

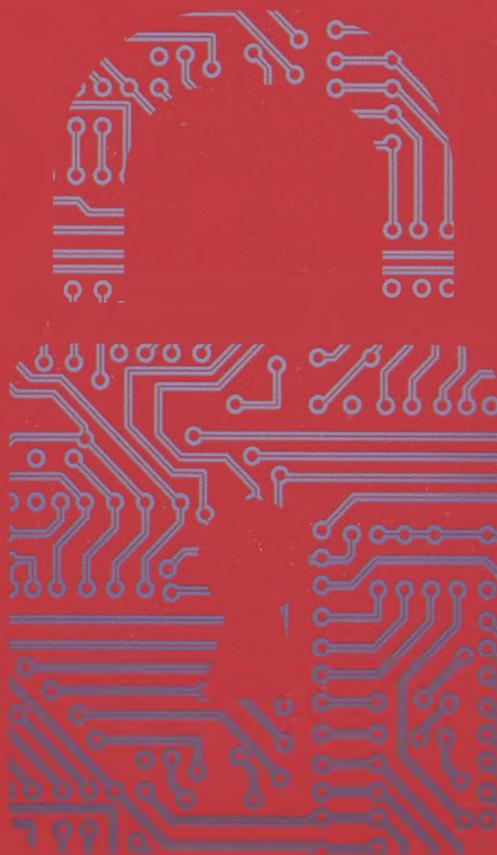
# CYBER SECURITY

Law and Practice

Dean Armstrong QC

Dan Hyde

Sam Thomas





Cyber Security:  
Law and Practice



# Cyber Security: Law and Practice

Dean Armstrong QC  
2 Bedford Row Chambers

Dan Hyde  
Penningtons Manches LLP

Sam Thomas  
2 Bedford Row Chambers



LexisNexis®

Published by LexisNexis

LexisNexis  
Regus  
Terrace Floor  
Castlemead  
Lower Castle Street  
Bristol BS1 3AG

Whilst the publishers and the author have taken every care in preparing the material included in this work, any statements made as to the legal or other implications of particular transactions are made in good faith purely for general guidance and cannot be regarded as a substitute for professional advice. Consequently, no liability can be accepted for loss or expense incurred as a result of relying in particular circumstances on statements made in this work.

© RELX (UK) Limited, trading as LexisNexis 2017

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any way or by any means, including photocopying or recording, without the written permission of the copyright holder, application for which should be addressed to the publisher.

Crown Copyright material is reproduced with kind permission of the Controller of Her Majesty's Stationery Office.

**British Library Cataloguing-in-Publication Data**

A catalogue record for this book is available from the British Library.

ISBN 9 78178 473345 2

Typeset by Letterpart Limited, Caterham on the Hill, Surrey CR3 5XL

Printed in Great Britain by CPI Group (UK) Ltd, Croydon, CR0 4YY

Dedicated to my son, Freddie.  
My special thanks to my parents, Merle and Paul, and to Paula, Oliver  
and Anna for their unstinting help, encouragement and support in all  
that I do.

*Dean Armstrong QC*

Dedicated to Emily Greenwood, Lesley Rockley and Roger Thomas,  
thank you for all your support.

*Sam Thomas*

Dedicated to my parents, Terence and Shirley Hyde,  
for their inestimable support and faith in this and everything.

*Dan Hyde*



## PREFACE

This work seeks to cover a wide spectrum of legal issues, both civil and criminal, that can conveniently be termed ‘cyber security law’. We define ‘cyber’ to mean using, involving or relating to computers and the online environment. Cyber law, in the context of this book, refers to those laws that govern the use and control of information within this cyber arena. Accordingly a ‘cyber-attack’ denotes the misappropriation or misuse of this information as well as any crime perpetrated by use of a computer or other electronic storage device. A cyber-attack can take a multitude of forms, be launched by a diverse range of perpetrators against a range of victims for innumerable purposes; we have sought to ensure this work addresses all those possibilities and is equally relevant to online trade mark infringement or employee misuse of confidential data as it is to disruption of service attacks or other such system or equipment attacks. While striving to provide comprehensive coverage we accept this book does not cover every element of cyber-related law. In particular, certain well-referenced areas within intellectual property are deliberately excluded as being outside the scope of this work.

The law faces huge challenges to keep up with the rapid development of technology, which provides opportunities for the misuse of information for commercial gain or other objectives.

