RIPA and the Riots
Summary Report from a closed workshop on 23rd September 2011
Hosted by the Security Panel of the IT Livery Company

Chairman and Rapporteur: Philip Virgo

The meeting brought together a small cross-section of representatives of the law enforcement, communications and intelligence with operational experience. The chairman also received inputs from others with similar backgrounds. Much of the discussion was off the record. Those present had no wish to be involved in public debate on the RIPA or PACE.

The objectives were:

1) To identify whether operational experience in the courses of the riots raises issues to do with the practical operation of RIPA, PACE and the use of Mobile Communications (whether by rioters or police) that could/should be addressed as matter of urgency (e.g. in advance of the Olympics).

2) Whether other experience with RIPA and PACE needs to be fed into policy reviews.

3) If so, what channels of communication should be used.

The main points raised during discussion for use with wider audiences were:

1) What problems were there, if any, with regard to RIPA and PACE getting in the way of effective response, where political attention would help?

There were many problems during the Riots but RIPA was not one of them. We did not discuss PACE.

The RIPA routines worked well and there were no problems with volumes of requests or response. The main problem was with information overload on the police side, e.g. twenty tweets per second to be collated, and the inability to take and use direct feeds from proprietary systems. The analytics tools/teams were not capable to handle the load and the filtering systems did not do the business. All but one of the operators and telcos have automated systems for handling requests and the exception appears to have been fully staffed for the volumes. The response times of the mobile operators, including those based outside the UK, were excellent once a prioritisation routine had been agreed.

The SPOC system worked and contrasts well with those in other countries, but it would be helpful if there fewer of them (why is the word “single” such a problem) and if those running them were better trained both on how to use the routines and what they could reasonably request. Response can be delayed and opportunities lost in consequence, but there was no indication that this was a problem during the riots when both sides rose to the occasion. The bigger test of RIPA may, however, be yet to come with requests for analyses to aid investigation and prosecution as opposed to operational response.

3. What other problems are there with RIPA and PACE, including the use of intercept as evidence which need better informed political attention?

There are many problems with the use of intercept as evidence which lead to a view that it should not have priority. Those nations which allow intercept as evidence have different legal regimes (e.g. examining magistrates who “filter” the evidence) but even so have they practical problems. The US/Aus/Can don't have ECHR and can keep classified techniques hidden. UK protectively marked

material has no automatic exemption from release to defence counsel. The US/France “control abuse” of non-judicial interception by having a limit on number of targets but there are ways round. The Dutch recognise that encrypted data has (by the act of encrypting it) no expectation of privacy.

The most significant obstacle is the extra cost (substantial) of gathering, securing (to preserve integrity) and retaining data that may need to be used in evidence, as opposed to throwing away that which is of no value for intelligence purposes. That which is collected and used for intelligence purposes is often not of evidential value. There was discussion of the problems of quality in general: from packet loss to corruption before the material has been secured with hash trees.

The law distinguishes presumed sensitive content from presumed less-sensitive transaction records and focuses is on initial collection of what you already know you want and how it will be addressed, presuming that you have had time to make a case and get it approved. It does not distinguish computer scanning from human listening. This could hobble the routine protective monitoring of communications against virus and other attacks - if the material collected might also be called on for evidential purposes by the defence or in support of private prosecutions – whether relevant or not. The current legal situation prevents such legal fishing and also helps restrict demands (increasingly common in the part of financial services and other regulators) to retain just about everything.

The issue of threats against staff (or facilities) seen (or assumed) to be involved, especially staff of service providers is very real, given that complex intercept evidence would most likely be used against organised crime or terrorism. The protection of staff or service providers might be addressed by an amendment to RIPA to restrict court access to the government interception services which have taken information under approved processes from the service providers. That would not address the wider and growing problems of witness intimidation in general leaves. The latter was not discussed.

Those likely to be subjects of interception choose service providers to protect their interests and increasingly use international/global service providers. It is common that only one end is the target and the interests cross borders anyway. Organised crime soon organises around known capabilities.

The current situation reduces collateral damage to innocent parties – as in the US where there is a requirement to not only tell you when a warrant is cancelled, but also to inform all your contacts that their calls to you had been listened to, but have now been deleted **and you are no longer a suspect for something serious but unspecified**!

