'Techno Risk' — Technology and Intelligence Data Need to Be Pushed

John Sliter

INTRODUCTION

On 1st August, 2003, a 15-year-old boy in the State of New Jersey foiled an abduction attempt when he pulled out his mobile camera and snapped photos of a man trying to lure him into a car. The teen also photographed the vehicle's licence plate and gave the evidence to police, who arrested a suspect the next day.

This is an example of the use of modern day technology to report crime, to exemplify a great 'techno risk' to international law enforcement.

When considering intelligence and risk, there have been numerous media articles about the failure of intelligence in the 11th September, 2001, attacks. This was the topic of discussion at the past two Cambridge International Symposiums on Economic Crime. How does the discussion around intelligence and the 11th September attacks fit into techno risk? The issue here is on how electronic intelligence is stored and subsequently used. 'Passive databases that simply record information are no longer appropriate, the database also needs to be designed so that it can push key information to relevant parties.'[1]

It is worth reflecting for a moment on the old adage that 'information is only data until it is shared'. This should include 'shared *quickly*' and 'shared *widely*' — with all law enforcement, regulators, and private sector investigative agencies.

RECOL — REPORTING ECONOMIC CRIME ON-LINE

The law enforcement community is well aware that international financial crime uses regulatory borders and concern for sovereignty to its advantage. Quite simply, criminals are well aware that the more borders they can cross, either physical or virtual, the less the likelihood that law enforcement will be able to catch up with them. The Royal Canadian Mounted Police (RCMP), together with some key partners, are developing a new tool that will allow victims of crime and other concerned citizens to keep pace with international organised crime. The initiative is entitled RECOL and the objective is to offer citizens a single point of entry, via the internet, to lodge a complaint concerning any fraud, traditional or internet-based, and have it directed quickly and efficiently around the globe to the appropriate law enforcement or investigative agency for action.

Journal of Financial Crime
Vol. 11, No. 4, 2004, pp. 322–324
© Henry Stewart Publications
ISSN 1359-0790

The integrated policing philosophy involves all levels of law enforcement working cohesively with one another, exchanging strategic and criminal intelligence, sharing tactical and operational knowledge, planning joint and individual actions, and communicating effectively. Using this philosophy and looking towards the future, it was possible to foresee a requirement for an internationally coordinated web-based complaint reporting system. Such a system would provide for strategic intelligence reports to ensure there is a national and international strategy, as well as tactical intelligence reports that are compiled and sent to the law enforcement agency (or investigative agency) of local jurisdiction to enable the targeting of specific organised crime groups.

Another key element of RECOL is the recognition of the need to partner with the private sector. If complaint information can be sent to the police force of local jurisdiction, why not to regulators or even to private agencies that have an interest as well? After all, global organised crime involved in international fraud does not pay heed to these 'boundaries'. To deal with this particular aspect the RCMP has partnered with an agency called the National White Collar Crime Center of Canada (NW4C). This agency was based, at least in part, on principles that stem from the NW3C (US-based National White Collar Crime Center).

One of the key components of RECOL consists of automating much of the functionality in the 'clustering, profiling and packaging' process. The RCMP uses an automated system of prioritising national investigations by scoring each incoming complaint using a system entitled PROOF (Prioritisation of Operational Files). Each file is assigned a score out of a possible 100 that is based on a comparison of each active investigation against a set of weighted criteria. Similarly, RECOL will continuously assess and reassess each incoming complaint in an effort to determine its PROOF score. This is a behind the scenes operation that dictates to which agencies a given complaint will be directed and whether a given complaint should be clustered, profiled and packaged. This involves an interface with various open-source research tools, including searches of the internet, to prepare background material on a given suspect or suspects with a view to the automated compilation of an investigative packet suitable for distribution to appropriate investigative agencies.

The G8 Lyon/Roma Group, Law Enforcement Projects Subgroup (LEPSG) has recently agreed to adopt stewardship of the RECOL project with a commitment of G8 members to provide a contact within each country, with a view to establishing a link into the RECOL and the US Internet Fraud Complaint Center (IFCC) systems. It is hoped that other G8 countries will create a similar reporting entity to RECOL and IFCC in order that all complaints involving a respective country could be filtered within each sovereignty. Only then will consumers be in a position to direct complaints that are of a cross-border nature to appropriate investigative agencies on a global basis.

The RECOL initiative is essentially a web-based distribution system — a means of improving customer service and allowing a complainant simultaneously to direct allegations of illegal behaviour to appropriate investigative agencies. RECOL is also a means of smart notification, smart in the sense that it will collect key supporting information and forward it to alert key agencies in a consistent and informed fashion. Expert investigation still requires the skills of expert investigators. However, RECOL will ease the administration time required by the various investigative agencies as they collect the basic data and consider initiating an investigation.

Implementation of RECOL will help to level the playing field by limiting the ability of transnational criminal organisations to use regulatory borders and concern for sovereignty to their advantage. Complaint information will fly across the globe on a real time basis to all levels of law enforcement and, for the first time, to regulators and private sector investigative agencies as well. More information on Canada's RECOL project is available at www.Recol.ca.

