for the US Intelligence Community. The introduction, by John McConnell, the Director of National Intelligence, sets the scene: *“Together, we must challenge the status quo of a “need-to-know” culture and move to one of a “responsibility to provide” mindset.”*

The secondary introduction, by Dale Mayerrose, the Associate Director and CIO, goes on to say that *“...we should reiterate our commitment to develop a risk management approach where we carefully contemplate anticipated benefits and potential costs, ensuring mission success and protection of privacy, civil liberties, and sources and methods.”*

A new, risk-based management – within the context of collaboration – has been developed and the need for a uniform model of trust across the intelligence community has been identified,

whilst acknowledging the “dynamic tension” between the benefits of making information available and the risks of unauthorized information disclosure. *“In today’s environment, the risks associated with not sharing can lead to missing clues of an attack, cost lives, and endanger our Nation’s security. This new environment requires the Intelligence Community to move to a “responsibility to provide” culture to ensure all members of the Community can retrieve the information they need and effectively support intelligence customers. The “responsibility to provide” culture is predicated on managing risks associated with mission effectiveness and unauthorized disclosure of sensitive information.”*

The strategy paper contains this diagram representing the shift from the old ways of doing business to the new information sharing model:



Whilst the DNI’s vision of Information Sharing as *“An integrated intelligence enterprise that anticipates mission needs for information by making the complete spectrum of intelligence information seamlessly available to support all stages of the intelligence process”* goes far beyond what would be considered acceptable in a European civil government context, the consideration of the problems and some of the goals and solutions proposed are very relevant.

The report goes on to set out these five strategic “keystones”:

- Intelligence Information Retrieval and Dissemination Moves Toward Maximizing Availability
- All Intelligence is Discoverable, and All Intelligence is Accessible by Mission
- Sharing Requires Greater Trust and Understanding of Mission Imperatives
- Developing a Culture that Rewards Information Sharing is Central to Changing Behaviours
- Creating a Single Information Environment (SIE) Will Enable Improved Information Sharing

It contains this diagram of the “Building Blocks and Key Questions” of Information Sharing:

	Description	Key Questions
Governance The “environment” influencing sharing	Oversight and leadership that help govern information sharing. How managers drive initiatives within organization and across agencies. Standards and guidelines to ensure a consistent approach.	<ul style="list-style-type: none"> Is there a clear value proposition for sharing among partners, i.e., quid pro quo or negotiated trade offs? Are MOUs or service-level agreements required? Do people understand how to abide by the law and policies? How are information sharing disputes resolved? Who are the key stakeholders?
Policy The “rules” for sharing	National policies, internal policies, rules of engagement, standards, and role of players internal and external to the organization.	<ul style="list-style-type: none"> Are laws, regulations, policies, and procedures in place that authorize, mandate and/or enable the organization to share? Is the organization complying with these mandates? Do laws/regulations/policies/procedures impede or constrain the organization/people from sharing? Are privacy and civil liberties sufficiently protected?
Technology The “capability” to enable sharing	The technology, systems, and protocols that provide the platform for enabling the sharing of information and that address security and privacy issues.	<ul style="list-style-type: none"> Are there common data standards and systems for organizing, identifying, and searching? Can participants push and pull data across networks? How is information protected; is the system auditable? Are tools/mechanisms available to manage identities; authorize, authenticate, and audit users; and ensure confidentiality?
Culture The “will” to share	The organizational approach and philosophy around sharing information and its ability to realign and adapt as circumstances change.	<ul style="list-style-type: none"> How do we motivate people and create incentives to collaborate and share information across organizations? Does the organization communicate across all levels? How does the organization adapt to change, and how responsive is it to stresses and opportunities? How are decisions and conclusions reached?
Economics The “value” of sharing	Ability to obtain and provide resources for information sharing initiatives, and external pressures (e.g., budget) that influence how resources are allocated and managed.	<ul style="list-style-type: none"> Has sufficient funding been appropriated to support the initiative? Have incentive structures been developed? Is the funding reaching the appropriate level within the enterprise to fully implement the sharing program? How do we measure performance?

The report concludes with a five-year long term plan and a 500 day mid-term plan to move towards four strategic goals.

STRATEGIC GOAL	500 DAY PLAN
Goal #1: Institute Uniform Information Sharing Policy and Governance	<ul style="list-style-type: none"> Core Initiative: Update Policy Documents Clarifying and Aligning Intelligence Community Authorities Initiative 5B: Collaborate to Protect Privacy and Civil Liberties Initiative 6E: Harmonize Intelligence Community Policy on “US Person” Information
Goal #2: Advance Universal Information Discovery and Retrieval	<ul style="list-style-type: none"> Initiative 2A: Create a Single Information Environment Initiative 2B: Implement Attribute-Based Access and Discovery
Goal #3: Establish a Common Trust Environment	<ul style="list-style-type: none"> Initiative 2B: Implement Attribute-Based Access and Discovery Initiative 2D: Establish a Single Community Classification Guide Initiative 5D: Improve the Information Technology Certification & Accreditation Process
Goal #4: Enhance Collaboration Across the Community	<ul style="list-style-type: none"> Core Initiative: Create Collaborative Environment for All Analysts Initiative 2C: Provide Collaborative Information Technology to Federal Executive Department Agencies and Organizations Initiative 2D: Establish a Single Community Classification Guide

Many of these questions and initiatives are relevant to the UK debate on Information Sharing.

Weapons of Mass Destruction

The lengthy report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction which might not, at first sight, seem relevant actually devotes a whole chapter to the subject of Information Sharing, starting with a strident call for An End to “Sharing”: *“The term information “sharing” suggests that the federal government entity that collects the information “owns” it and can decide whether or not to “share” it with others. [...] We reject it”*. They then, ruefully, have to accept that although they would prefer to use another term, “information sharing” has now become the accepted name (hence the title of this paper).

