BOOK REVIEW

INFORMATION TECHNOLOGY LAW

Fifth Edition

By Ian J. Lloyd

Oxford: Oxford University Press, Fifth Edition, 2008, 650 pp. (incl. index), £34.99,
ISBN: 978-0-19-929977-5

In the present era of cyber laws, the issues of privacy, data protection and control (especially trans-border data flows); cyber crimes and crimes assisted by computers, cyber-terrorism, computer forgery and fraud; cyber squatting, intellectual property protection including Digital Rights Management (DRM); various Internet regulations coming up time to time; e-commercial ventures; applied cryptography, digital watermarking; online memorandum of understanding between various parties and stake holders; have become open. The academic courses in cyber law with a pre-defined body of knowledge often fail to answer the questions related to multi-faceted cyber issues. Starting from the post- Second World War expansion of rights to privacy and travelling through the emergence of data protection, the author, Ian J Lloyd, successfully covers the cyber-legal issues that require to be addressed in the light of today's enactment of IT Laws. He also recognizes the dynamic nature of cyber-legal problems as his each chapter is followed by 'Suggestions for further reading'. The reading suggestions were carefully crafted by the author who used his keen skill to premeditate the queries that readers are likely to have and to provide relevant tools and sources to independently investigate them. In practice, the sources were seen to lead the reader to the answers to further questions – almost as if Ian J Lloyd was able to read the minds of his readers.

The purpose of this review is to offer a quick run through Professor Lloyd's arguments so that other teachers and professionals can make the best out of this book. IT law in all flavour can be considered as the central premise of this book. The central chapters present enough case studies on the application of IT law and closing chapters assess the implications of legal processes in the purely digital media of the Internet interwoven with the impact of advance digital technology.

The introductory pages of the book do talk about 'ambivalent feelings' toward the ever-changing nature of technological development that brings or suggests some new cyber-legal instrument everyday. The author has taken up the challenge to complete a new edition whenever such updating is required. Other than the latest IT laws of the United Kingdom; Austria, France, Germany, Republic of Ireland, Sweden and the United States have IT laws that provide a bigger arena for combating issues. Knowledge of European legislation would help the reader to swim fast through the sea of knowledge created by the author. In this context, examples of regulations and cases from the developing countries are not abundant, which otherwise would have provided a more complete picture of global technocracy governed by IT laws.

Nevertheless, the learned author explores the vast unknown terrain of IT law such as 'Non-contractual Liability'[1] and 'Defamation and the Internet.'[2]

The issues of IT law are explored by devising a four-part approach. Part I is related to privacy and data protection. Part II deals with computer related crime. Part III takes care of Intellectual property issues. Part IV addresses the various legal intricacies of the Internet.

Part I is expanded through eight well-devised chapters that address the various aspects of privacy and data protection. The famous report, 'A Surveillance Society,' issued by the UK Government's Information Commissioner's Office in 2006, sets the backdrop for privacy implications of information technology. The forms of surveillance by Alan Westin are detailed, however, the application of surveillance devices for these different forms are not differentiated and it remains confined to the area of data surveillance. Chapter 2 gives a comprehensive history on the emergence of data protection through the effort of the United Nation's Economic and Social Council to the UK Data Protection Act of 1998. The scope of data protection in Chapter 3 illustrates the different kinds of data that were used to devise different remedies. An attempt to adopt an expansive definition of the scope of personal data has been made successfully and data processing in such cases is elaborated. Jurisdictional issues are to be discussed keeping the UK as the base country and the European Union as the directive authority. Chapter 4 introduces the supervising agencies such as the Information Commissioner and Information Tribunal, independent data protection supervisors, and the data protection registrar. The Chapter is able to capture the significance of the debate on the role of data protection in a modern society. Chapter 5 lays down the Data Protection Principles, which leaves enough scope to doubt "whether any changes of substance have been made from the situation existing under Data Protection Act 1984." The Chapter on individual Rights and Remedies discusses subject access provisions and exceptions that lead to denial of access. Automated decision-making is considered as one of the remedies, though limitations are considered circumstance-specific. Sectoral aspects of data protection are the subject matter of Chapter 7, where the communication sector is given its due importance in terms of intrinsic security. The desired objective is fulfilled as the author employed the technique of 'opt-out'; he concludes that that various forms of unsolicited communication using media such as telephone or e-mail can operate on an 'opt-out' basis. Chapter 8 brings the regulation regarding the trans - border data flow and provides 'Safe Harbour' principle. This chapter is crucial to understand intended transfer of data with and/or without adequate levels of protection. The Recommendation on Cross Border Co-operation in the Enforcement of Laws protecting Privacy adopted by OECD in 2007 provides a solution for trans-border issues with a national point of contact in each member state.

