

INFORMATION TECHNOLOGY

& The Law

SECOND EDITION

EDITORS: Chris Edwards, Nigel Savage and Ian Walden

- Information Technology and the Law
- An Introduction to the Legal Liabilities of Information Producers
- Negotiation, Performance and Enforcement of Contracts
- Software Protection
 - Data Privacy: the UK Experience
 - Transborder Data Flows
- Facilities Management and Other Computer Services Contracts
- Computer-Related Crime
 - Telecommunications
- Legal Issues of Employing Computer Personnel
 - Computing Insurance
 - EDI and the Law
 - EEC Law and the Information Technology Industry
 - Data Security

**INFORMATION
TECHNOLOGY**

*&
The Law*

SECOND EDITION

INFORMATION TECHNOLOGY

& The Law

SECOND EDITION

EDITORS: Chris Edwards, Nigel Savage and Ian Walden



M

© Chris Edwards and Nigel Savage, 1986
Chris Edwards, Nigel Savage, Ian Walden, 1990
Softcover reprint of the hardcover 2nd edition 1990

All rights reserved. No part of this publication
may be reproduced, or transmitted, in any form
or by any means, without permission.

Second edition published in the United Kingdom by
MACMILLAN PUBLISHERS LTD, 1990

British Library Cataloguing in Publication Data

Information technology & the law. Second edition
1. Computers – Law and legislation
I. Edwards, Chris, 1947- 2. Savage, Nigel
3. Walden, Ian.
342.64 K564.C6

ISBN 978-1-349-11770-3 ISBN 978-1-349-11768-0 (eBook)
DOI 10.1007/978-1-349-11768-0

Contents

Contributors xvii

1 Information Technology and the Law 1

- 1.1 What is Information Technology? 1
- 1.2 What is the History of Information Systems in Organisations? 1
- 1.3 What is the Direction for Tomorrow? 2
- 1.4 Can the Law Cope? 2
- 1.5 Role of This Book 3

2 An Introduction to the Legal Liabilities of Information Producers 4

- 2.1 What Kinds of Liability can Software Producers Incur? 4
- 2.2 Contractual Liability 6
- 2.3 Goods and Services Contrasted 6
- 2.4 Conditions, Warranties and Other Terms 8
- 2.5 Misrepresentation 9
- 2.6 Restraint of Trade 9
- 2.7 Restrictive Trade Practices Act 1976: Registrable Restrictions 10
- 2.8 Contractual Liability and Limitation 11
- 2.9 Breach and Repudiation 12
- 2.10 Termination without Breach 12
- 2.11 Damages for Breach 13
- 2.12 Limitation of Liability 14
- 2.13 Negligence and Product Liability 15
- 2.14 The Principles of Negligence 15
- 2.15 Economic Loss 15
- 2.16 Negligent Mis-Statement 16
- 2.17 Negligence and Software 16
- 2.18 Strict Liability for Defective Products 17
- 2.19 Recoverable Damage for Product Liability 17
- 2.20 Liability for Copyright Infringement 18
- 2.21 Confidence-related Liability 19
- 2.22 Patents 19
- 2.23 Trade Marks and Service Marks 20
- 2.24 Measure of Damages 20

- 2.25 Delivery-up in Copyright 20
- 2.26 Injunctions 21
- 2.27 Suppliers' Liabilities for Intellectual Property Infringement 21
- 2.28 Other Forms of Liability 22
- 2.29 Conclusions 23

