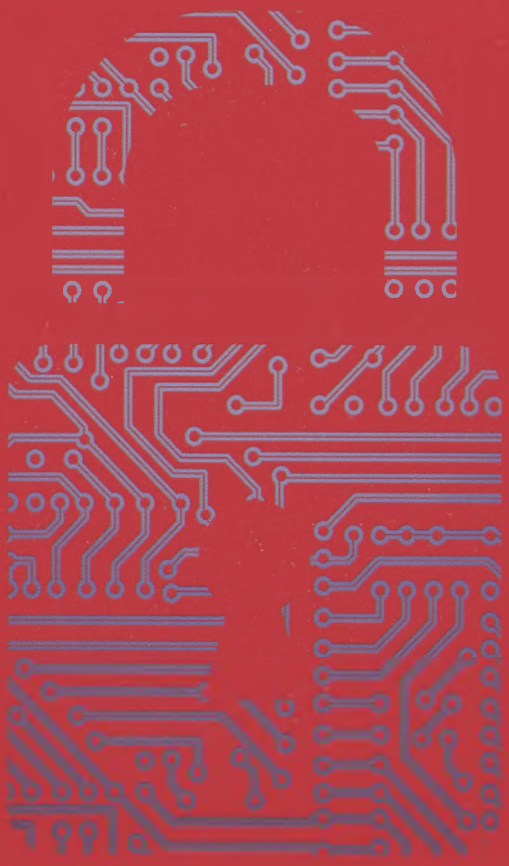
CYBER SECURITY

Law and Practice

Dean Armstrong QC
Dan Hyde
Sam Thomas



LexisNexis®

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

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

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

ISBN 978-1-78473-345-2

9 781784 733452