*Journal of Advances and Scholarly Researches in Allied Education*

*Vol. IV, Issue VII, July-2012, ISSN 2230-7540*

REVIEW ARTICLE

# LEGAL ISSUES RAISED BY THE DEMOCRATIZATION OF CRYPTOGRAPHY

www.ignited.in

*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. IV, Issue VII, July-2012, ISSN 2230-7540*

# Legal Issues Raised by the Democratization of Cryptography

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

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

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

----------♦----------

Export controls imposed on cryptographic software affect the possibilities of individuals and companies of lawfully obtaining cryptographic software, in order to protect themselves against breaches of security. On the other hand, export control regimes constantly face new challenges from non- lawabiding people, who seek to discover new ways and means to circumvent controls. The inherently global nature of information and communication networks makes the task of export control enforcement quite difficult and the difficulties of defining and enforcing jurisdictional boundaries in the international environment become more and more evident.

In order to properly understand the field of cryptography, one must bear in mind that there are three main reasons why a person might want to use cryptography. These are to ensure the confidentiality of data, authenticate data, and to ensure its integrity. Cryptography is used to protect inter alia information and communications systems. Also digital signatures are based on encryption algorithms. The importance of information and communications systems for society and the global economy is intensifying with the increasing value and quantity of data that is trans-mitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorised access and use, misappropriation, alteration, and destruction.

The confidentiality of information that cryptography can provide is useful not only for the legitimate purposes of preventing information crimes (e.g. the theft of trade secrets or unauthorized disclosure of sensitive medical records) but also for illegitimate purposes (e.g., shielding from law enforcement officials a conversation between two terrorists planning to bomb a building). Although strong automatic encryption implemented as an integral part of data processing and communications provides confidentiality for 'good guys' against 'bad guys' (e.g. business protecting information against economic intelligence efforts of foreign nations), it unfortunately also protects 'bad guys' against 'good guys' (e.g. terrorists evading law enforcement agencies). Under appropriate legal authorization law enforcement authorities may gain access to 'bad guy' information for the purpose of investigating and prosecuting criminal activity. Similarly intelligence gathering for national security and foreign policy purposes depends on having access to information of foreign governments and other foreign entities. Because such activities benefit society as a whole (e.g. by limiting organized crime and terrorist activities), 'bad guy' use of cryptography used for confidentiality poses a problem for society as a whole, not just for law enforcement.

Considered in these terms, it is clear that the development and widespread deployment of cryptography that can be used to deny government access to information represents a challenge to the balance of power between the government and the individual. Historically all governments, under circumstances that further the common good, have asserted the right to compromise the privacy of individuals, e.g. through opening mail, tapping telephone calls, inspecting bank records. Unbreakable cryptography for confidentiality provides the individual with the ability to frustrate assertions of that right.

Export controls imposed on cryptography have generated considerable controversy. Export controls on cryptography have been controversial because they pit the interests of vendors and multinational corporations against the needs of State security. Two members of the Finnish Parliament crystallized the problems of the "cryptography controversy", clearly and in a down-to- earth way, in their parliamentary question, debating Finland's decision to join the WA:

"Popularly encryption technology can be compared to a lock, it is a method to lock information so, that trespassers cannot access it without a key. Maybe in the past, locks were only in the door of the king's treasury, but can you imagine that modern society could be safe without locks protecting the doors of homes and establishments? So not only doors of WMD -factories need locks. Nowadays we use encryption technology every day in bank cards, in

GSM-telephones, in Internet bank connections and so on. Encryption technology also plays a more and more important part in so-called embedded systems, in other words in those computers which control all kinds of equipment and institutions, like factories, power plants, access control systems, telephone networks and power grids. More and more often also the control of embedded systems is handled over open information network. If information moves unencrypted or weakly encrypted, it would be like the doors of those establishments which would be unlocked. Any given hostile party could destroy or paralyze in an instant this nation's vi- tally important infrastructure."

Encryption functions can be both hardware and software based. Usually the same rules apply to hardware and software, because in Wassenaar Arrangement, which is the principal foundation to all encryption software export control regimes around the world, controlled information security products are controlled or relaxed from controls principally on the basis of the method used. It can also be, in some situations, quite difficult to judge whether some high technology item is software or hardware or a combination of both, because both are used hand in hand in computational processes. One must also bear in mind that this dichotomy is inherently not a legal but technical problem, and should be discussed elsewhere. Of course one cannot forget that in the highly specialized legal field of encryption software export controls, technical and legal expertise is closely linked together. Categorically this marriage of jurisprudence and technical expertise is commonplace in the domain of cyber law or jurisprudence linked to emerging technologies.