3 Negotiation, Performance and Enforcement of Contracts 24

- 3.1 What are the important factors in respect of contracts for the supply of equipment? 24
 - 3.1.1 Contracts of Sale 25
 - 3.1.2 What Are The Important Factors In Hiring Or Leasing? 30
- 3.2 What are the important factors in respect of contracts for the supply of proprietary programs? 32
 - 3.2.1 Licence Or Sale? 32
 - 3.2.2 The Licence Grant 33
 - 3.2.3 Enhancements And Modifications 34
 - 3.2.4 Services 35
 - 3.2.5 Software Warranties 35
 - 3.2.6 Intellectual Property Rights In Programs 36
- 3.3 What are the important factors in respect to contracts for developing bespoke programs? 37
 - 3.3.1 Introduction 37
 - 3.3.2 Specifying The Work 38
 - 3.3.3 Ownership Of Copyright 39
 - 3.3.4 Change Control 41
 - 3.3.5 Remedies For Default 41
- 3.4 What type of maintenance contracts should I have? 42
 - 3.4.1 Equipment Maintenance Service 42
 - 3.4.2 Total Systems Maintenance 44
- 3.5 What other issues should I be concerned with? 45
 - 3.5.1 Liquidated Damages 45
 - 3.5.2 Prohibition Against Exporting 46
 - 3.5.3 Time and Materials Contracts 46

4 Software Protection 47

- 4.1 How can software be protected legally? 47
- 4.2 Why does software need protection? 47
- 4.3 Does contract protect software? 48
- 4.4 Does Patent Law protect software? 48
 - 4.4.1 Patents at the European Patent Office 48
 - 4.4.2 Patents in the UK 50

4.5	Does copyright protect software?	51
4.5.1	Outline Of Copyright – General Principles	51
4.5.2	Restricted Acts And Infringements	52
4.5.3	Remedies For Infringement	53
4.5.4	Copyright And Software in the UK	54
4.5.5	Maximising Copyright Protection	58
4.5.6	Copyright Marking	59
4.5.7	Computer Storage Of Copyright Works	60
4.5.8	Cassette, Disk And Chip Based Software And Network Systems	60
4.5.9	International Protection	61
4.5.10	Copyright Protection Of Computer Programs International Review	61
4.5.11	A Proposal for a Council Directive on the Legal Protection of Computer Programs	64
4.6	Does the law of trade secret and confidential information offer protection?	64
4.7	Protection by Trade Marks	65
4.8	Protection for semi-conductor chips	65
4.8.1	United States of America	66
4.8.2	Protection For Semiconductor Products In The UK	66

5 Data Privacy: the UK Experience 70

5.1	Why was the Data Protection Act necessary?	70
5.2	What are the basic principles underlying the Act?	72
5.3	Who does the legislation affect?	74
5.4	What types of data are regulated under the legislation?	78
5.5	What is the scope of the exemptions?	83
5.6	Are any payroll and accounting systems exempt?	84
5.7	Are mailing lists exempt?	87
5.8	Are research and statistical data exempt?	88
5.9	Is data connected with crime prevention or tax evasion?	89
5.10	What is the health and social work data exemption?	90
5.11	What other exemptions are there?	90
5.12	How do we register?	93
5.13	How do we complete the application form?	94
5.14	How should our automated office systems be registered?	95
5.15	How should groups be registered?	96
5.16	Can I alter my registration?	96
5.17	What happens if my registration is refused?	97
5.18	Why should I bother to register at all?	97
5.19	What happens if I do not keep my registration up-to-date?	98
5.20	Can the Registrar enter premises and seize my disks, etc?	98
5.21	What can the Registrar do to make us comply with the Act?	99
5.22	Do I have a right of appeal against the Registrar?	104

- 5.23 What rights are introduced for data subjects? 105
- 5.24 How do I comply with the access rights? 105
- 5.25 When can compensation be claimed under the Act? 108
- 5.26 Can inaccurate data be corrected? 111
- 5.27 Can individuals complain to the Registrar? 112
- 5.28 What should we be doing within the Organisation to ensure compliance with the Act? 113
- 5.29 What is the future for the Data Protection Act 1984? 120

6 Transborder Data Flows 121

- 6.1 What are Transborder Data Flows? 121
- 6.2 What types of data are transferred across national borders? 121
- 6.3 Why regulate transborder data flows? 122
- 6.4 How do countries regulate transborder data flows? 124
- 6.5 What international initiatives and developments deal with TDF? 126
- 6.6 How do companies perceive the threat of TDF restrictions, and avoid it? 127
- 6.7 Do restrictions on transborder data flows pose a real treat to trade? 128

