Mad scramble

THE THREAT OF KEY ESCROW HAS GONE AWAY — BUT IT COULD BE BACK. DANIEL SABBAGH TRACES ITS TROUBLED HISTORY AND AWAITS A GOVERNMENT/INDUSTRY-INSPIRED ALTERNATIVE.

Encryption and its regulation by the Government has become the most controversial issue in the IT industry over the past five years. It has been the subject of a sustained rebellion by big business, in an unlikely alliance with cyber-liberties groups, against politicians. It has seen one ex-government IT minister admit that his policy was wrong just a week before the current IT Minister announced a partial back-down over plans to regulate its use. And the debate has been dogged by unproven accusations that successive government policies, Tory and Labour, are just a front for the interests of intelligence agencies MI5 and GCHQ.

Yet encryption is also crucial to the future of electronic commerce. How can the stuff of spy thrillers also be the technology of SSL transactions? What on earth is going on?

This year, the Government plans to pass an e-commerce Bill — late April saw its first publication. It aims to clear up the laws governing e-commerce in a new Labour bid to make the UK 'the best environment worldwide in which to trade electronically by 2002'. It is this long-awaited Bill, that will regulate e-commerce, which has been the subject of three years of intense debate and persistent controversy since the plans to regulate e-commerce first emerged in 1996.

Caspar Bowden, director of the Foundation for Information Policy Research (FIPR), says: 'The public introduction of cryptography lit a slow-burning fuse that has created the most intractable civil liberties dilemma of the computer age and paralysed public policy on how the explosive growth of the net should be regulated.'

This March, after more than two months of waiting, the debate should have come to an end. The Government was expected to lay down the law, by publishing the principles for the e-commerce Bill which even then was only weeks away. It failed to do so. Instead, the Government partially backed down, giving the industry just over three weeks, until 1st April, to come up with a better policy in the most controversial area of the Bill: encryption. The result is a policy which, at the time of writing, is in some disarray.

What the Government wanted to do, and had to retreat over, was find a way of controlling the use of encryption by tapping it. Encryption is used to scramble email messages to make them unreadable to prying eyes and ensure financial transactions on the web are unhackable.

The problem is that the only encryption worth having cannot be cracked by the fastest supercomputers. That's no problem for Joe Public, but it's a big worry for governments. Their concern is the use of the internet by organised crime. How can you prove that drug money or mob messages were sent from Colombia to Manchester, or that somebody has pornography on their hard drive, when you cannot crack their code?

The Government, in short, is scared of good encryption. The development of it has, until the internet came along, always been tightly regulated. The only centres of expertise were intelligence organisations; in Britain, an arm of Cheltenham-based GCHQ, the Communications Electronics Security Group (CESG). Even when academic publication began in the seventies, encryption was tightly controlled and today encryption policy has not recovered from the grip of intelligence agencies. But the explosion of the internet in the early nineties made its impact; it made encryption necessary for e-commerce. At the same time, the internet provides an easy means to evade national jurisdiction and distribute encryption technology beyond government efforts at regulation — and it comes with a vibrant pioneering culture opposed to any government control.

The Government's plans to regulate the use of e-commerce took two forms. Firstly, it wanted to provide legal backing to a secure form of identification – digital signatures; effectively an encrypted certificate backed by a third party which proves you are who you claim to be. Secondly, the Government wanted to tap into the encryption used for scrambling messages and transactions in the same way that phone calls and post can be intercepted.

The mechanism chosen is generally called 'key escrow'. Encrypted messages are created using keys (very long numbers). Key escrow means that a third party holds a copy of your private encryption key, which it would give over to law enforcement agencies if required.

Key escrow has always been controversial. Opposition from loud-mouthed cyber libertarians would have come as no surprise to the Government and was a lobby it doubtless believed it could safely ignore. Yet the concerted opposition that followed from big business must have been surprising. Neil Barrett, a security expert with Bull Systems, said: 'The Government didn't anticipate that level of opposition. But if you look at the people who came out against key escrow, most of them are reasonable, sensible, business people.'

The plan first surfaced, bizarrely, in an independent analysis of the security needs of the network for the National Health Service, NHS net, published in April 1996. It proposed an encryption system for doctors which should support key escrow and hinted that it was likely to become a standard restriction on the use of encryption in the UK.

Early fears focused on the perceived invasion of privacy. Doctors saw encryption as a tool to secure patient data across new health networks; key escrow was a licence for the Government to hack in to medical secrets. To this day, IT-savvy GPs in the British Medical Association remain deeply opposed to key escrow.

Other arguments emerged which proved more successful. Firstly, key escrow is not technology-neutral, a point which later began to worry the banks. Secondly, the internet's global nature meant that the policy was practically unenforceable. Criminals were hardly likely to use UK-mandated key escrow if they could get away with it.

Despite the objections of the BMA, the last Conservative government bought the proposal. Just two months before 1997's general election, Ian Taylor, then IT Minister, published a plan to regulate the use of e-commerce. Rather long-windedly, it effectively insisted that virtually everybody adopted key escrow by stating that all providers of encryption services, to be called Trusted Third Parties (TTPs), had to be licensed. A condition of licensing was key escrow.

TTPs do have some use in e-commerce. They can provide external validation for digital signatures, date- and time-stamping services, provide encryption software or even generate encryption keys for you, and can list a directory of users with a link to their encryption keys so you can send them scrambled email.

