JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME (2d ed. 2015)
Cambridge University Press (Cambridge, UK: 2015), IBSN: 978-1-107-69816-1
Price: $64.99, pp.524
Cybercrime, Computers, Crime, Internet

Reviewed by Jaclyn Collier
Journal of High Technology Law
Suffolk University Law School

The Evolution of Crime in an Increasingly Digital World

"[T]his case illustrates many of the features and challenges of modern cybercrimes; it was organized, financially motivated, technologically sophisticated and transnational."[1]

Principles of Cybercrime, by Jonathan Clough, examines the elements and theories that apply to cybercrimes across four jurisdictions. This book review examines the entire volume, which covers major doctrines and elements of cybercrime law and jurisdictional theory, and assesses the book as an introductory reference tool to gain a better understanding of the principles of cybercrime. The author, Jonathan Clough, is a professor at Monash University, Australia in the Faculty of Law.[2] Although Clough has a particular focus on cybercrime, he teaches and conducts research more broadly in the areas of evidence and criminal law.[3] He has co-authored two books, *The Prosecution of Corporations* (Oxford University Press, 2002) and *Criminal Law* (Buttersworths, 1999), and has published numerous articles on evidence, cybercrime, juries, and criminal liability.[4] He was also a member of the Commonwealth Working Group of Experts on Cybercrime.[5]

---

[1] JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME 3 (2d ed. 2015).
[2] *See Professor Jonathan Clough – Researcher Profile*, MONASH UNIVERSITY, (Oct. 1, 2013), *archived at* https://perma.cc/EM8Z-AKZ4.
[3] *See Professor Jonathan Clough – Researcher Profile*, *supra* note 2.
[4] *See Professor Jonathan Clough – Researcher Profile*, *supra* note 2.
[5] *See* CLOUGH, *supra* note 1, at back cover.

Principles of Cybercrime is just that – an analysis of the legal principles pertaining to a range of cybercrimes. This second edition is divided into six parts. Part I provides valuable background and context for the aspects of cybercrime to be discussed in the subsequent sections. Clough walks the reader through the various types of activity that have been defined as cybercrime or cyberterrorism,[6] and supplies examples to help the reader understand the scope of cybercrime.[7] Importantly, Part I explains the focus of the remaining sections of the book, which is a comparative review and analysis of the substantive criminal law of cybercrime in Australia, Canada, the United Kingdom, and the United States.[8] This analysis also factors in principles from the Cybercrime Convention,[9] which Clough uses as an anchor for the comparative analysis throughout the book.

In each of the following sections, Clough arranges the material clearly and carefully, guiding the reader through an explanation and discussion of the elements of the crimes and the jurisdictional differences and similarities. Each section starts with background information on the offense and an overview of the law pertaining to that offense in each of the four jurisdictions. Part II, the lengthiest section, covers what is commonly known as hacking, or crimes where the computer is the target of the offense.[10] The offenses discussed include access offenses, modification or impairment of data, misuse of devices, and interception of data. Clough details the various types of computer attacks, including unauthorized access to computers and malicious software. Clough also explains a fundamental component to "computer as target" offenses: what is the meaning of "computer" in the context of criminal law.[11] The definition of a computer for

[6] *See* CLOUGH, *supra* note 1, at 9-15.
[7] *See* CLOUGH, *supra* note 1, at 18-22.
[8] *See* CLOUGH, *supra* note 1, at 26-27.
[9] *See* Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
[10] *See* CLOUGH, *supra* note 1, at 31.
[11] *See* CLOUGH, *supra* note 1, at 59.

each jurisdiction is skillfully teased out by the author, who also engages in a balanced assessment of the pros and cons of the different approaches.[12] This type of analysis, which continues throughout the book, allows the reader to get a good understanding of how virtual activity and technology are broken down and factored into criminal elements in the lawmaking and judicial processes.

Part III discusses fraud and offenses related to fraud, including spam and criminal copyright infringement.[13] The author reviews the way the four jurisdictions handle fraud in cyberspace, with a particular focus on identity theft.[14] Clough's studied analysis of the existing regulations and criminal statutes and the extremely varied approaches in each jurisdiction brings clarity and simplicity to the topic. The section on spam, which is arguably one of the more controversial topics of criminalization in the book, showcases Clough's ability to present both sides of an argument objectively,[15] as well as to provide logical, reasoned analysis of those arguments.[16]

Part IV, entitled "content-related offenses", delves exclusively into child pornography cybercrimes.[17] After covering the basics of these offenses, Clough focuses on the elements that can be difficult to pin down in cyberspace, such as the definition of "distribution" or "possession". These sections in particular go deep into the technological weeds, but the author breaks the concepts down in a way that makes it relatively easy for a person with little high technology background to grasp. For example, in the section on possession, Clough outlines the four elements of possession, which are (1) having physical possession of the item; (2) knowing