7 Facilities Management and Other Computer Services Contracts 130

- 7.1 What is Facilities Management? 130
- 7.2 What is the relationship between FM and Computer Bureaux? 130
- 7.3 What provisions should be incorporated in FM contracts? 131
 - 7.3.1 What structure should be adopted? 131
 - 7.3.2 What aspects of the Implementation Phase should be addressed? 132
 - 7.3.3 System 132
 - 7.3.4 Employees 133
 - 7.3.5 What aspects of the Operation Phase should be addressed? 133
 - 7.3.6 Services and Standards 133
 - 7.3.7 Disaster Recovery 134
 - 7.3.8 Charges 134
 - 7.3.9 User's Obligations 134
 - 7.3.10 Security of Data 135
 - 7.3.11 Change and Development 135
 - 7.3.12 Disputes 136
 - 7.3.13 Non-competition 136
 - 7.3.14 Remedies and Liability 136
 - 7.3.15 What aspects of the Termination Phase should be addressed? 138
 - 7.3.16 Duration and Termination 138
 - 7.3.17 Transfer of data 138

- 7.3.18 Transfer of hardware 139
- 7.3.19 Transfer of agreements 139
- 7.3.20 Non-Poaching 139
- 7.4 How are computer bureaux affected by the Data Protection Act 1984? 139
 - 7.4.1 Is the Bureau Also a Data User? 139
 - 7.4.2 How Does the Position of a Computer Bureau Differ from that of a Data User? 140
 - 7.4.3 What if a Computer Bureau processes data abroad? 140
 - 7.4.4 What are the Obligations of a Computer Bureau? 140
 - 7.4.5 What constitute 'appropriate security measures'? 141
 - 7.4.6 Are there any Provisions Specific to Computer Bureaux? 141
 - 7.4.7 What Criminal Offences can a Computer Bureaux be Liable for? 141
 - 7.4.8 What is the Liability of a Computer Bureaux to Data Subjects? 141

8 Computer-Related Crime 142

- 8.1 What is Computer Related Crime? 142
 - 8.1.1 Review 142
 - 8.1.2 Peripheral Crimes 142
 - 8.1.3 Computer-Assisted Fraud 143
 - 8.1.4 Computer-Based Crime 144
 - 8.1.5 Other Computer-Related Offences 144
 - 8.1.6 Are All Computer-Related Crimes Offences Under UK Criminal Law? 145
- 8.2 How extensive is computer related crime? 145
 - 8.2.1 Overview 145
 - 8.2.2 Survey 147
- 8.3 Who are the offenders? 148
 - 8.3.1 Research 148
- 8.4 What offences are committed in computer-related crimes? 149
 - 8.4.1 Overview 149
 - 8.4.2 Theft of Information 150
 - 8.4.3 Computer Misuse 151
 - 8.4.4 Eavesdropping 152
 - 8.4.5 Copyright Infringement 152
 - 8.4.6 Alternative Charges 152
- 8.5 Are Companies concerned at the level of computer fraud? 153
- 8.6 What areas of computer operations are most at risk from fraud? 153
 - 8.6.1 Input 153
 - 8.6.2 Output 154
 - 8.6.3 Misuse of Resources 154
 - 8.6.4 Programs And Data Bases 155
 - 8.6.5 A case in detail 156

- 8.6.6 The Skill of the Offender 157
- 8.7 What are the penalties for computer-related crime? 157
- 8.8 How can computer-related crime be prevented? 160
 - 8.8.1 Prevention Or Deterrence? 160
 - 8.8.2 Management Policies 161
 - 8.8.3 Personnel Policies 161
 - 8.8.4 Internal Controls 161
 - 8.8.5 Physical Access Controls 164
 - 8.8.6 Software Controls 164
 - 8.8.7 Data Communications Controls 164
- 8.9 What is the role of the Auditor in suppressing computer-related fraud? 165
 - 8.9.1 Introduction 165
 - 8.9.2 External Audits 165
 - 8.9.3 Internal Audits 166
 - 8.9.4 Computer Audits 167
- 8.10 How is computer-related crime detected? 168
 - 8.10.1 Overview 168
 - 8.10.2 Fraud 168
- 8.11 Why is prosecuting computer-related crime so difficult? 170