Legislation in this area must strike a balance between enabling interception, monitoring and proper surveillance of communications by intelligence and investigative agencies on the one hand and maintaining user security and confidentiality on the other. A conflict often arises where the rights to privacy and freedom of expression are set against the desire to access all areas so as to effectively police cyber communications and data use. End-to-end encryption used in applications such as WhatsApp, iMessage or BBM are an example where security may be viewed as welcome confidentiality by the user but as dark corners of inaccessibility by the state.

The worldwide dimension adds a further complexity. There can be serious problems in bringing civil suits where there is little prospect of obtaining or enforcing judgments, or where countries have neither the means nor the political will to effectively investigate and prosecute criminal offences. The Serious Crime Act 2015 recognised this and introduced amendments to the Computer Misuse Act 1990 to address the issues by extending the United Kingdom territorial reach and ability to prosecute where there is a significant

link to the United Kingdom. This may be no more than a sticking plaster given the situations where it will be impractical or impossible to prosecute and international perspective is even more difficult where a state, as has frequently been alleged, is itself either perpetrating or aiding the behaviour. We have sought to tackle this and other issues, both legal and practical, that may arise in a cyber security context. We acknowledge the novel and developing nature of law in this area made that objective a challenge.

Our aim was to produce a comprehensive reference work that provides both a narrative and practical guidance on the many aspects of cyber security law. Cyber laws cover a vast range of areas and such is the volume of material that each chapter in this book could be a book in itself. With that in mind we have been selective in the hope that the book's content is sufficiently focused as to enable an understanding of the law as it applies to cyber security. We hope we have achieved our objective. The law is stated as at 1 February 2017.

The authors would like to thank Anita Noerr for her research and Christopher Saad for his help with Chapter 10.

Dean Armstrong QC and Sam Thomas, 2 Bedford Row Chambers  
Dan Hyde, Pennington Manches LLP

*1 February 2017*

# CONTENTS

Preface	vii
Table of Cases	xv
Table of Statutes	xxi
Table of Statutory Instruments	xxvii
Table of European Materials	xxix
<b>Part 1</b>	
<b>The Legal Framework</b>	
<b>Chapter 1</b>	
<b>Cyber Crime</b>	<b>3</b>
The offences	3
Offences under the Computer Misuse Act 1990	4
Unauthorised access to a computer (s 1)	6
Unauthorised access with intent to commit further offences (s 2)	9
Unauthorised acts with intent to impair the operation of a computer (s 3)	10
Making, adapting, supplying or offering to supply an article (s 3A)	13
Unauthorised acts causing or creating the risk of serious damage (s 3ZA)	15
Defences	17
Territorial scope	17
Inchoate offences	21
Nationality	23
Law enforcement officers	23
Serious crime prevention orders	24
Sentencing	24
<i>R v Mangham</i>	24
<i>R v Martin</i>	26
Fraud	27
Fraud Act 2006	28
False or offensive social media profiles	31
Data use offences	32
Data Protection Act 1998	32
Failure to register as a data controller	34
Unlawfully obtaining or disclosing personal data	35
Enforcement	36

Improper use of networks	38
Dishonestly obtaining electronic communications services (ss 125–126)	39
Improper use of public electronic communications network (s 127)	40
<i>Chambers v DPP</i>	41
The Guidelines on Prosecuting Cases involving Communications sent via Social Media	43
Cyberstalking	44
Malicious Communications Act 1988	45
Revenge pornography	48
<b>Chapter 2</b>	
<b>Civil Liability under the Data Protection Act 1998</b>	<b>53</b>
Liability for personal data	53
Data Protection Act 1998 – an overview	53
Definition of key terms (s 1)	54
The data protection principles (s 4)	54
The first principle – ‘data must be processed fairly and lawfully’	55
The second principle – ‘data must be obtained only for one or more specified purpose’	56
The third principle – ‘personal data shall be adequate, relevant and not excessive’	56
The fourth principle – ‘personal data shall be accurate and, where necessary, kept up to date’	57
The fifth principle – ‘personal data shall not be kept for longer than is necessary’	57
The sixth principle – ‘personal data shall be processed in accordance with the rights of data subjects under this Act’	58
The seventh principle – appropriate technical and organisational measures to secure personal data	58
The eighth principle – data not be transferred outside the EEA unless that country ensures an adequate level of protection for the processing of personal data	59
Application of the Act (s 5)	60
Right of access to personal data (s 7)	61
Enforced subject access request (s 56)	63
Right to prevent processing likely to cause damage or distress (s 10)	64
Rights in relation to automated decision making (s 12)	66
Compensation for breach (s 13)	66
<b>Chapter 3</b>	
<b>Civil Liability and Redress</b>	<b>69</b>
Deceit	69
Breach of trust	70
Dishonest assistance	71
Conversion	72
Trespass	73