This March, the Post Office launched the UK's first major home grown service for businesses. But the licensing condition was a special extension. Its core purpose was to permit the tapping of encryption, although the DTI tried to argue that business would want a facility to recover lost or forgotten encryption keys.

Now the Government got serious. Business began to wake up and became very concerned. Objections were led by whole sections of the technology industry. But more importantly, opposition came from the banks, who were most likely to launch TTP services, led by the banks' trade body, APACS.

Steve Thomas, head of security with APACS, said: 'We accept that there is a need to meet the needs of law enforcement, but key escrow has always been the wrong way to do it.'

Banks realised that the proposals were not technology neutral and could have an impact on their existing encryption systems, many of which had been obtained under special licences. Key escrow was totally technologically unproven, costly to implement, potentially unpopular with customers, and was not proving popular in competitor economies. Countries such as Germany, Canada and Ireland were not intending to adopt key escrow, despite American pressure.

Labour appeared, in Opposition, to be against

The new policy at a glance

- **Key escrow to be dropped if industry can come up with a better alternative.**
- **Special industry/government taskforce created to consider alternatives.**
- **Emphasis on maintaining existing legal powers to intercept and access email.**
- **Digital signatures to be made legal when backed up by a licensed certification authority, or when covered by existing contract law.**
- **No escrow of digital signatures.**
- **Voluntary licensing of certification authorities.**
- **Consultation on the problems of legal liabilities in e-commerce.**
- **Consultation on the problem of spam email.**
- **No change in export controls of cryptographic products.**

the plan, stating in a pre-election policy document that was to be repeatedly quoted (and in reality taken too seriously) by anti-escrow campaigners: 'Attempts to control encryption are wrong in principle, unworkable in practice and damaging to the long-term economic value of corporate networks.'

When the Labour Party won the election, the policy was thrown into limbo. What came out the other side was another dose of key escrow. A consultation document appeared in April 1998 backing key escrow through the licensing scheme. This time, the scheme became voluntary as a concession to growing criticism. It also added a clear decision to make digital signatures legal, but then undermined this by linking this to key escrow. The Government did not want escrow — to take copies of citizens' or companies' digital signatures, which clearly would have been a very worrying development — but it did say the only legal digital signatures would be those which were validated by a licensed TTP, one that used key escrow. The Government also appeared to forget that some encryption standards, such as s/Mime used in Microsoft Outlook, generated encryption and digital signatures from the same key.

> **Ministers told industry that the Government was PREPARED TO DROP KEY ESCROW if business could come up with a better solution**

The result was an outcry which failed to go away — an alliance of civil liberties groups, banks, doctors and the IT industry. And the lobbying intensified when the Government announced last November that it was going to legislate. All eyes were on a final consultation paper which would outline the principles in the Bill, promised before or shortly after Christmas '98.

The paper was held up when Peter Mandelson, who was rumoured to want to drop key escrow, resigned as boss of the DTI. In the meantime, the final blows against the policy were struck in public hearings in Parliament, of the Commons Trade and Industry select committee. With canny timing, the select committee began the hearings into e-commerce. It heard a remarkable range of opposition to the key escrow policy, from banks to the Post Office and legal and cryptography academics. Only the police, in the form of the heavyweight National Criminal Intelligence Service, were in favour. The writing was on the wall. And finally, Ian Taylor, now an ex-minister, publicly recanted. Just a week before the final government consultation paper arrived in March, the man who introduced the policy said: 'I'm beginning to think that I was wrong.'

When the paper came out, the Government gave in. The decision was leaked after a business breakfast held at Number 10, attended by Tony Blair, the Prime Minister, and Home Secretary Jack Straw, with Trade Secretary Stephen Byers, as well as chairmen and chief executives of IT and telecommunications companies. Over breakfast, ministers told industry that the Government was prepared to drop key escrow if business could come up with a better alternative. A special government-industry task force, called Cojet, has been set up (1st April) to find a solution. But the Government told the industry it was still concerned about the use of strong encryption by criminals, leaving a difficult balance to be struck.

In a press conference, IT Minister Michael Wills did his best to put a positive spin on the climbdown, while warning that if no better solution could be identified, then key escrow could be back. The paper also retained the idea of voluntary licensing of TTPs, to set minimum service standards, but did not link it to key escrow.

Digital signatures would be made unambiguously legal if they were validated by a licensed Third Party — a contorted process which FIPR's Bowden describes as a 'stump from the old policy which should be cut off'. But the Government also admitted that in most cases digital signatures were legal, rendering the licensing process not strictly necessary. For good measure, the Government chucked in a consultation of whether it should legislate on the growing levels of spam email and the balance of legal liabilities in electronic commerce transactions. The reaction was, in the words of APACS' Steve Thomas, 'two cheers'. Now the race is on for a compromise solution.

The preferred approach from industry is two-pronged. First, replace key escrow with a simpler and cheaper legal requirement to compel a plain text version of an encrypted document or communication from a suspect. Second, invest serious money in a public/private partnership into creating a centre of expertise in investigating crime involving computers, which could include the development of monitoring techniques which don't require the creation of a complex, costly system with no other useful purpose.

Getting the compromise right will be vital. Nicholas Lansman, secretary-general of the Internet Service Providers Association, said: 'The Government has had three years to get this right. We've got three weeks. But we've got to do it; we have to make e-commerce work for everyone.' □

● *Daniel Sabbagh is senior reporter on Computing magazine.*

PCW CONTACTS

Further information
www.starfish.com
www.imc.org/pdi
www.argosoft.com/vcard.html