9 Telecommunications 173

- 9.1 What is the Structure of UK and EEC Telecommunication Regulation 173
- 9.2 What is the UK Network Infrastructure 174
 - 9.2.1 Licensed Operators 174
 - 9.2.2 Duopoly Review 174
 - 9.2.3 Interconnection 174
 - 9.2.4 Code Powers 175
 - 9.2.5 Licence Terms 175
 - 9.2.6 Enforcement of Licence Conditions 176
 - 9.2.7 Changing Licence Conditions 176
- 9.3 What is "Resale" on private networks? 177
 - 9.3.1 Permitted services 177
 - 9.3.2 Licence Conditions in the new BSGL 178
- 9.4 Are Video Services Regulated? 178
- 9.5 Are Mobile and Radiopaging Services Regulated? 178
 - 9.5.1 Cellular Services 178
 - 9.5.2 Personal Communication Network ("PCN") Services 179
 - 9.5.3 Telepoint Services 179
 - 9.5.4 Nationwide Radiopaging Services 180
- 9.6 How are Specialised Satellite Services regulated? 180
- 9.7 What are Technical Approvals? 181

- 9.8 How are Contracts for services changing? 181
- 9.8.1 PTO Contracts 181
- 9.8.2 Managed Data Network Contracts 182
- 9.9 What are the Competition Law Issues? 182
- 9.10 What Regulations apply to Premium Rate Information and Entertainment Services? 183

10 Legal Issues of Employing Computer Personnel 184

- 10.1 Introduction 184
- 10.2 Who is an Employee? 185
- 10.3 Would a label make a difference? 188
- 10.4 Protection of Confidential Information 189
- 10.5 Protection through the implied duties 190
- 10.6 The duty not to disclose confidential information 192
- 10.7 Acting against the ex-employee 194
- 10.8 The use of express restraints 197
- 10.9 The Question of Reasonableness 199
- 10.10 Trade Connection Restraints 199
- 10.11 Trade Secret Restraints 201
- 10.12 Statutory Protection of Intellectual Property 203
- 10.13 Copyright, Designs and Patents Act 1988 204
- 10.14 Patents Act 1977 206
- 10.15 Changing the Employee's Terms 208
- 10.16 Looking after the Employees' Health and Safety 209
- 10.17 Does an Employer need to protect an Independent Contractor? 210

11 Computing Insurance 212

- 11.1 Cover for the IT User? 212
- 11.2 What are the risks in respect of Data and Software? 213
- 11.3 Failure of the Computing Function 214
 - 11.3.1 The Risk 214
 - 11.3.2 Typical Cover 214
- 11.4 Consequential Loss Cover in Detail? 215
 - 11.4.1 The Indemnity Period 215
 - 11.4.2 Consequences 217
 - 11.4.3 The Sums Insured 219
 - 11.4.4 The Excess 219
 - 11.4.5 The Premium 219
 - 11.4.6 Claims Conditions 220
 - 11.4.7 Conclusions 226
- 11.5 What Areas of Exposure are there in respect of computer crime? 221

- 11.5.1 Managing the New Risks 221
- 11.5.2 The Insurance Industry's Response 222
- 11.5.3 Third Party Computer Fraud 223
- 11.5.4 Computer-specific Fraud Covers 224
- 11.5.5 The American Approach 225
- 11.6 What Insurance cover is available for the IT Supplier? 226
 - 11.6.1 Product Liability 227
 - 11.6.2 Financial Loss insurance 227
 - 11.6.3 Product Guarantee Cover 227
 - 11.6.4 Fines, damages and penalty clauses 227
 - 11.6.5 Legal Costs and Expenses 228
 - 11.6.6 The Professional Indemnity Policy 228
 - 11.6.7 The Small Print 233
 - 11.6.8 Negotiating the Liability Jungle 234
- 11.7 What Liabilities arise under the Data Protection Act? 235
 - 11.7.1 Standard (Public/Product Liability) policies 235
 - 11.7.2 Commercial Legal Expenses 236
 - 11.7.3 Directors and Officers Liability 236
 - 11.7.4 Professional Indemnity 236
- 11.8 What are Uninsurable Risks? 237
- 11.9 What are The Limitations of Insurance? 237