Conspiracy	73
‘Unlawful means conspiracy’	74
‘Lawful means conspiracy’	74
Liability to third parties	75
Directors’ duties	75
Consumer rights	77
<b>Chapter 4</b>	
<b>Cyber Property</b>	<b>79</b>
Introduction	79
Misuse of private information	80
Misuse of private information in a cyber context	82
Jurisdiction	83
Data Protection Act 1998	83
Damages	85
Interception of telecommunications	86
Compulsion to provide private information	88
The Freedom of Information Act 2000	89
<b>Chapter 5</b>	
<b>Employer Liability and Protection</b>	<b>91</b>
Introduction	91
Confidential information	92
<i>Crowson Fabrics Ltd v Rider</i>	94
<i>Brandeaux Advisers (UK) Ltd v Chadwick</i>	97
<i>Pintorex Ltd v Keyvanfar</i>	98
Protecting confidential information	99
Trade secrets	101
The Trade Secrets Directive	101
Copyright	102
The Software Directive	102
Copyright, Designs and Patents Act 1988	104
<i>Navitaire v Easyjet</i>	106
<i>Nova Productions Ltd v Mazooma Games Ltd</i>	109
<i>SAS Institute Inc v World Programming Ltd</i>	110
Databases	112
Copyright and Rights in Databases Regulations 1997, Part III	114
Databases to protect software	115
<i>Cantor Gaming Ltd v GameAccount Global Ltd</i>	115
<i>Navitaire v Easyjet</i>	116
<i>Flogas Britain Ltd v Calor Gas Ltd</i>	117
Employer liability	119
Direct liability	119
Vicarious liability	120
Directors’ liability	121
Employer measures, systems and procedures	124
Cyber terms of use and the employee contract	124
Practical measures	126

Disciplinary procedures	126
<b>Chapter 6</b>	
<b>Commercial Espionage</b>	<b>129</b>
Introduction	129
Intelligence Services Act 1994	130
State immunity	131
Computer Misuse Act 1990	132
<i>Oxford v Moss</i>	133
Statutory provisions	134
Trade marks	134
Trade Mark Directive	136
Trade Mark Regulation	137
Internet and trade marks	139
Copyright, Designs and Patents Act 1988	141
Patents	142
Difference between trade marks and patents	143
Common law	144
Passing off	144
Passing off and cyber squatting	147
Passing off and trade marks	149
International/European approach	150
<b>Chapter 7</b>	
<b>Control Mechanisms for Embedded Devices</b>	<b>153</b>
Introduction	153
Technical protection	154
Awareness of threats to embedded systems	154
External threats	155
Internal threats	156
Access control	157
Copy control	159
The legal and regulatory context	160
The Copyright Directive	160
Mens rea	163
The Software Directive	164
Mens rea	165
Conditional Access Directive	165
Mens rea	166
Copyright, Designs and Patents Act 1988	166
Circumvention of technical devices applied to computer programs (s 296)	167
Circumvention of technological measures (ss 296Z–296ZG)	168
Unauthorised decoders: s 297A	169
European Union Agency for Network and Information Security	170
Protection through litigation	171
Copyright	172
Digital Economy Act 2010	173