## 1.2 THE ROLE OF EXPORT CONTROLS

Internationally, export controls are the strongest tool used by governments to limit development of encryption products. Export controls on cryptography and related technical data have been a pillar of cryptography policy for many years. Increasingly, they have generated controversy because they pit the needs of national security to conduct signals intelligence against the information security needs of legitimate businesses and the markets of manufacturers whose products might meet these needs. Export controls reduce the availability of encryption in common programs such as operating systems, electronic mail and word processors. The restrictions make it difficult to develop international standards for encryption and interoperability of different programs. Countries must develop their own local programs, which do not interoperate well (if at all) with other programs developed independently in other countries. They may not be as secure because of a lack of peer review. Because markets are smaller, companies and individuals are not as interested in developing programs because of smaller potential profits. In some Wassenaar member countries export controls are used as a justification to limit the availability of encryption on domestic Internet sites and thus serve as indirect domestic controls on encryption.

Some countries have taken advantage of the situation by promoting the lack of controls in their countries. One result of this has been the emergence of small companies, in many countries without restrictions, which produce encryption products. Another result has been companies moving their encryption production divisions overseas to countries with fewer controls, such as Switzerland or Anguilla, a British self-governing territory in the Caribbean. Switzerland officials have stated according to Cryptography and Liberty 1999 : "Switzerland will keep its efficient export permit process for cryptographic goods in order to encourage Swiss exports to increase their sales and share worldwide while being mindful of national security interests." Although Switzerland is member of WA, it is pursuing very liberal crypto policy, under full compliance with its provisions. It must be recognized that all the other WA –countries also had their national economic interests in mind when they joined it. Had they deemed it detrimental to their national interests they probably would not have joined.

The Internet has changed significantly the effectiveness of export controls. Strong, unbreakable encryption programs can instantly be delivered anywhere in the world. It is increasingly difficult for countries to limit digital dissemination, and once a program is released, it is nearly im- possible to stop its dissemination, especially if it occurs in one of the many countries around the world with no export controls.

## 1.3 THE RATIONALE OF ENCRYPTION SOFTWARE EXPORT CONTROLS

The true ratio of export controls on cryptographic products is rather self-evident. It is not publicly stated anywhere in the Wassenaar Arrangement's official documents, but one can add one and one together after some time spent researching nature of the Arrangement. As stated in the Initial Elements, the WA is established in order to" prevent the acquisition of ... sensitive dual- use items for military end uses, if the situation in a region or the behaviour of a State is, or becomes, a cause for serious concern to the participating States."

In the case of crypto products, this means that those products should not be exported to a State, which is, or most likely will in the future be, an adversary of one or more participating States. An export restriction, presumably effectively enforced, will deny a potential adversary the capabilities to secure its military, diplomatic, other official and private sector communications.

This means that the adversary's military and civilian infrastructures are prone to effective SI- GINT efforts. Also industrial espionage, conducted by

private sector operatives, is easier if the subject does not use cryptography.

Laws governing privacy can conflict with laws on cryptography. For example, a law on data privacy may require that certain sensitive data associated with an individual be protected, while a law on cryptography may forbid the use of cryptography. Such laws would obviously conflict if a situation arose in which cryptography were the only feasible tool for protecting such data. In short, policies regarding data export, import, and privacy are an additional dimension of resolving policy with respect to cryptography. EC Data Protection Directive 95/46/EC require inter alia that personal information, such as medical records, should be adequately protected from outside intrusions. However, in the EU, strong crypto products are classified as sensitive, and at present also intra-Community transfers require a license. Therefore protection of personal information is made more difficult, because obtaining protective software or hardware is harder due to export control laws, namely EU Dual-Use Regulation 3381/94 EC. The export authorization procedure established by this EC regulation does not help European public or private entities which seek to acquire best products in order to fulfil the requirements of the Data Protection Directive.

It is important to keep in mind that the ultimate goal of export controls on cryptography is to keep strong cryptography out of the hands of potential targets of signals intelligence. Some WA participating States have very powerful SIGINT bodies, capable of eavesdropping large amounts of communication all over the world. Wide availability of strong unbreakable encryption means a threat to efforts of those intelligence gathering bodies. In small WA countries, like Finland, SIGINT capabilities are quite modest, and therefore interest in limiting the use of cryptography is smaller.

