USA's new encryption policy: balancing e-commerce needs with security interests

Jay Forder

Bond University, jay_forder@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder. (1999) "USA's new encryption policy: balancing e-commerce needs with security interests".

By the end of this year, [395x691] will allow the export of [27x691] Strong encryption is an obvious [27x678] requirement before trade over an open [27x666] network (like the internet) is widely [27x654] accepted. This explains why a lot of [26x641] criticism has been directed at the US [26x617] administration for its ban on the export [26x604] of strong encryption products. [26x604] US companies in particular argue [166x604] they [26x592] are prejudiced when competing with [26x580] non-US encryption products. Over the [26x568] last 5 years the US government has [26x555] responded by gradually relaxing its [26x543] controls. This article notes the latest [25x531] development, an announcement by the [158x531] US administration that it will almost [25x506] completely relax the ban, while at the [25x494] same time introducing legislation to [25x481] strengthen and clarify the powers [25x469] of law enforcement agencies.

**US insistence on key recovery systems**

The US exercises control through the [International Traffic in Arms Regulations and the Export Administration Regulations]. The administration holds the view that electronic intelligence, especially wiretapping, is crucial to effective law enforcement. It argues that the export of strong encryption products would enable the country’s enemies to avoid effective surveillance of electronic communications, and this would hamper the fight against terrorism, foreign threats, drug trafficking, espionage, etc.

Until 1994, applications by US companies to export anything more powerful than the 40-bit Data Encryption Standard (DES) were routinely denied. In February 1994 a special arrangement was introduced for key escrow systems. A key escrow system requires a copy of the decryption key to be split into several parts, and for each part to be lodged with a trusted third party (“escrow agent”), so the key can be reconstructed when required. This special arrangement for key escrow systems allowed multiple exports without individual licences after an initial review of the escrow system. It marked the beginning of preferential treatment for systems with a recoverable key.

Later changes in 1995 and 1996 were designed to further encourage the development of recoverable key systems. They allowed export of 64-bit key systems if the keys were escrowed with government-approved key agents, or 56-bit key systems if the exporter made satisfactory commitments to build or market recoverable key systems. Through 1997 and 1998, exemptions were extended to specific market sectors. It began with exemptions for US companies engaged in banking and financial services, and, in September 1998, was extended to certain exports in the financial, health, medical and electronic commerce sectors.

**The latest US policy**

In its announcement of 16 September 1999, the White House claims to be introducing a new policy that continues to maintain the balance between three competing needs:

- strong protection of sensitive electronic data;
- controlling the export of encryption products in the interests of security; and
- enabling law enforcement authorities to decrypt messages in certain circumstances to protect the public.

Later changes in 1995 and 1996 were designed to further encourage the development of recoverable key systems. They allowed export of 64-bit key systems if the keys were escrowed with government-approved key agents, or 56-bit key systems if the exporter made satisfactory commitments to build or market recoverable key systems. Through 1997 and 1998, exemptions were extended to specific market sectors. It began with exemptions for US companies engaged in banking and financial services, and, in September 1998, was extended to certain exports in the financial, health, medical and electronic commerce sectors.

**The proposed Cyberspace Electronic Security Act (CESA)**

The Clinton administration proposes an Act clarifying and strengthening the hand of law enforcement agencies to decrypt communications. According to the White House press release, “… [the new Act] would:

- Ensure that law enforcement maintains its ability to access decryption information stored with third parties, while protecting such information from inappropriate release.
- Authorize $80 million over four years for the FBI’s Technical Support Center, which will serve as a centralized technical resource for Federal, State, and local law enforcement in responding to the increasing use of encryption by criminals.
- Protect sensitive investigative techniques and industry trade secrets from unnecessary disclosure in litigation or criminal trials involving encryption, consistent with fully protecting defendants’ rights to a fair trial.”
A sixth advantage is the digital time stamp, which will attest that a document was in existence at a particular time. Other services, such as Surety's Digital Notary Service, already offer similar security through the use of cryptographic functions called "one-way hash functions", "message digest functions" or "digital fingerprint functions".

Finally, the ICC proposal addresses problems associated with a loss of collateral information in electronic transactions. Such information is typically inessential to a transaction but provides useful context and often enhances confidence in barely perceptible ways, eg intuition tells me this person has a trustworthy face. So long as the parties retain trust in the ICC Repository or similar service, they will be more willing to deal despite a lack of familiar "trust signals".

Global Action Plan for Electronic Commerce

As mentioned, the ICC has a newly proposed business action plan, which was tabled at an OECD forum on e-commerce held on 12-14 October 1999. The Global Action Plan for Electronic Commerce is available on the ICC WebPage and was timed to stimulate discussion at the upcoming World Trade Organization (WTO) meeting in Seattle in November.

Other major contributors to the plan were:

- BIAC – Business and Industry Advisory Committee to the OECD (www.biac.org)
- GIIC – Forum for the Global Information Infrastructure (www.giic.org)
- INTUG – International Telecommunication Users Group (www.intug.net) and
- WITSA – World Information Technology and Services Alliance (www.witsta.org)

The plan canvasses a wide range of issues including standards, Internet names and numbers, consumer trust, electronic signatures, taxation and intellectual property.

2 CyberNotary Committee of the Electronic Commerce and Information Technology Division, Section of Science and Technology, of the American Bar Association. http://www.abanet.org/scitech/ec/cn/
3 http://www.surety.com/dns.html