This is indeed intelligence-led, integrated policing.

HOW WILL FUTURE ONLINE REPORTING SYSTEMS LOOK?

Herein lies the techno risk. A search of the internet for 'on-line crime reporting systems' results in well over 300,000 hits. There are a great number of smaller independent police forces around the world starting to accept online crime reports for what they refer to as 'non-violent' crime. These are all individual and quite separate databases. In Canada they are called 'stovepipes' — those areas of singular interest that, by their inherent design, do not promote information sharing.

In the coming months and years it is hoped that these stovepipes will be torn down as quickly as they become established. Next month, Canada will host the first meeting of the G8 Law Enforcement Sub-Group RECOL project and it will be ensured that all international systems are designed to talk to each other.

In the long run, it is the author's personal vision that there will be systems around the world that are all linked and that all can accept digital reporting. Imagine walking down the street, spotting a known felon or a terrorist, and having the ability to snap a digital photo on a telephone, send it into a central reporting centre, and have that centre utilise facial recognition software to determine if it is the right person. A one-on-one comparison can be done in microseconds. Imagine that this centre would then cluster, profile and prioritise the information provided and, with the photographer's consent, send out a real time package to an appropriate law enforcement agency of local jurisdiction. They would also ensure that the intelligence information is shared with law enforcement and private sector investigative agencies from across the globe. *There will be no room for intelligence failures*.

All of this said, it must be appreciated that there are real privacy concerns with respect to facial recognition software and in some jurisdictions it has actually been considered a failure. For example, in Tampa, Florida, police recently removed the software. City Police Chief Bennie Holder said that the department had decided not to renew its annual agreement with Identix Inc. on using the company's Facial Recognition Software. 'While the software proved reliable in testing, there have been no positive identifications or arrests attributed to the software.'[2]

It almost goes without saying that civil rights groups hailed the move. Civil rights activists were of the belief that every person who walked down the street was subjected to an electronic police line-up without their consent. The Tampa police said the decision to end the test programme, which was paid for by the company, was based on the fact that it had not produced results, not on the privacy issues. This same face recognition product is used in similar form in Virginia Beach, Virginia, and also in several locations in the UK.

In summary, the future could be quite bright for law enforcement with respect to techno risk. However, it is imperative that full use of advances is made as they occur, and most importantly, ensure that the technology is used wisely. No more 'stovepipes', no more new databases. The current ones must be used wisely and technology must be allowed to assist in creating a truly integrated and international force to be reckoned with.

References

(1) The Dobney Corporation Ltd, Bath, England: 'Sharing Customer Knowledge', http://www.dobney.com/knowledge/ck_sharing.htm

(2) Holder, B. (2003) 'Facial Recognition Software Phased Out', press release, City of Tampa Police Department, 20th August.

***Supt John Sliter**, Director, Integrated Market Enforcement Team Program, Royal Canadian Mounted Police, Ottawa, Ontario.*

Bolkestein lays into financial services industry over Parmalat

The financial services industry has been lambasted by European Internal Market Commissioner Frits Bolkestein in the course of an address to a plenary session of the European Parliament during which he explained what is being or should be done in the light of the Parmalat collapse.

Describing the apparent size of the fraud as 'staggering', Mr Bolkestein said that 'the financial services industry had better get its act together, and do so fast. We need some real industry leadership to stand up and take charge: to clear out the crooks, expose their unscrupulous practices and curb excessive greed.' He also lamented the apparent complicity of professionals, together with failures of regulatory control.

Telling European MPs that better industry leadership is required, Mr Bolkestein outlined a range of EU measures in hand, including the market abuse, prospectus, investment services and transparency Directives. Parmalat has directly influenced the content of the draft revised company law Directive on the statutory audit function, which as a result of the scandal is likely to include additional provisions including: full auditor group responsibility for consolidated accounts of a group of companies; obligatory independent audit committees for listed companies; stricter auditor rotation requirements; and strengthened sanctions.

Also prompted by Parmalat, work in three other areas of corporate governance/company law will be accelerated in an attempt to have proposals ready by the end of this year concerning the role of non-executive directors, directors' responsibility for company accounts, and full disclosure in company accounts of offshore special purpose vehicles. Options for tightening the role and regulatory control of offshore centres are also being considered.

The failure of the giant Italian dairy-foods multinational has created a huge financial scandal, with PricewaterhouseCoopers calculating that the company owes €14.3bn. Parmalat founder and former chief executive Calisto Tanzi has been arrested on suspicion of fraud, embezzlement and false accounting. It has been discovered by Italian prosecutors that over the years Parmalat managers forged documents and invented billions of dollars worth of assets to offset liabilities — including an account at the Bank of America in the Cayman Islands of a Parmalat subsidiary which supposedly held €4bn of the company's assets but was found not to exist.