Title**: Listening In Cybersecurity in an Insecure Age**

Author**: Susan Landau**

Date and place of publication: **2017, United States of America**

Publisher**: Yale University Press**

ISBN**: 978 0 300 22744 4**

Susan Landau is Bridge Professor of Cyber Security and Policy at the Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University. Susan Landau was a Senior Staff Privacy Analyst at Google, a Guggenheim Fellow and a Visiting Scholar at the Computer Science Department, Harvard University in 2012.

The author is well qualified to write this book. This is a book that appears to be a mature synthesises of the range of issues that Landau has considered over a number of decades in various forums. It is a highly readable book that puts the development of the digital world into perspective, specifically on politics and the tussle over encryption, with digital forensics mentioned in passing to illustrate the state of ignorance of some lawyers.

The book is an extended argument for the implementation of good quality secure encryption across all devices and the internet. Although not a text that discusses legal issues in the same way as a lawyer would expect, it is a book that judges and lawyers would learn from if they read it.

Landau provides a number of excellent examples of how hackers and people working for a state can break into and disrupt commercial and governmental organizations: such as switching power or water on or off at will. The numerous examples serve to illustrate the point that few people are concerned about the security of data, and that even the most private of personal data and state secrets are connected to the internet. It is astonishing how people at the apex of organizations are allowed to get away with treating security so cavalierly, yet data protection bodies across the world merely fine the offenders, and millions of bits of personal data continue to circulate well after the event.

The author sets out the problems at pp 57-61:

> (i) The precursor to the internet, the ARPANET was developed as research, rather than 'production' platforms. The underlying assumption was that everyone on the network could be trusted.
>
> (ii) System administrators discounted the level of skill and the motivation of potential hackers.
>
> (iii) The nature of humans is such that we do not use complex passwords.
>
> (iv) The flexibility that characterizes computer code enables changes in functionality that are not necessarily anticipated at the time the code is written. This means systems can be manipulated in ways their designers never intended.
>
> (v) Complex systems linked together leads to combined, unexpected interactions, which leads to greater insecurity.

Part of the difficulty, in the context of the law, is the ignorance of those involved with the law – not just judges, lawyers and legal academics, but

also such important people as the Director of the Federal Bureau of Investigation (for which see the exchange between Congressman Darrell Issa and James Comey in 2014 (at pp 122-123)). This exchange of ignorance is also noted in respect of lawyers (pp 147-149).

In the context of the overall tenor of the book, Susan Landau indicates, on p 171:

> '[And] the only way … is to make both the mode of communication and the devices themselves secure. …
>
> And that, in a nutshell, is it. The government's role is to provide security – national security and law enforcement – and not to prevent individuals from maintaining their own security.'

The encryption debate (the topic of the book) is 'not really about balancing public safety, national security, and privacy. It's about balancing law enforcement's easier access to intelligence with society's need for strong online security.' (p 169)

In the context of this journal, the book is a very good introduction to the practical issues that arise from the topic. It offers a rational approach to dealing with encryption, but more importantly, provides lawyers and law students with an insight into the world in which they deal every day – yet know so little about.

Highly recommended.

Contents

Title: **Reset: Reclaiming the Internet for Civil Society**

Author: **Ronald J. Deibert**

Date and place of publication**: 2020 in Canada and the United States of America, 2021 in the United Kingdom**

Publisher: **House of Anansi Press Inc (September Publishing in the United Kingdom)**

ISBN (paperback): **978-1-9128-3677-2**

Ronald J. Deibert is a professor at the Munk School of Global Affairs, the Department of Political Science, and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He explains that the genesis for this book came out of the Ninth Global Assembly of the World Movement for Democracy, held between 6 and 9 May 2018 in Dakar, Senegal.

In essence, this book is an extended essay of the work that he and his colleagues have been doing at the Citizen Lab for decades.

As a polemic, the book provides a number of arresting examples of how the networked world has developed over the past twenty years, highlighting the control of the internet exercised by the massive and not-so-massive technology corporations – how dominance has been achieved, why such domination is sought, and the failure of politicians to counter the pervasive reach that even the most innocuous app will try to achieve once it is downloaded.