The main emphasis of the chapter is on the absence of , and need for, structures and processes for sharing intelligence information that are driven by commonly accepted principles of *risk management*.

“Finding the right compromise between information sharing and information security is a question of risk management. Each of these values should be accorded its proper weight, with due recognition of the increased importance of information sharing in the current threat environment. Successful execution of this risk management function requires hands-on, continuous planning and leadership—not disjointed and occasional adjudication by committee.”

It is hard not to interpret that as very strong criticism of the usual way governments go about implementing change.

The report also contains this very pertinent remark: *“No Information Sharing Environment can succeed unless it also acts as an information security environment.”*

Whether the purpose of the environment is to facilitate sharing or to limit it, many of the same principles hold – good security, reliable identification and authentication mechanisms, etc, as the chapter’s closing paragraph notes: *“The pursuit of privacy and national security is not a zero-sum game. The same technologies that protect against violations of privacy can also provide strong counterintelligence capabilities—something that will be essential if the Information Sharing Environment is to work over the long run. As the Markle Foundation plainly put it, any information sharing system must come with mechanisms designed to foster trust, “[f]or without trust, no one will share.”* Turn that sentence around and it more closely aligns with our current discussions and concerns in the UK and Europe.

Markle Foundation Task Force on National Security

The Markle Foundation Task Force on National Security in the Information Age has so far produced three reports on trusted information networks and sharing. In the second, “Creating a Trusted Network for Homeland Security” (Dec 2003), they are cautious about authentication:

“While authentication technologies are improving, no single approach can provide high assurance on its own. There are no smart cards or tokens that cannot be cracked, biometrics are not 100 percent reliable, and high-quality passwords are difficult to remember, manage, and enforce. With all of these technologies there are also people and process issues (such as enrollment procedures and audit trails) that can undermine their integrity. Therefore, a multifactor system is a preferable approach.”

However, it is more optimistic about the use of technology to help with accountability and oversight: *“Technology can play a key role in assuring accountability and transparency. For example, personally identifiable data can be anonymized so that personal data is not seen unless and until the requisite showing (specified in guidelines) is made. Selective revelation, another technique that permits a user to see only that data for which he or she has the appropriate permissions, can also be used. Auditing technology, too, can provide built-in recording and documentation capabilities to track how information is used, retained, and shared.”*

It also encourages the use of technology in the management and maintenance of stored information. *“Version control and update software can also ensure that information is updated according to a regular schedule. Expiration-enforcement software can ensure that data is unusable after a certain date. And data pedigree technology can permit users to track the information that has been used in an analytical product and visualize information dependencies.”*

Much of this is relevant to UK Data Protection concerns about information governance, accuracy and retention time.

The report also contains this interesting observation: *“Information sharing itself is not the goal; rather, it is the means by which we can maximize our ability to make sense of the information available.”* It is worth bearing this in mind when considering the subject – it is a means to an end.

It is also clear that, despite the sense of urgency created by 9/11, things in the US have not been progressing as fast as they could or should. The third Markle report “Mobilizing Information to Prevent Terrorism – Accelerating Development of a Trusted Information Sharing Environment (2006)” contains a copy of the letter they wrote to the President in 2005 saying *“We remain concerned, however, that risk aversion and bureaucratic resistance to change continue to hamper the carrying out of announced new policies.”* The report notes that:

“... many projects and initiatives have been delayed because key organizations have not yet internalized these changes, and because many still cling to previous ways of doing business. Clear government-wide guidelines for the careful handling of personally-identifiable information have not yet been promulgated. Information sharing efforts have been stalled by turf wars and unclear lines of authority and control.”

This echoes concerns raised here, e.g. on the implementation of changes recommended by the reports on the HRMC data loss incident, and elsewhere.

The report goes on to recommend the implementation of policies *“to overcome the significant cultural and bureaucratic hurdles that impede sharing”*, including:

- Adopting an authorized use standard to protect civil liberties in the sharing and accessing of information the government has lawfully collected [...]
- Taking a “risk management” approach to classified information that better balances the risks of disclosure with the risks of failing to share information
- Creating a government-wide dispute resolution mechanism to facilitate responsible, consistent and lawful information sharing
- Developing tools, training and procedures to enhance senior officials’ use of the information sharing environment and its technological capabilities.
- Encouraging the use of new technologies such as anonymization and the use of expert and data dictionaries.

- Employing immutable audit systems to facilitate both accountability and better coordination of analytical activities. [immutable audit logs was the subject of another of the Task Force's reports]

The report concludes that trust is the foundation and ends with these words, which are just as relevant here in the UK:

- For information sharing to succeed, there must be trust...
- Building trust requires strong leadership, clear laws and guidelines, and advanced technologies...
- Without trust, we will be less safe.
- Respect for privacy and other civil liberties, and adherence to the law, are core obligations of a democratic government, even when the nation faces grave threats.
- Such an integrated information sharing environment and policy framework, properly designed and implemented, will empower officials to act swiftly and confidently, but within democratic accountability...

Conclusions

The debate in the UK about government information sharing is very different from that in the US Intelligence Community but, in some key areas, there are clear synergies and lessons to be learned, primarily on the subjects of systems design and management policy and structures. It is hoped that this summary, by highlighting some of the common areas, can help that debate.

References

ODNI – Office of the Director of National Intelligence (<http://www.dni.gov/reports/>)

WMD – The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the President of the United States March 31, 2005 (<http://www.wmd.gov/report/index.html>)

MARKLE – Markle Foundation Task Force on National Security in the Information Age (http://www.markle.org/resources/reports_and_publications/national_security/index.php)