12 EDI and the Law 239

- 12.1 What is EDI? 239
- 12.2 What legal problems does EDI raise? 240
- 12.3 How can EDI reduce the risks that generate legal disputes? 241
- 12.4 Interchange Agreements: What are we dealing with? 242
- 12.5 So what are the reasons for using an interchange agreement? 244
- 12.6 What is the nature of an interchange agreement? 244
- 12.7 What should be dealt with in an interchange agreement? 245
 - 12.7.1 Definitions and Scope 245
 - 12.7.2 Liability and Insurance 245
 - 12.7.3 Security, Confidentiality and Integrity 246
 - 12.7.4 Verification, Acknowledgement, Confirmation and Action 246
 - 12.7.5 Storage and Evidence 247
 - 12.7.6 Third Parties 248
 - 12.7.7 Dispute Resolution 248
 - 12.7.8 Miscellaneous 248
- 12.8 What contractual arrangements exist with the EDI service provider? 249
 - 12.8.1 Data Control and Ownership 249
 - 12.8.2 Confidentiality and Security 249
 - 12.8.3 Audit 250

12.8.4 Warranties, Liabilities and Remedies 250
 12.8.5 Internetwork Connections 251
 12.8.6 Termination 251
 12.9 Conclusion 252

13 EEC Law and the Information Technology Industry 253

13.1 Introduction 253
 13.2 Why is EEC law important to the Information Technology industries? 253
 13.3 Where is Competition Law found in the EEC Treaty? 254
 13.4 How Does Article 85(1) apply? 254
 13.4.1 Appreciability Test 256
 13.5 Is it possible to obtain Exemption from Article 85(1)? 256
 13.6 What types of agreement are commonly caught by Article 85(1)? 258
 13.7 Which Common Clauses infringe Article 85(1)? 258
 13.8 What types of common trading agreement are outside the scope of Article 85(1)? 260
 13.8.1 Selective distribution 260
 13.8.2 Intellectual Property 261
 13.8.3 Nungesser 262
 13.8.4 Coditel 263
 13.9 Article 86: What is a Dominant Position? 263
 13.10 What is an "abuse"? 265
 13.10.1 BT/Telespeed 265
 13.10.2 IBM 266
 13.10.3 Mergers 267
 13.11 What are the consequences of infringing Article 85(1) and Article 86? 268
 13.12 What are the Commission's Procedures for Exemption and Negative Clearance? 269
 13.13 Articles 30-36 of the EEC Treaty: The Free Movement of Goods 269
 13.14 How does Article 36 apply to protect intellectual property rights? 271
 13.14.1 Harmonisation of intellectual property laws. 272
 13.14.2 Trade Marks 272
 13.14.3 Patents 272
 13.14.4 Copyright 272
 13.14.5 Semi-conductors 273
 13.15 Article 59: The freedom to provide services across EEC Frontiers 273
 13.16 What Remedies are available for breach of Articles 30 and 59? 274
 13.17 How does the 1992 Legislation Relate to the Free Movement of Goods? 274

- 13.17.1 "New Approach" 275
- 13.17.2 Telecommunications 275
- 13.18 How is Public Procurement Governed by EEC law? 277
- 13.19 Public Procurement Legislation? 277
- 13.20 Anti-Dumping: What is "Dumping"? 279
- 13.21 Conclusions 280

