CONTENTS

PREFACE ..... **III**

CONTENTS ..... **V**

REFERENCES ..... **VIII**

REFERRED CASES ..... **XII**

GLOSSARY OF ABBREVIATIONS, ACRONYMS AND TERMS ..... **XIII**

1 INTRODUCTION **1**

1.1 The Problem – Legal Issues Raised by the Democratization of Cryptography 1

1.2 The Role of Export Controls 3

1.3 The Rationale of Encryption Software Export Controls 4

2 THE IMPACT OF OECD CRYPTOGRAPHY POLICY **7**

3 THE WASSENAAR ARRANGEMENT **10**

3.1 History of the WA – From COCOM to the Wassenaar Arrangement 10

3.2 The Legal Status of WA 11

3.3 The Aims of the Wassenaar Arrangement 13

3.4 Wassenaar Arrangement Co-operative Procedures Pursuant to Initial Elements 15

3.4.1 Participation, Meetings and Administration 15

3.4.2 Procedures for the Information Exchange 17

3.5 Relevant Provisions of Wassenaar Arrangement Affecting Encryption Software Transfers 19

3.5.1 Controlled Encryption Software Items and Related Technology According to WA-LIST Category 5 Part 2 ”Information Security” and GSN & GTN 20

3.5.1.1 Information Security Items relaxed from controls 21

3.5.1.1.1 General Software Note (GSN) 21

3.5.1.1.2 General Technology Note (GTN) 22

3.5.1.1.3 Items Relaxed Pursuant to Cryptography Note 23

3.5.1.1.4 Products Accompanying User for the User’s Personal Use 26

3.5.1.2 Controlled Software, Software in Systems, Equipment and Components, Software in Test, Inspection and Production Equipment and Controlled Software Technology 26

3.5.1.2.1 Symmetric Algorithms 27

3.5.1.2.2 Asymmetric Algorithms 28

3.5.1.2.2.1 Classical Asymmetric Systems 29

3.5.1.2.2.1.1 Discrete Logarithms (DLs) in a Multiplicative Group 29

3.5.1.2.2.1.2 Elliptic Curve Systems 29

3.5.1.2.3 Software Performing Cryptanalytic Functions 29

3.5.1.2.4 Software to Reduce Compromising Emanations of Information-Bearing Systems 30

3.5.1.2.5 Software for Spread Spectrum Systems Use 30

3.5.1.2.6 Software to Provide Multilevel Security 30
3.5.1.2.7 Software to Detect Surreptitious Intrusion in Communications Cable Systems 30
3.5.1.2.8 Software for Decryption in Global Navigation Satellite Systems Receiving Equipment 31
3.5.1.3 Exemptions from Control of Software, Software in Systems, Equipment and Components, Software in Test, Inspection and Production Equipment and Controlled Software Technology 31
3.5.1.3.1 Exemption for Cryptography Used for Certain Authentication or Digital Signature Functions 31
3.5.1.3.2 Restricted Audience Broadcast Equipment 31
3.5.1.3.3 Cryptographic Software Protecting IPR-rights 31
3.5.1.3.4 Banking Exemption 32
3.5.1.3.5 Exemption for Portable and Mobile Radiophones 33
3.5.1.3.6 Cordless Telephony Exemption 34
3.5.1.3.7 Exemption for Certain Personalized Smart Cards 34
3.5.2 The Dichotomy – Tangible and Intangible Transfers 34
3.5.3 Some Final Conclusions 36

4 EXPORT CONTROL LAWS IN THE EUROPEAN UNION 38

4.1 Introduction into the Community's Legal Activity in the Domain of Export Controls 38
4.2 Wassenaar Arrangement from the European Union Perspective 38
4.3 Relevant Acquis Communautaire 40
4.3.1 European Community's Common Commercial Policy 40
4.3.1.1 Interpretation of Article 1 of the Export Regulation 2603/69 43
4.3.2 Member State's Possibility to Derogate from Common Commercial Policy 46
4.3.2.1 Article 11 of the Export Regulation 2603/69 46
4.3.2.1.1 Similarities Between Article 30 EC and Article 11 of the Export Regulation 48
4.3.2.2 The Concept of Public Security Under Community Law 50
4.3.2.3 Proportionality Principle Considerations 53
4.3.2.4 Applicability of Articles 296 and 297 EC 57
4.4 Export Control Regime in the Community 59
4.4.1 Some Remarks on Interpretation of Dual-Use Regulation 59
4.4.2 Controlled Encryption Software 62
4.4.3 Transfers Inside Community Boundaries 63
4.4.4 Controls of Items Not Listed in DUD 64
4.4.5 Types of Authorizations When Exporting Outside the Community 66
4.4.5.1 Types of Simplified Procedures 66
4.4.5.1.1 General Authorization 66
4.4.5.1.2 Global Authorization 67
4.4.5.1.3 Simplified Procedures 67

4.4.5.1.4 End Use and Re-Export Statements and Other Requirements and Conditions for Export 68
4.4.6 The Validity of Export Authorizations 69
4.4.7 Some General Remarks About Export Authorization Procedure 69
4.4.8 Exporter's Duties Under DUR 71
4.4.9 A Member State's Right to Stop a Dual-Use Item Transfer Already Authorized in Another Member State 72
4.5 Common Foreign and Security Policy Considerations 73

5 EXPORT CONTROLS IN SOME RELEVANT EU MEMBER STATES 75

5.1 Finland 76
5.1.1 Overview 76
5.1.2 Export Control Procedure 76
5.1.3 MTI's Garden Variety Licensing Practices When Exporting Cryptographic Software 78
5.2 Sweden 79
5.2.1 Relevant Legislation and National Export Control Authority 79
5.2.2 Export Control Procedure 79
5.2.3 Licensing Practices Concerning Cryptographic Software 81
5.3 Germany 82
5.3.1 National Authority and Relevant Legislation 82
5.3.2 Export Authorization Procedure 83
5.4 France 86
5.4.1 Overview 86
5.4.2 Export Licensing Procedures 87
5.5 United Kingdom 87
5.5.1 National Authority and Relevant Legislation 87
5.5.2 Authorization Procedure 88

APPENDIX 1: Relevant Portions of the WA-LIST