The internet has developed as a free-for-all, a lop-sided affair, in which traditional forms of media remain responsible for the publication of defamatory comments, but internet-related hosts are absolved from such responsibility. As a result, the internet has developed in a particular manner, which has led to unsavoury consequences. Whether it is possible to rectify this is debatable, according to Professor Deibert.

In addition, the development of sophisticated intrusive surveillance software has meant that intelligence agencies reap vast amounts of data about people for political reasons, as much as to

investigate crimes and potential crimes, or for the purposes of espionage.

Professor Deibert sets out a number of proposals in an attempt to rectify the problems we now collectively face, some of which involve, among other things, regulating monopolies (of course, the monopolies we see now would never have developed if regulators had prevented the giants taking over companies with technologies that clearly permitted the buyer to strengthen its stranglehold with the technologies it bought), and passing new laws. Taken together, and with the political will, the recommendations made in this book might go some way towards ameliorating the dreadful situation we find ourselves in, as described in the main chapters.

From the perspective of this journal, this book conveniently illustrates where some forms of electronic evidence comes from and illustrates that the evidence in some cases might be difficult to obtain or use, given its provenance. In addition, the inference is that dealing with such evidence is expensive, both financially and bearing in mind the need for appropriate knowledge, expertise and resources to follow through in the event it is decided to take legal action.

Although this book is not directly related to electronic evidence, any lawyer reading through the examples of use and misuse of technology would readily identify some much-needed areas of a change in the law, from rules relating to electronic evidence to the need for changes relating to unfair contract terms. On the latter, it would not be quite so necessary to make any changes in the law if judges took a more active role in unfair contract terms. It remains to be seen if they ever will.

Contents

Title: **Electronic Evidence and Electronic Signatures**

Editors: **Stephen Mason and Daniel Seng**

Edition: **5th**

Date and place of publication: **2021**,**London**

Publisher: **Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London**

ISBN Hardback **978 1 911507 26 0**

ISBN Paperback **978 1 911507 22 2**

ISBN epub **978 1 911507 23 9**

ISBN Kindle **978 1 911507 25 3**

ISBN Open Source PDF **978 1 911507 24 6**

In this updated edition of the well-established practitioner text, Stephen Mason and Daniel Seng have brought together a team of experts in the field to provide an exhaustive treatment of electronic evidence. This fifth edition continues to follow the tradition in English evidence text books by basing the text on the law of England and Wales, with appropriate citations of relevant case law and legislation from other jurisdictions.

Contents

Chapter 3 : Hearsay

Chapter 4 : Software code as the witness

Chapter 5 : The presumption that computers are 'reliable'

Chapter 6 : Authenticating electronic evidence

Chapter 7 : Electronic signatures

Chapter 8 : Encrypted data

Chapter 9 : Proof: the technical collection and examination of electronic evidence

Chapter 10 : Competence of witnesses

Notification of a book

Title: **Foong's Malaysia Cyber, Electronic Evidence and Information Technology Law**

Author: **Foong Cheng Leong**

Date and place of publication: **October 2020**

Publisher: **Thomson Reuters Asia Sdn Bhd**

ISBN: **9789672339816**

ISBN (ebook): **9789672339823**

This is a practical title written for litigators who are involved in matters concerning electronic evidence, information technology and cyberlaw.

Contents

Chapter 1 Civil Matters

Chapter 2 Cybercrime

Chapter 3 Admissibility of Computer- Generated Documents

Chapter 4 Presumption of Fact in Publication

Chapter 5 Instant Messages, Social Media Postings and Other Electronic Evidence

Chapter 6 Electronic Evidence in Industrial Relations Disputes

Chapter 7 Electronic Evidence in Family Disputes

Chapter 8 Discovery

Chapter 9 ".My" Domain Names

Chapter 10 Legal Practice and Technology

Chapter 11 Digital Economy

Chapter 12 Electronic Commercial Transactions

Chapter 13 Electronic and Digital Signatures

Chapter 14 Digital Assets

Chapter 15 E- Commerce