Patents	178
The commercial approach	178
<i>British Phonographic Industry Ltd v Mechanical-Copyright Protection Society Ltd</i>	180
<b>Part 2</b>	
<b>Responding to a Data Breach</b>	
<b>Chapter 8</b>	
<b>Responding to a Data Breach</b>	185
Introduction	185
The data security breach	185
Notification	187
Legal remedies	188
Risk-based approach	190
<b>Chapter 9</b>	
<b>Investigating Incidents and Powers of Investigators</b>	191
Introduction	191
Powers of authorities	192
The investigating authorities	192
The relevant powers	193
Data Retention and Investigatory Powers Act 2014	196
Investigatory Powers Act 2016	199
Oversight	202
New provisions	203
Regulation of Investigatory Powers Act 2000 (RIPA 2000) and interception of communications	204
The Investigatory Powers Tribunal	208
SFO section 2 powers	210
The Intelligence Services Act 1994	213
Obtaining of warrants	215
Pre-arrest	216
Post-arrest	216
Specific premises	221
All premises warrant	221
Protected materials	222
Legally privileged material	222
Excluded material	223
Special procedure material	223
<b>Part 3</b>	
<b>Litigation, Evidence and Remedies</b>	
<b>Chapter 10</b>	
<b>Remedial Steps and Mitigating the Loss</b>	231
Introduction	231
Remedial steps	232
Injunctions in cases of copyright infringement	233

Stop and desist notices: Data Protection Act 1998	236
Where the s 10 notices do not apply	236
Who or what is a data controller?	237
What must the data controller do upon receipt of a s 10 notice?	237
What if damage has already been suffered?	238
Who to approach?	238
Criminal prosecutions	238
Computer Misuse Act 1990	239
Data Protection Act 1998: the criminal offences	240
Unlawful obtaining etc of personal data (s 55(1))	240
Practical steps	241
<b>Chapter 11</b>	
<b>Litigating and Rules of Evidence</b>	<b>245</b>
Introduction	245
Good Practice Guide for Computer Based Electronic Evidence	246
Practical issues facing law enforcement and other officials in evidence	
gathering in computer and electronic storage devices cases	247
Significant distinction between ‘directed’ and ‘intrusive surveillance’	249
Jurisdictional issues and ‘forum shopping’	251
Locus of the perpetrator	251
<i>Wintersteiger AG v Products 4U Sondermaschinenbau GmbH</i>	252
Evidence obtained abroad – general principles including letters of	
request	253
Obtaining evidence from abroad	253
Evidence obtained illegally – general principles	255
<b>Part 4</b>	
<b>The Future</b>	
<b>Chapter 12</b>	
<b>The Legal Environment post-Brexit</b>	<b>259</b>
The effect of Brexit	259
The immediate future	259
The medium term	260
Practical steps	260
Different interconnectivity models	261
Where does that leave GDPR?	262
Jurisdiction	264
How extensive are the new proposals?	265
What can be done now to ensure that the transition to compliance	
with the GDPR or UK equivalent is as smooth as possible?	269
Directive on Security of Network and Information Systems (NIS	
Directive)	269
<b>Index</b>	<b>273</b>

Biblioteka Główna  
Akademii Sztuki Wojennej

26635/III (CB)



03-026635-000-0

# CYBER SECURITY

## Law and Practice

**Dean Armstrong QC**, 2 Bedford Row

**Dan Hyde**, Partner, Penningtons Manches LLP

**Sam Thomas**, Barrister, 2 Bedford Row

Cyber security and data management are among the biggest issues facing business and other organisations today. The law faces huge challenges to keep up with the rapid development of technology which provides opportunities for the misuse of computers for commercial gain or other reasons.

This new work covers the vast spectrum of law, both civil and criminal, as it applies to data control, data management and cyber security issues. It considers the legal implications of internal threats from employees, data mismanagement or inadequate software, together with external threats from competitors or criminals, and looks at practical ways to deal with potential or actual cyber incidents.

**Cyber Security: Law and Practice** provides a unique, comprehensive coverage, looking at three main areas:

- Legal Framework – Part 1 covers cyber crime, civil liability under the Data Protection Act, other forms of civil liability and redress, cyber property, employee liability and protection, commercial espionage, and control mechanisms for embedded devices
- Data Issues – Part 2 considers how to respond to a data breach, and legal aspects of investigating incidents and the powers of investigators
- Litigation – Part 3 examines what remedial steps can be taken and how to mitigate loss, as well as issues surrounding litigation and the rules of evidence.

The work concludes by looking at the potential impact of 'Brexit' on data management and control, and the significance of the General Data Protection Regulation.

This valuable new resource will be a single point of reference for legal practitioners including solicitors, barristers, in-house counsel, compliance officers and those dealing with cyber risk and data protection/management not only as it affects corporations but also other entities, individuals and States.



 LexisNexis®

Also available as an eBook,  
visit [www.jordanpublishing.co.uk](http://www.jordanpublishing.co.uk)

ISBN 978-1-78473-345-2

9 781784 733452