URN:NBN:fi-fe20001230

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta/Osasto – Fakultet/Sektion – Faculty/Section	Laitos – Institution – Department
Faculty of Law	Department of Public Law

Tekijä – Författare – Author

Parviainen, Simo-Pekka

Työn nimi – Arbetets titel – Title

Cryptographic Software Export Controls in the EU

Oppiaine – Läroämne – Subject

Administrative Law

Työn laji – Arbetets art – Level	Aika – Datum – Date	Sivumäärä – Sidoantal – Number of Pages
Pro-gradu thesis	1. 7.2000	89 pages

Tiivistelmä – Referat – Abstract

Certain software products employing digital techniques for encryption of data are subject to export controls in the EU Member States pursuant to Community law and relevant laws in the Member States. These controls are agreed globally in the framework of the so-called Wassenaar Arrangement. Wassenaar is an informal non-proliferation regime aimed at promoting international stability and responsibility in transfers of strategic (dual-use) products and technology. This thesis covers provisions of Wassenaar, Community export control laws and export control laws of Finland, Sweden, Germany, France and United Kingdom.

This thesis consists of five chapters. The first chapter discusses the *ratio* of export control laws and the impact they have on global trade. The *ratio* is originally defence-related – in general to prevent potential adversaries of participating States from having the same tools, and in particular in the case of cryptographic software to enable signals intelligence efforts. Increasingly as the use of cryptography in a civilian context has mushroomed, export restrictions can have negative effects on civilian trade. Information security solutions may also be took weak because of export restrictions on cryptography.

The second chapter covers the OECD's Cryptography Policy, which had a significant effect on its member nations' national cryptography policies and legislation. The OECD is a significant organization, because it acts as a meeting forum for most important industrialized nations.

The third chapter covers the Wassenaar Arrangement. The Arrangement is covered from the viewpoint of international law and politics. The Wassenaar control list provisions affecting cryptographic software transfers are also covered in detail. Control lists in the EU and in Member States are usually directly copied from Wassenaar control lists. Controls agreed in its framework set only a minimum level for participating States. However, Wassenaar countries can adopt stricter controls.

The fourth chapter covers Community export control law. Export controls are viewed in Community law as falling within the domain of Common Commercial Policy pursuant to Article 133 of the EC Treaty. Therefore the Community has exclusive competence in export matters, save where a national measure is authorized by the Community or falls under foreign or security policy derogations established in Community law. The Member States still have a considerable amount of power in the domain of Common Foreign and Security Policy. They are able to maintain national export controls because export control laws are not fully harmonized. This can also have possible detrimental effects on the functioning of internal market and common export policies. In 1995 the EU adopted Dual-Use Regulation 3381/94/EC, which sets common rules for exports in Member States. Provisions of this regulation receive detailed coverage in this chapter.

The fifth chapter covers national legislation and export authorization practices in five different Member States – in Finland, Sweden, Germany, France and in United Kingdom. Export control laws of those Member States are covered when the national laws differ from the uniform approach of the Community's *acquis communautaire*.

Avainsanat – Nyckelord – Keywords

export control, encryption, software, dual-use, license, foreign trade, e-commerce, Internet

Säilytyspaikka – Förvaringställe – Where deposited

Faculty of Law Library

Muita tietoja – Övriga information – Additional information

Also available online at: http://ethesis.helsinki.fi or http://personal.inet.fi/business/parviainen/thesis.html in .pdf format, for other formats and information email author at Simo-Pekka Parviainen <spp@iki.fi>.

PREFACE

> *"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files."*[1]

Encryption technology regulation may seem, at first glance, as quite a narrow topic in the family of jurisprudence.[2] It may still be so, but one thing is for certain - it is relatively unexplored among legal scholars. Needless to say, this makes the task of the humble law student quite challenging.

Since the triumphant rise of the Information Society, use and distribution of encryption software has been a hot topic in policy discussions. Still classified as a dual-use commodity, governments in major industrial nations want to limit its use, using their export control regimes as an enforcement tool. It seems that the only thing for certain in this field is change – export control regimes are in a state of flux.

Obviously one can see certain trends in the field concerned. One big trend in recent years has been liberalization. Especially in the United States and France governments have been cutting some slack in controls. On the other hand, in those nations especially the export controls have been quite strict in comparison to other industrialized nations. But one trend in the international policy arena has also been quite clear – national governments' willingness to maintain their regimes as intact as possible in spite of liberalization. One must also bear in mind that there are strongly legitimate grounds for maintaining export controls on dual-use goods especially in cases of non-proliferation and trade embargoes. Still one can argue that encryption is defensive in its true nature, used to protect the information from unauthorised access, and cannot be directly used for hostile purposes. Therefore it should not be deemed a dual-use product at all. The future will show us which trend will prevail.

However, the rapid development of technology may render the controls obsolete and the laws may suffer the faith of *desuetudo*. It may well be that controls on encryption products will be abolished in the near future. In my opinion, we can be relatively sure about one thing - governments and intergovernmental organizations are adapting their approach, as they face the new challenges provided by the new information technologies. In the field of export controls this

[1] *Bruce Schneier*; Applied Cryptography: Protocols, Algorithms, and Source Code in C.
[2] Words 'encryption' and 'cryptography' derive from Greek word *kryptikós* (hidden).

means that governments are moving from a gatekeeper model to a surveillance model, [3] because they are unable or unwilling to control certain dual-use exports.

Also it can be considered that when some product is classified as a dual-use product (a strategic product or technology - an item which can be used for both civil and military purposes), it can be used as a part of a weapon or in the manufacturing of weapons. Still almost any item can be used as a weapon if one has the intention, and therefore almost any item could also be classified as a dual-use item. Therefore the whole concept of dual-use products is somewhat problematic and should be used only for products which are mainly used in defence-related fields and only rarely in a civilian setting.

As a general academic remark I should also point out, that this is a legal study in a field filled with myriad technical details. The technical details, however, are beyond the scope of this study.

Finally I would like to thank Jari Puhakka, Päivi Hautamäki, Jari Holmborg and Mikko Maijala, all from the F-Secure Corporation, for giving me the opportunity to do research work for F-Secure Corp. Thank you very much for having confidence in me and my work. Also, I would like to thank Ms Jane Keates M.Sc. for giving me lifesaving guidance in English grammar.

Helsinki, Finland 1. 7.2000

Simo-Pekka Parviainen

[3] *Rotenberg, Marc*, Executive Director of the Electronic Privacy Information Center, interviewed in the New York Times, January 18, 2000.