Computer related crime is the context of Part II. The phenomenon of computer related crime includes computer fraud, hacking, viruses, DoS attacks, etc. The enactment of computer misuse legislation and legislation for Computer related crime is the subject matter of Chapter 10. This chapter follows the view of Europe's Convention on Cyber Crime. The offences are categorized into computer related, content related,

---

[1] Ian J Lloyd, Information Technology Law fifth edition, at pages 547 - 570

[2] Ian J Lloyd, Information Technology Law fifth edition, at pages 571 - 586

infringement of copyright & related rights and offences against confidentiality, integrity and availability of computer data and systems. The section on unauthorized users is well illustrated using a number of cases, with the author providing a detailed discussion on each. Illegal inception is discussed in relation to the Cyber Crime Convention and the solution offered has been backed up by the provisions of the Regulation of Investigatory Powers Act 2000 (UK). However, in the absence of such regulation in other countries, the line of treatment remains to be devised. Damage of data and conviction is duly supported by Computer Misuse Act 1990; it broadly covers the DoS attacks, although today DoS attacks often have different strains and cannot be generalized into one broad category. The section on the misuse of devices that contributes to cyber crime leaves further scope for supplementary reading. The chapter on computer forgery and fraud gets a similar exclusive treatment through various acts, regulations and related cases. The section on 'the dishonest obtaining of services' is very apt in the present day introduction of various web services on a service oriented architecture, though I expect a further revision of this section is likely to come up in future editions. The problems of family users are highlighted in the chapter 'the Internet and computer Pornography.' The issues around the safe use of the Internet bring out a number of protection mechanisms, both technical and legal. The cases cited bring out the nature of offence committed by using pseudo-photographs or illegal synchronization of multimedia products. The inadequacy of actions taken by law enforcing agencies can be tackled rightly on the basis of jurisdiction of creation of material and access of material. The following chapter, Chapter 13, discusses detecting and prosecuting computer crime. The evidence of criminality is countered mainly from a legal angle; for example, the grant of a search warrant, extradition, the provisions of Criminal Evidence act 1984 (UK), etc. The missing link to computer forensics or digital forensics would have provided further fullness to this chapter.

Part III examines Intellectual Property (IP) issues, which originally attracted me to use the book for teaching learning. The Intellectual Property Law, in spite of having a 'long and varied history,' requires a newer and fuller treatment to deal with the commodities of our information society and the author deals with the issues by emphasizing effectiveness. Chapter 14 is totally devoted to the history of IP, different forms of intellectual property and the development of IP treatment. Chapter 15 brings out the key elements of the patent systems, including the patents in the international arena, requirements for patentability and matters that are excluded from patent protection. However, the section on 'Patenting Software' provides insufficient information and fails to provide a direction to the software patent applicants. In the case that there is a lack of guidelines for software patents, the software authors become software copyright applicants by default, which may not be a desirable situation. The process of obtaining and enforcing a patent gives a preliminary exposure to the procedure. The above lacuna is filled to a greater extent in Chapter 16 on Patents and Software through examples of specific cases and various conventions and treaties. The development of software patent jurisprudence has again paved its way through a number of important case histories. The controversy on technical effect approach is weighed on the basis of a number of principles that are called the 'Four Stage Test.' Chapter 17 covers copyright protection, which starts with copyright basics and rightly moves towards the development of software copyright. The author supports some of the principles of copyright that prevent piracy effectively. The section on 'Applying Copyright Principles to Software' compares physical infringement of copyrighted works and software piracy, and discusses fair dealing

provisions of copyright and users' rights for software. In the case of software, unlike other copyrighted works, error correction, back up copies, reverse engineering and decompilation requires special provisions. The author has done justice in this respect by mentioning a number of important judgments to support his view toward the various topics that are covered. By considering computer programs as visual works like an image, their related protection mechanisms are given a fair treatment. The much-needed topic 'Copyright in the Information Society' is the concern of Chapter 18. The Directive on Copyright in the Information Society, adopted by the European Parliament in 2001 and enforced fully in 2003, chalks out the role of copy protection and Digital Rights Management (DRM) (the digital equivalent of physical copyright). DRM is defined as a technology that creates and protects access, as well as disseminating the copyrighted works in electronic media over the Internet. Professor Lloyd also addresses the question of choice between copyright and DRM; he successfully separates the two on the basis of technology used. Private copying in the digital age makes the definition of infringement more complex and needs to be redefined. Protection of databases, similarly, is the main thrust of Chapter 19, in which traditional forms of protection in the new technology era is compared. Implementation of the Software Protection Directive saw a number of copyright changes; for example, the Database Right was created on the basis of the implementation of the Database Directive, although the duration of the right differs from other copyrighted works (typically 15 years). Other forms of IP, like trademark, are having their digital counter part as Domain Name System (DNS). Trademark and Domain Name issues are the corner stone of Chapter 20. Domain Name hijacking, or cyber squatting, is discussed using an ample number of cases as examples. At the same time, the author also considers the concurrent use of domain names. He traverses the effectiveness of trademark jurisprudence. The Uniform Dispute Resolution rules are discussed as per ICAAN rules and the supplementary reading provided with this chapter is well selected. Chapter 21 deals with competition and IP issues which have not been dealt in detail by authors of other information technology law books.