Agencies would quite like successes under the current regime to be more visible when funding is debated.

4. Were there problems with regard to police communications which need attention? e.g. over-load?

Airwave performed well because the volumes of police traffic were not abnormal, unlike on New Years Eve or at a major sporting (Olympics) or social event (Royal Wedding). Similarly the volumes of mobile traffic were not abnormal. The riots did not involve large crowds or numbers. There are problems with procurement and inter-operability but these did not have impact during the riots. They are unlikely to be addressed by current plans for a procurement company.

5. Are there areas where the more rapid, perhaps "real time", analysis and presentation of large volumes of data could make a significant operational difference?

Yes. The mobile operators have the technologies to map mobiles on the move, including samples/targets (using these operationally for service monitoring) but the police struggle to handle the material already passed to them. A distinction was made between riots involving hundreds and major sports/social events with 100,000s. In the latter event sampling (say 1%, of a large crowd) could help avoid the problems of overload.

6. Other areas that need to be addressed:

Mobile operators already have the ability to disable sim cards individually, (for fraud prevention purposes), or geographically, (to give priority to the emergency services). But the latter will also take off air those emergency services which have not registered their phones (Airwave phones are registered

as part of the service). It will also affect current or prospective victims as well as perpetrators and remove a valuable source of operational intelligence. None of those present thought that proposals to shut down mobile or social networks in the event of rioting or disturbance was a good idea.

The routine use of security systems that depend on always-on communications systems, e.g. electronic tagging, needs review and debate in the light of known vulnerabilities (including systemic compromise).

There is a need for constructive debate on the use of data matching to bring together multiple sources of information across organisational and technology boundaries for crime (including fraud but not just for fraud) detection and prevention. We need to remember that in the terms of European Human Rights Convention “Right to Life” (2) comes before that to “Privacy” (8) and the restrictions "necessary in a democratic society" which apply to 8 do not necessarily apply to 2.

There is a need for the cross-boundary sharing of information on known fraudsters - including those formally dismissed for fraud even if not prosecuted or convicted.

A major problem is that “there is no money other than from law enforcement budgets”. Spend does not help improve supplier profitability except when it can be directly related to the reduction of fraud against Telcos and ISPs themselves or their customers (e.g. Banks) will pay. Most customers will want a similar “business” case.

There is evidence that cuts are being made to reduce spend from communications budgets which have a disproportionate on overall costs/service: e.g. the withdrawal of data mobiles used by front-line staff – police, emergency services, health etc. to record and transmit data at the scene/time of incident/encounter/transaction.

There is also a need for continuity of effort, particularly on skills issues where Skills for Justice has just issued a call for another round of activity on National Occupational Standards after a gap of three years. Meanwhile e-Skills has launched the Security Stream of the National Academy for IT Skills based on those qualifications which are already recognised by employers.

7. Who could/should take action and/or be consulted with regard to the problem areas identified?
8. What channels could/should be used to communicate the need for action (and to whom)?

The Communications Crimes Strategy Group (CCSG) brings together the mobile operators, telcos, ISPs, Home Office and Law Enforcement and is the main channel of communication for those actions which do not require political action or the involvement of the communities not represented.

The Communications Data Stakeholders Working Group has a much narrower remit. It currently excludes any defensive use/motivation/justification. Should that be reviewed?

9. Follow up action plans for those present, including agreement on what should be reported

The need to improve the analytics capabilities of the police should be raised via CCSG, including the need to assemble a business case for predictive analytics for crime prevention and to act on the skills problems.

The EURIM Information and Identity Governance Group should be asked to address the conflict between requirements to retain data (without recognising the costs and vulnerabilities this leads to) and requirements to delete it as soon as no longer required.

The EURIM Information and Identity Governance Group should also be asked to look at the benefits of feeding data from multiple sources (and across organisational boundaries) into shared analytics engines for fraud detection and preventions and to address the issues this raises.

Philip Virgo will circulate a call for expressions of interest on the action on issues raised and will follow up on the skills issues with Skills for Justice, e-Skills and the Council of Professors and Heads of Computing (many of whose members already help train local police and forensics teams).