In Cryptography's Role in Securing the Information Society it was concluded that the U.S. ex- port control regime on cryptographic products was intended to serve two primary purposes. My understanding is that this can be applied also to WA export controls on cryptography mutatis mutandis, as far as WA's rationale is concerned:

- To delay the spread of strong cryptographic capabilities and the use of those capabilities throughout the world. Senior intelligence officials recognize that in the long run, the ability of intelligence agencies to engage in signals intelligence will inevitably diminish due to a variety of technological trends, including the greater use of cryptography."

- To give the U.S. government a tool for monitoring and influencing the commercial development of cryptography. Since any U.S. vendor that wishes to export a product with encryption capabilities for confidentiality must approach the U.S. government for permission to do so, the export license approval process is an opportunity for the U.S. government to learn in detail about the capabilities of such products. Moreover, the results of the license approval process have influenced the cryptography that is available on the international market."

Also the economic aspects cannot be forgotten, because export controls obviously have some effect on the exporters' market position. Especially the European Commission has been concerned about this. Differences between Member States' export controls may adversely affect the functioning of the Single European Market (SEM), by creating obstacles to free circulation of goods within the Community or in relation to non-Member countries. Differences can also lead to distortion of competition.

There are also underlying trade policy issues involved. At least for the time being there are so- me facts to be recognized. Export controls on cryptographic technologies have a negative effect on commercial interests. The global software business is dominated by U.S.-controlled corporations. They hold the largest market shares. The majority of mass-market applications, for example, are created in the U.S. Another fact is that the U.S. has a very large domestic marketplace for encryption software. For an EU software developer it is very important to be able to reach this market.

In the era of free trade and global marketplace, the U.S. Government simply cannot, and probably would not even want to be so protective that it would impose import controls in order to protect US companies. Import restrictions have not even been contemplated in the U.S. or el sew here, with a few minor exceptions. Therefore, for an EU software developer exporting to the U.S. the only legal obstacles that remain are the export licensing procedures imposed under the EU's or Member States' legal systems. These export regimes can decide the business success right from the start. Too bureaucratic or cumbersome regimes may halt the exports to- tally to the U.S. and elsewhere. Reseach indicates that at present regimes are not that bureaucratic in the EU region, and if the liberalization and harmonization trend continues in the EU, there is no great cause for concern for European software developer. Finally, although export controls may have significant economic effects, they have not been constructed to enhance fo- reign trade, but to enforce nations' security and foreign policy interests. Therefore export controls will remain an obstacle to free trade, although a formally legitimate one.

**REFERENCES:-**


1. Baker 1997, chapter 'Background' para 5. However, the use of cryptography falls beyond the scope of this study.

2. The term was invented by Bert-Jaap Koops PhD, University of Tillburg, Netherlands scholar, whose PhD -thesis covers cryptography policy issues. See Koops 2000.

3. KK 1445/1998 vp.The concept of firmware makes things even more complicated.

4. Cryptography's Role in Securing the Information Society, chapter 4 paragraph 1.

5. See Cryptography and Liberty 1999 for further details. Domestic controls are not examined in this thesis.

6. Baker-Hurst:"... many companies in the United States are considering ways to avoid U.S. controls legally. Some ... have announced relationships with foreign entities that develop encryption and plan to incorporate this encryption into their product line." In U.S. export controls are allegedly even stricter than in the EU region.

7. There are no cryptography export controls in Anguilla. Cryptography and Liberty 1999.

8. Initial Elements I.3.

9. This aspect of export controls was also recognized in European Commission Communication, COM (97) 503, in chapter 2.1. paragraph 1.

10. Cryptanalysis for inter alia SIGINT purposes is also a part of the techniques of possible information warfare,

11. Tietoturvallisuus ja laki, p. 86.

12. Cryptography's Role in Securing the Information Society , Appendix G.3. See also chapter 4.

13. Cryptography's Role in Securing the Information Society chapter 4.2.

14. Largest of them is the U.S. NSA, which has had historically very close cooperation with its British counterpart GCHQ, Interception Capabilities 2000. Russians have similar SIGINT agency called FAPSI.

15. Cryptography's Role in Securing the Information Society , chapter 4.1.1.

16. COM (97) 503 2.1.

17. Of EU Member States only France has limited import controls. See chapter 5.4 covering France.

18. Of course one must comply with possible customs and other laws, national or EC based, but those problems fall beyond the scope of this study.

19. KK 1430/1998 vp.