

Summary evidence for All Party Internet Group Inquiry into the retention of and access to communications data for law enforcement purposes

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



Introduction

EURIM supports the need for reasonable extensions to surveillance measures that assist law enforcement agencies as criminal and terrorist activity increasingly makes use of the electronic world. However, such measures must have appropriate safeguards, be proportionate in their impact on industry and human rights and be likely to achieve the objectives targeted. Some of EURIM's industry members have operations in countries where terrorist activities, including kidnapping and extortion, are a daily operational risk. Others lost friends and colleagues on September 11th and are similarly "in the front line". They are concerned that current proposals could make them more, not less vulnerable, while diverting resources from that which is worth doing.

One of EURIM's main concerns during the course of debate on the retention and use of communications data for law enforcement purposes has been the need to educate successive generations of officials. Career rotation means that those who have come to understand what is practical are replaced every year or so. Those responsible for consultations tend to contact only suppliers and are often separated from those responsible for implementation by two or more staff rotations. They commonly have no previous experience of working with the electronic communications or the private sector security communities. One consequence is the use of definitions, concepts and analogies which have little meaning outside the world of legislative draftsmen. Another is the assumption that "Trusted Third Parties", including public sector agencies, are actually trusted. Those responsible for security in major international and financial services users are well aware of incidents in recent years where those in national security, law enforcement and other public sector agencies in the US and UK have abused positions of trust for personal gain. Some agencies are known to have internal processes that would not be tolerated by any private sector regulator, let alone a financial services regulator. There are similar issues with regard to some suppliers of security software (including encryption) and services (including technology support).

Another concern has been to try to reconcile the stated objectives with the advice given to large Corporations by their legal advisors as to the practical interpretation of the legislation as drafted. Thus the definitions of communications service providers appear to embrace the ICT operations of almost any organisation, however modest, as well as data in transit through the UK or held overseas. The UK subsidiaries of major US financial institutions have expressed concerns that a combination of UK law and loose statements on "mutual assistance" may be used by their own Federal or State governments, let alone other national governments, to gain accesses which would not be permissible under US domestic law. It is proving difficult to reconcile definitions of communications data for authorisation purposes with the way that routing and billing data is identified, stored and retained (or not) in the real world. This problem is compounded by the changing scope and nature of "communications" data as technology evolves and new services and business models emerge. The benefits from creating a stereotyped model for those wishing access to data on who is communicating with who, but not to other types of stored information, need to be balanced not only against the costs and liabilities to which CSPs might be exposed but also the ways in which such a model might distort the evolution of e-business as a whole. There is a need to expose draft legislation to broad industry review for meaning, practicality and impact assessment at the earliest possible stage. There is also a need for open and publicly accountable processes for regularly updating guidelines as to what is practical and reasonable at any point in time.

Putting the Regulation into RIPA

The trigger for RIPA was the need to review the Interception of Communications Act but that the legislation now covers many more statutory authorities than had powers under IOCA. There appears, as yet, to have been no public consultation on what powers those other authorities should have in this area, if any.

Moreover, it is now apparent that many authorities claim access to stored data (not just communications data) under previous legislation: some under World War 2 emergency powers, others under more recent legislation. The validation of requests from such authorities for information on staff and/or customers is a growing problem for those who take Data Protection seriously. Thus one EURIM member with branches in most high streets instructs staff to pass all such requests to central point for validation. They inform the originator of the single central point of contact (SPOC) to which information will be passed and request confirmation of the reference and contact details to be quoted. Many enquiries “lapse” at that point. The confirmed requests are then passed back to the branch for processing. Four full time staff are needed to handle the enquiries (excluding those who actually process the requests). There is no time or resource to check whether lapsed enquiries were attempts to gain data for the purposes of fraud or impersonation.

EURIM therefore flagged the need for a single, well-publicised point of contact (SPOC) for all enquiries under RIPA, to enable organisations to rapidly check the provenance of requests for information. The implication is that all requests from originating organisations would have to be routed through, or at least notified to, that point of contact. It was also suggested that point of contact also be responsible for the necessary training and support of those claiming investigatory powers. Since then, it has emerged that not only does every law enforcement agency wish its own SPOC (and some want multiple SPOCS), but none wishes act on behalf of the 1400 or so other statutory bodies claiming investigatory powers. Meanwhile the Gloucester SPOC through which most Trading Standards Officers routed their requests has been dismantled, following advice that it might not be legal under RIPA to handle enquiries for others.

Given concerns regarding the possible abuse of investigatory powers, whether by those genuinely working for authorities with powers or by those impersonating them, there is also a need for well-publicised codes of conduct for all with investigatory powers, with greater transparency of the whole process to enable reaction to potential, as well as actual, breaches. These need to be backed up by effective processes (at all levels), including for taking effective action against those in breach - with realistic and enforceable penalties and sanctions. There is also a need for clarity and transparency with regard to the meaning of “mutual assistance” and the routines for approving this. This is particularly important for organisations operating internationally under multiple jurisdictions whose data may only be in transit through the UK or who may have contracted operations to facilities management suppliers who hold data outside the UK or move processes and/or control between global centres according to time of day or other operational considerations.

Given the growth in controversy and complexity there appear to be a number of possible ways forward but none is likely to be practical without a wholesale rationalisation of those able to claim access to stored information, including communications information, and the publication and enforcement of standard codes of conduct and practice and the necessary supporting processes. The starting point should be the production of a grid of those public authorities which already claim access to information, the legislation under which they claim that access, how many requests they have made over the past 18 months (or so), how many they are forecast to make under the reformed RIPA - and why the number is expected to fall or rise. This is, however, only a starting point. Rather than enshrine the past and/or try to predict the future it may be better to involve a broad representation from industry and public sector, with open and transparent consultation and approval routines, in maintaining rolling lists of relevant authorities and definitions.

Building Co-operation in the Fight against E-Crime

The debate over investigatory powers has revealed widespread confusion and ignorance on all sides and it is apparent that effective investigation in the electronic worlds requires not only skills and resources that are in particularly scarce supply among law enforcement agencies, but co-operation with industry, both suppliers and users, that goes well beyond “mere” access to information. Effective action to help the fight against crime and terrorism, as opposed to “merely” investigating after the event, also requires being able to rapidly call on the assistance of industry experts with law enforcement training and powers who can use the technology itself to rapidly identify and track, trace and authenticate the information really needed (e.g. calls being made and messages sent) and also preserve it for forensic use if necessary. This raises issues of governance that in North America are handled by the use of reservists, deputies or specials (agents or constables). We need an open debate as to whether we can adequately address the challenges we now face, internationally as well as nationally, without following suit.