Part IV, the last section of the book, pertains to legal issues of the Internet of interest to legal professionals who are newly introduced to cases in digital world. The author appreciates that the issues have contemporary importance in today's world. Chapter 22 – 'Internet Regulations and the Rise, fall and Rise of .com' – is catchy enough to draw the interest of the reader and explains top level domain names in a very simple manner. Various reforms of Internet Regulations in view of problems of cyber squatting and commercialization in a global market through the Internet are explained with the help of cases and regulations. Legal issues of the Internet remain incomplete and initiatives in e-commerce and the legal significance are not given its due. Chapter 23 discusses International and European initiatives as outcomes of Electronic Commerce Directive regulations 2002 (UK). Online contracts and determination of its jurisdiction are attempted through a number of texts with which the author is well versed. Chapter 24 is a continuation of such initiatives to be incorporated into the mechanism of e-commerce. The chapter gives the inherent mechanism of cryptography, electronic (digital signatures) and Electronic Communication Act 2000 for use in e-commercial venture. The nature of encryption is explained in accessible to informed laymen or legal professionals. The role of trusted third parties, with respect to Guidelines for Cryptography Policy, is narrated. The Electronic Signature Directive and its various implementable electronic signatures are the concerns of this chapter. The cryptography service providers (like Certification Authority) are defined to

encompass the facility of cryptographic techniques. The issue of contractual liability for defective software is a very timely argument which can be equally appreciated by the defenders of legal services as well as the users of the software. The different forms of software and related contracts must be understood by considering a number of major and minor factors (e.g. it can be customized software supplied on a storage device such as a disk or CD). The storage device in this case involves goods, but in the case of downloaded software goods are not the part of the equation. There are certain implied terms in software contracts that require training to read in between the lines. The section on implied terms on Software Contracts not only gives the right exposure to prepare the users to not be caught unaware, but also gives remedies for breach of the implied terms. Exclusion or limitation of liability, enforceability of shrink-wrap licenses and its effect on consumer contract and other non-consumer contracts are other topics of interest which vie for attention of the readers. Non-contractual liability is the context in which Chapter 26 has been set. It sets out the provisions of tortuous liability such as duty of care, breach of duty, etc. The applications of the concept of negligence to software are explained with an example of a case (a typical approach of the author). Liability for the use of information technology and liability for the failure to use information technology are issues of equal importance and in each case 'proximate cause of resulting damage' is to be established; elaborate cases therefore provide a point to help establish this. The author successfully introduces the issues on remoteness of damage, compensatable loss, defenses and measures of damages, which certainly improve the legal insight of a software professional and the tech-legal wisdom of a legal enthusiast. The legal issue of the last part of the book is on defamation and the Internet. In the consequent chapter the author deals with liability for defamatory comments (e.g. an employer's liability, liability of ISPs, etc.). Liability of an ISP is described according to the Electronic Commerce Directive, which provides some rudimentary protection to ISPs. The author further suggests how to deal with such liability. The last chapter throws out some open questions such as, 'Who is liable for defamatory Comments?'[3] Or 'Single or multiple publications?'[4] The curtain is drawn after answering these questions satisfactorily which comprehensively addresses the possibility of many other such questions to be raised.

Ian J Lloyd is an extremely well read author in the area of information Technology Law. He has been the Director of the Center of law, Computers and Technology at the University of Strathclyde, Glasgow. Professor Lloyd's sophistication and breadth of knowledge is demonstrated in this book, which has seen various editions over the past twenty years. The continuous updating allows him to maintain a gamut of newer IT strategies before they become obsolete. The entire book is explained through the lens of the UK's IT scene and therefore makes it an authentic contribution towards UK IT law. The book examines IT law from a multi-disciplinary perspective and therefore serves as a ready help for teachers and academics in this field and would make a worthwhile addition to teaching material. The students of IT law will definitely find the book as useful reference. On the whole, this document is a peaceful co-existence of laws & technology and academics & profession, which is likely to remain a standard work for years to come.

---

[3] Ian J Lloyd, Information Technology Law fifth edition, at page 574

[4] Ian J Lloyd, Information Technology Law fifth edition, at page 584

Shefalika Ghosh Samaddar,

Lecturer (Senior Grade), Department of Computer Science & Engineering, Motilal Nehru national Institute of Technology
Allahabad, India

DOI: 10.2966/scrip.060109.188