The Risks and Costs of UK Escrow Policy

Ross Anderson

The Committee will have heard from others that the Electronic Commerce Bill proposals will impose considerable costs on industry and infringe personal privacy. The Committee already has a copy of a paper I wrote with some US colleagues on this issue for a similar investigation by the US Senate. I would like to add some further observations which may help the Committee assess the balance of costs and benefits, with particular reference to consumer rights and law enforcement. These two interests are crucial to the growth of public confidence in electronic commerce, and they are not really in conflict.

I have worked in computer security and cryptography for over fifteen years. I presently lead the computer security group at Cambridge University where I have been since 1992; before that I worked mostly in bank computer security and for bank suppliers. I have consulted on many other applications since; most recently I have been advising the Department of the Environment, Transport and the Regions on a potential move from lorry tachographs based on paper discs to devices that use smartcards. I have also helped the insurance industry assess the security of burglar alarm signalling, acted as an expert witness in cases of 'phantom withdrawals' from cash machines on behalf of both customers and the police, and helped the electricity industry build more robust prepayment electricity meter systems.

These 'industrial' uses of cryptography are now dominant. In addition to cash machines, electricity meters and burglar alarms, people use mobile phones, satellite TV set-top boxes, and encryption routines in their web browsers which enable them to shop reasonably safely on the net. Many more such applications are in the pipeline. Almost all of them are designed to prevent fraud of one kind or another; there is no tension with law enforcement. Laws which make it more expensive to use cryptography will harm consumers and have a directly adverse effect on crime prevention.

Let me deal firstly with consumer rights. The proposed Bill's presumption of validity for electronic signatures which met the liceinsing criteria could make it much harder for the victims of electronic frauds to seek redress, whether against banks, merchants, credit card companies or insurers. Many people have bitter experience of the banks refusing to refund 'phantom withdrawals' made from their accounts as a result of cash machine fraud – even once a number of people had been sent to prison for this offence, many banks continued to maintain that their systems could not possibly be at fault.

Some people in industry claim that smartcards will solve the problem but I do not believe them. I will show the Committee some slides of attacks on smartcards; even in the absence of technical attacks, the customer will still depend completely on the terminal in the shop for knowledge of what she is signing; so the terminal might display an electronic cheque saying "pay Bloggs market traders ten pounds", while the electronic transaction presented to her card and which she actually 'signs' might say "I hereby mortgage my home and make over the proceeds to Mafia Real Estate Ltd". For these reasons and many others, it is certain that electronic signatures will turn out to be open to forgery and manipulation, just as plastic cards have been.

As a model of legislative restraint and good sense, I would respectfully commend the Australian draft e-commerce Bill, whose section 15 provides that *'For the purposes of a law of the Commonwealth, unless otherwise agreed between the purported sender and the recipient of an electronic communication, the purported sender of the electronic communication is bound by that communication only if the communication was sent by the purported sender or with the authority of the purported sender'.*

There is also the matter of continuing the enforcement of those existing laws which are relevant and workable. As an example, I recently discovered that Amazon.co.uk has failed to register under the Data Protection Act, and passed the matter to the Registrar. It should be of concern to the Committee that a company seen as the model for information age businesses everywhere should trade in open defiance of UK law.

This leads naturally to the law enforcement issue. The proponents of key escrow often talk about police communications intelligence, but in my experience of helping police with investigations (both as a banker and since), the police interest is overwhelmingly in traffic data (who called whom) rather than access to content. Although, as NCIS recently observed, there have been some cases in which encrypted data was found on storage media, this is different from encryption of message traffic and would not be affected by key escrow. Message encryption has not yet been a problem, and given UK policing practice it is unlikely to become one. The Committee should note the unwillingness of the Home Office to spend the money to provide a decent national computer forensics lab. Such an investment is in my experience long overdue.

From the criminal viewpoint, message encryption is relatively uninteresting – if you have a three hour encrypted phone conversation with someone in Medellin you will bring yourself to attention. Instead, criminals try to make their communications unobtrusive, and the typical tool is the prepaid mobile phone. The rational countermeasure (now law in France) is to require purchasers of prepaid mobile phones to show proof of identity.

However it is not police concerns which drive cryptography policy, but national intelligence concerns.

Organisations such as GCHQ and the NSA gather much of their material by intercepting communications and there has been a fear that if target countries got access to good cryptography, this source would dry up. Cryptography policy was therefore aimed at nonproliferation, and operated by a combination of export controls and informal arm-twisting of suppliers. This used to be secret – hence the cover story about police communications intelligence – but the veil has started to lift. I recommend that the Committee read the appended paper by Henry Beker and Chris Amery; Beker is a long time insider whose companies have supplied both GCHQ and banks for decades.

The old nonproliferation policy has failed because the demand for good cryptography in the commercial applications mentioned above has created many companies worldwide with the necessary skills, supported by open research and development. More and more exceptions had to be made, firstly for banking, then for pay-TV, then for electricity meters; in the end, the policy suffered a 'death of a thousand cuts'. It has now been abandoned by many governments. The USA has released the KEA and Skipjack encryption algorithms which it uses to protect its own secret data, and the French government has lifted its traditionally strong crypto controls with the comment that defensive information security (i.e., enabling French businesses to protect their commercial secrets from us) is more important than the offensive kind (their getting secrets from our companies). Insofar as cryptography is used to protect the privacy of communications, French crypto controls hindered the defensive mission while not helping the offensive one. Similarly, British crypto controls will make it harder for our firms to protect their communications while not helping GCHQ much with reading French, or Russian, or Indonesian traffic.

Key escrow would have to be global to achieve its stated purpose, and there is now no prospect of this. Yet the intelligence agencies cling to their traditional policies. It is natural that organisations do this in times of change, and the cryptologic environment is changing rapidly; from military to commercial products, from secrecy mechanisms to authentication mechanisms, from a few closely controlled cost-plus suppliers to the rough and tumble of the marketplace. Even at the most basic level, the scientific emphasis is shifting from mathematics to computer science. We have had a change of government, the start of a shift from official secrecy to freedom of information, and to cap it all, GCHQ has had three Directors in the past two years.

What should be done? Well, the UK suffers from a peculiar disability in that the organ of central government responsible for defensive information warfare, CESG, is subordinate to the body responsible for offensive activites, GCHQ. In many other European countries these two functions are separate and report through separate ministers. Thus a more balanced view can be taken of the merits of defence and offence, and the usual result is that defence prevails – as for example in France. I suggest that CESG be set free and transferred to another department, such as the MoD or DTI. Such a change could provide the organisational shake-up and change of focus which now appears to be needed if the UK is to acquire modern and effective policies on information security.