Journal of Advances and Scholarly Researches in Allied Education

Vol. IV, Issue VIII, October-2012, ISSN 2230-7540

REVIEW ARTICLE

THE IMPACT OF OECD CRYPTOGRAPHY POLICY DATA SECURITY

www.ignited.in

Journal of Advances and Scholarly Researches in Allied Education
Vol. IV, Issue VIII, October-2012, ISSN 2230-7540

The Impact of OECD Cryptography Policy Data Security

Narata Ram[1] Dr. Surendra Kumar Gupta[2]

[1]Research Scholar, Singhania University, Rajasthan, India.

[2]Asst. Prof., Rajiv Gandhi College, India

----------♦----------

REVIEW ARTICLE

In 1997 OECD released Guidelines for Cryptography Policy. Within the OECD it was recognised early on that disparities in laws could create obstacles to the development of national and global information and communications networks. Cryptography is thought to be particularly valuable in fostering global electronic commerce. The OECD recommendation sets out eight principles that should be followed by member nations in establishing their own cryptography policies. OECD Guidelines are only" recommendations" - but because the OECD functions as a consensus forum for the most developed countries, the Guidelines are had a significant international impact. For example the Finnish and Swedish Governments have adopted cryptography policies pursuant to OECD's challenge to national governments to draft national cryptography policies. In fact, many nations have not stated their cryptography policies openly in the past. In the most egregious cases, business users learned the scope of a nation's policy only when the authorities appeared at their hotel or office to confiscate their ' unauthorized' communications equipment. If followed faithfully, this OECD recommendation will move regulation of cryptography out of the shadows and into the normal world of business regulation.

It must also be noted that at present all OECD countries, except Iceland and Mexico, are members of WA. Therefore OECD Guidelines have probably influenced somehow respective national policies, which national governments assert inter alia in WA-related negotiations.

Guidelines are aimed primarily at governments, though with the expectation that they will be widely read and followed in the private sector as well. The document states that all eight principles are interdependent and should be implemented as a whole. It calls for a 'balance' among the interests at stake, but it provides no further guidance to policymakers, who will understandably feel that the various principles often look in quite contradictory directions. In the end, then, the Guidelines and the integration section can best be seen as creating a series of policy objectives, all of which must be given some gravitational force. Perhaps one can best imagine the principles as fixed points, to which may be attached elastic bands of varying strengths. If all Report on Background and Issues of Cryptography Policy, Chapter IV, National Level Activities. Of the bands are joined, the point at which they come to equilibrium will vary depending on the strength of each band. But it is impermissible to give no weight at all to any one of the principles (with the possible exception of the lawful access principle). In the Guidelines it is also stated that they are to be reviewed at least every five years.

Very interesting and significant was the inclusion of a specific recommendation that members avoid policies that create unjustified obstacles to trade and to the development of networks:

INTERNATIONAL CO-OPERATION

Governments Should Co-Operate To Co-Ordinate Cryptography Policies. As Part Of This Effort, Governments Should Remove, Or Avoid Creating In The Name Of Cryptography Policy, Unjustified Obstacles To Trade.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for inter- national use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.

This language is similar to injunctions contained in WTO agreements. By placing this recommendation on an equal footing with the recommendation that nations adopt the Guidelines, OECD made avoidance of unjustified obstacles to trade an overarching recommendation that is both independent of the Guidelines and a lodestar for interpreting and applying all aspects of the Guidelines. Governments are to co-operate in order to avoid unjustified obstacles to global trade, and even to remove existing obstacles created by cryptography policy if they cannot be justified.

This principle obviously begs the question of how such obstacles can be justified. The language is borrowed from international trade law, where what is unjustified has been defined by usage. The most likely interpretation in this context is that cryptography policy should not be used as a pretext to exclude or discriminate against foreign products. It is not intended to override national security or law enforcement policies if applied in good faith, and it clearly does not prohibit Wassenaar export controls, since several major OECD members maintained such controls on cryptography when the Guidelines were adopted. On the other hand there is a world of difference between "unjustified" and "unjustifiable" obstacles.

The text states further that nations should not impede the free flow of encrypted data passing across their national territory merely on the basis of cryptography policy. This principle is borrowed from a strong ITU rule against actions that impede the flow of international communications across the territory of a member State. This policy against impeding the flow of encrypted data is limited to data transiting a particular country. That is, when encrypted data crosses country A on its way from country B to country C, the cooperation principle calls on country A not to impede the flow of data between B and C.

REFERENCES:-

1. Baker-Hurst p. 70.

2. Baker-Hurst p. 49: ”The Guidelines do not apply to cryptography that protects military and diplomatic information. Precise scope of this exception is difficult to measure, because different nations treat different kinds of information as”classified” or otherwise protected”

3. Berg p. 80. The Guidelines are not legally binding on its member countries.

4. Governments are to:” state clearly and make publicly available” any national controls on cryptography. See Principle 8 of the OECD Guidelines for Cryptography Policy, subparagraph 1, 2nd sentence and OECD Adopts Guidelines for Cryptography Policy.

5. Baker 1997.

6. Principle 8 of the OECD Guidelines for Cryptography Policy, sub paragraph 4.

7. Baker 1997. Lawful access principle covers situations where national authorities can have access to plaintext in- formation.

8. OECD Guidelines for Cryptography Policy p. 7.

9. Baker-Hurst p. 47.

10. Baker-Hurst p. 69.