

Memex

Informant Management

The Need to Better Exploit
Technology

Author:

Peter Ship

Date

February 2010

Over recent years the sharing of intelligence by UK police forces and the security services such as MI5 has become increasingly important. A range of Government initiatives starting with the implementation of the National Intelligence Model, the roll out of the 'Impact Nominal Index' (INI) as an interim Solution and the future 'Police National Database' (PND)¹ show a clear desire to improve intelligence sharing, and there is no doubt that the picture across the UK has improved significantly.

My concern, however, is the gap that 'covert intelligence' leaves in this brave new world of intelligence sharing. At the highest level, intelligence sharing in respect to terror threats has improved dramatically. That said, above the Government Protective Marking System (GPMS)² restricted level, a huge amount of useful information sits untasked and unavailable to police and partner agencies across the UK.

While general police intelligence policy has shifted from 'do not share unless there is a specific reason to do so' to that of 'share unless there is a reason not to', this (partly cultural) change rarely encompasses covert intelligence operations. For much of the information gathered in a confidential environment (complex, challenging and involving understood risks) there may be no particular reason why information can't be shared, it is just that the process of sharing is seen as difficult and time-consuming.

In my own experience as a Senior Investigating Officer (SIO), in the aftermath of any sizable pro-active operation, for example a murder investigation, finding the will and the time to go through operational intelligence and then disseminate it was difficult. I was well aware of this failure to disseminate potentially-useful intelligence, but the pressures of work usually prevented it from happening.

While there may be little doubt that the utilisation of information gathered in a covert manner is more transparent than ever before, with international forces seeking advice on training and regulations in relation to how UK forces handle covert human intelligence,³ I feel that the UK is still suffering from a hangover linked to the traditional 'knowledge is power' approach to intelligence management, with police forces and individual departments wrestling with the perceived burden of de-sensitising and disseminating intelligence and not being fully able (or willing) to grasp the ideal of sharing information unless there is a clear reason to do so.

¹ IMPACT Nominal Index (INI): is enabling forces to establish whether any other force holds information on a person of interest. Police National Database (PND): will provide a single access point for searching information held across all of the forces' main local operational information systems and national police systems. <http://www.npia.police.uk/en/8489.htm>

² GPMS is the Government's administrative system "to ensure that access to information and other assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, storage, transmission and destruction" http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

³ Roger Billingsley (ed.) Covert Human Intelligence Sources; the 'unlovely face of Police work', Hampshire (2009).

Perhaps there is a little of the poacher-turned-gamekeeper situation here, because over the second half of my police career I was dealing daily with some of the issues discussed here and fully understand the need to keep sensitive information secure. In my role as an Informant Controller, I was responsible for retaining a vast amount of intelligence that was never acted upon.

For example, if suspect A was seen driving a car with the registration 'ABC123' by a beat officer it would be placed into the force's primary intelligence system and shared with others. However, if that same information was provided by an informant I would be far less confident that it would be shared. Given that informants are generally employed to provide 'hard to obtain' information, this failure to effectively utilise or share information clearly represents a significant gap that is likely to impact on the delivery of intelligence-led policing.

This single mundane example raises the issue of how many forces or agencies ultimately disseminate intelligence obtained from surveillance operations. How much legacy data, obtained in major or sensitive enquires, remains unshared, even following a prosecution which will see some of that information effectively become 'public knowledge'?

Another example can be found in relation to the UK's Holmes data.⁴ This UK case management system holds details of all murder enquiries and other major investigations such as serial rapes. While the enhanced Holmes II system (active since 2001) is easier to utilise, it is still difficult to search more than one account at a time, making the identification of relevant links or trends unlikely.

While Holmes accounts are generally initially sensitive, at some stage the majority of information and intelligence becomes less sensitive. Nevertheless, this information (ranging in sensitivity from details of those who live close to a murder scene, through to, personal information about the victim's family) is rarely then disseminated or even made searchable.

The same problem can be noted in surveillance logs, by their very nature full of information about suspected criminals, cars used, places visited, associates, etc. - all of which could potentially be linked to intelligence photographs. Whilst these logs are generally retained as paper records and not therefore not easily disseminated, statements are often generated to support prosecutions and relevant intelligence could easily be disseminated from documents that on disclosure become public knowledge.

⁴ Home Office Large Major Enquiry System 2 (HOLMES 2), the second incarnation of a case management system originally set up around the U.K. in the mid-1980s.

I am certainly not arguing that all crime or case information should be widely available, but much of it should be, especially where dissemination within police Intelligence Systems would not disclose sensitive information about operations or tactics. In my own professional experience, important intelligence about criminal association was often retained in Holmes and never shared – information which, as noted, is effectively within the public domain when it forms the basis of a prosecution case in the courts.

Technology, focused on a more holistic approach to an IT infrastructure, now allows organisations to create a simple but secure workflow processes which enables information - no matter what the source - to be safely aggregated along with 'restricted' intelligence to provide a complete intelligence picture of what is known. This intelligence picture could be made available to not just a single agency but nationally. Crucially, this type of approach is being adopted by UK police forces.

It is also worth briefly noting that the National Intelligence Model 5 has had a positive impact here, with standardised 'Problem and Subject' profiles now more often retained as sensitive until the conclusion of the operation and then made more widely available. The limits of dissemination are often dependent on the IT infrastructure of each force, but if such profiles are managed in a searchable database (Intelligence System) then it is more likely to be shared. When operations are managed in stand-alone systems or sometimes still on paper records, then the reality is that they will rarely be shared widely.

We are still some way off achieving a fully holistic approach to the management, sharing and use of information, particularly in relation to that contained in covert and sensitive databases. In order to deliver on such an approach, there needs to be a fundamental shift away from the traditional hiving off and siloing of covert information.

A force-wide covert solution would be one potential solution to the problem, allowing sensitive intelligence to be managed more effectively and assisting in the identification of links between operations and organised crime gangs at an early stage. Most importantly, such a solution could provide a structure to disseminate non-sensitive intelligence force-wide, with information appropriately marked during ongoing operations to allow for its rapid dissemination once an operation is concluded.

By disseminating covert intelligence to each forces Intelligence System, the government sharing protocols will ensure information is shared nationally.

For UK police forces and security services, the technology to build such a solution does currently exist. Now, in 2010, we just need attitudes to catch up with it – a step that will transform intelligence across the UK and better serve the requirements of today's intelligence-led policing environment.

⁵ The NIM is 'A Model for Policing' that ensures that information is fully researched, developed and analysed to provide intelligence that senior managers can use to provide strategic direction, make tactical resourcing decisions about operational policing and manage risk. <http://police.homeoffice.gov.uk/publications/operational-policing/nim-introduction.html>

Contact Us

Memex Technologies Ltd and Memex, Inc

UK and International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland
Telephone: +44 (0)1355 233804
Fax: +44 (0)1355 239676

America

Memex, Inc.
22636 Davis Drive, Suite 130
Sterling, VA 20164, USA
Telephone: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
Fax: +1 703 556 4282

Copyright ©

No part of the contents of this publication may be reproduced or transmitted in any form or by any means without the written permission of Memex.

More Information

For the latest information about our product and services, please visit

<http://www.memex.com>