14 Data Security 282

- 14.1 Why is Data Security currently of such concern to management? 282
- 14.2 What are the main sources of danger to data security? 285
- 14.3 What should be included in a data security policy? 285
- 14.4 What personnel policies are required for staff with access to sensitive data or facilities? 286
- 14.5 What personnel procedures for all staff should be reviewed in the light of data security requirements? 287
- 14.6 What is meant by access control? 289
- 14.7 Does access control guarantee data and computer security? 289
- 14.8 What forms of user verification are available? 291
- 14.9 If an access control system is completely secure can an attacker compromise information security? 295
- 14.10 How does a virus work? 295
- 14.11 How does a computer catch a virus? 296
- 14.12 Can viruses be automatically detected and killed? 296
- 14.13 What is Cryptography? 297
- 14.14 How is Cryptography used in data security? 298
- 14.15 Can Cryptography provide protection against forgery? 298
- 14.16 Are there different types of cipher? 299
- 14.17 What are the advantages of public key cryptography? 301
- 14.18 How can public key cryptography be used to sign a message? 302
- 14.19 What are the differences between encryption and authentication? 302
- 14.20 What is key management? 303
- 14.21 Are there significant differences between the security of stored and transmitted data? 304
- 14.22 Can databases be made secure? 304
- 14.23 What is inference control? 305
- 14.24 What is the role of monitoring in information security? 305
- 14.25 What is an audit trail? 306
- 14.26 What are the important considerations in the development of a security logging system? 306
- 14.27 What protection should be afforded to security logged data? 307
- 14.28 What data should be logged for security purposes? 307
- 14.29 How should security logs be processed? 308
- 14.30 How should security logs be used? 309

- 14.31 What are the main factors of physical security? 309
- 14.32 What are the physical security considerations of a computer centre location? 310
- 14.33 What are the essential differences between personal computer and mainframe security? 311
- 14.34 What are the potential threats to personal computer data? 312
- 14.35 What are the main aspects of personal computer security? 313
- 14.36 What are the security exposures associated with the connection of a microcomputer to host systems or networks? 314
- 14.37 What are the main concerns in network security? 315
- 14.38 How can networks be attacked? 316
- 14.39 What are the major parameters of network security? 317
- 14.40 Is there more risk associated with dial-up, or switched lines as compared with dedicated or leased lines? 317
- 14.41 How can cryptography be used in a data communications network? 318
- 14.42 What are the security implications of using Open Systems Interconnection (OSI)? 320
- 14.43 How will security be established in OSI systems? 321
- 14.44 What are the security concerns in relation to electronic mail services? 322
- 14.45 How can office data, and software be protected against malicious attack? 323

Index 325

26655/III (CB)

The legal framework within which information technology operates does not always keep pace with the technology. Although information technology has not yet fully accommodated



03-026655-000-0

traditional legal concepts. Such challenges require that existing law should either be adapted or interpreted in unfamiliar situations. If this is impossible or unsatisfactory then new legislation needs to be passed.

This second edition of *Information Technology & The Law* analyses and discusses:

- new legislation, such as data protection, which has an impact on information technology;
- legislation that has been extended or altered to take into account information technology — for example, copyright, patents, evidence;
- contractual means of ensuring legal security in the absence of legislation — for example, interchange agreements.

Information Technology & The Law, second edition has been significantly expanded and updated and provides new chapters on Electronic Data Interchange, European Community Law and Computer Security.

Chris Edwards is Professor of Management Information Systems at Cranfield School of Management. He is a consultant to a number of international organisations on strategic information systems matters.

Nigel Savage is Professor of Law and Head of Nottingham Law School, Nottingham Polytechnic. He is also Consultant Director of Training and Professional Development with the London solicitors firm of Frere Cholmeley and he acts as consultant to a number of organisations and journals.

Ian Walden is Tarlo Lyons Research Fellow in Information Technology at Nottingham Law School. He is editor of *EDI and the Law* and of the monthly newsletter *Applied Computer and Communications Law*. He is also a member of the ICC (UK) Committee on Computing, Telecommunications and Information Policy and the EDI Association's Legal Advisory Group.

ISBN 978-1-349-11770-3

9 781349 117703