[12] *See* CLOUGH, *supra* note 1, at 59-67.
[13] *See* CLOUGH, *supra* note 1, at 209-86.
[14] *See* CLOUGH, *supra* note 1, at 238-54.
[15] *See* CLOUGH, *supra* note 1, at 276-78.
[16] *See* CLOUGH, *supra* note 1, at 278.
[17] *See* CLOUGH, *supra* note 1, at 289-374.

that he or she had physical possession of the item; (3) intending to exercise physical possession of the item; and (4) knowing the nature of the thing possessed.[18] The author goes on to discuss the intricacies of each element by analyzing examples from cases, comparing how specific pieces of technology are handled in each jurisdiction. To illustrate this, the book reviews several cases addressing the question of whether or not a defendant can be considered in possession of an item that has been deleted, but the item still remains in the computer's cache folder or is still available on the hard drive until it is overwritten.[19]

Part V explains and analyzes crimes against people, including "grooming", harassment, and voyeurism,[20] which puts the technological focus of this section secondary to the conduct of the defendant. A mirror image to Part IV, in Part V Clough goes into great detail to explain the predatory and harassing behavior of the defendant, and technology is, for the most part, a backdrop to illustrate how that offense can be carried out. For example, "grooming" is not a new phenomenon, but email and electronic communication have afforded many more opportunities for predators to make contact with a child, and have made it far more likely for that contact to be unsupervised by the child's parent.[21] The author explains how these offenders leverage the internet and other types of electronic communication to engage in grooming behavior, and then presents and analyzes the legislative responses.

Part VI is an overview of the jurisdictional issues related to prosecuting cybercrime.[22] This section is a summary of the fundamental questions related to extraterritorial jurisdiction: prescriptive jurisdiction, adjudicative jurisdiction, and enforcement jurisdiction.[23] This section,

[18] *See* CLOUGH, *supra* note 1, at 345.
[19] *See* CLOUGH, *supra* note 1, at 348-50.
[20] *See* CLOUGH, *supra* note 1, at 377-472.
[21] *See* CLOUGH, *supra* note 1, at 378. Grooming is the process by which a predator befriends a child and works to gain that child's trust in order to get the child to acquiesce to activity that is abusive. *Id.*
[22] *See* CLOUGH, *supra* note 1, at 375-88.
[23] *See* CLOUGH, *supra* note 1, at 475.

at only thirteen pages, is relatively short given the length of the rest of the sections and the complexities around extraterritorial jurisdiction. Regardless, while this section does not probe deeply into the extraterritorial jurisdictional issues, Clough provides a solid, high-level overview of the jurisdictional concepts that the reader should be considering in the context of cybercrime.

This book is a thoughtful, realistic approach to a complicated topic. The book is an excellent primer for readers with some legal background, such as academics, professors, law enforcement, practicing attorneys, and law students. Because the nexus of this book is crime and technology, it presents technical concepts on both sides that are likely to be daunting for the casual reader. However, it may also be a good reference tool for someone who has a technology background and is interested in learning more about applicable criminal law theories.

Throughout the book, Clough's logical and methodical approach transforms complex criminal theories and advanced technological concepts into digestible segments, providing an accessible guide to the foundations of cybercrime law. The organizational structure is consistent throughout the book, with Clough explaining at the start of each section, subsection, and sub-subsection what elements or nuances will be discussed, which allows the reader to build a mental framework to easily absorb and grasp the material. This structure also complements Clough's choice to review each cybercrime principle through a comparative analysis of Australia, Canada, the United Kingdom, and the United States, which gives the reader meaningful context and comparison.

The author's mastery of the subject matter stands out not only in the organization of the material, but in the substance. The authorities and analysis throughout the book are of a high-quality and clearly well-researched. Clough argues both sides of an issue where appropriate and provides his own insights, which are carefully reasoned and substantiated by strong primary and

secondary authority. The sources, which are primarily primary sources in the form of statutes and cases, are organized for easy reference with tables of legislation and cases at the beginning of the book and a bibliography of secondary sources at the end. The author also makes heavy use of footnotes and provides a comprehensive index, which allows this book to be used as a reference guide that does not necessarily need to be read in its entirety. The structure of the citations and sourcing allow a reader to gather sources to conduct more in-depth research on a topic.

The book achieves what the author intended, which is to organize the legal principles that apply to cybercrimes into one cohesive, very well organized volume. This is not a book for the casual reader, but it is great reference material for legal or high technology professionals who are interested in becoming better acquainted with cybercrime. Technology has become so ingrained in our everyday lives to the point where most people rarely think about the technology itself or understand how it works. What Clough does in this book is to bring technology to the reader without overwhelming while at the same time addressing key elements of cybercrimes.

Overall, the book was very well structured. However, the discussion of extraterritorial jurisdictional principles would have been more functionally useful if the overview were presented at the beginning in the introduction and the more topical concepts were woven into the section of the book where a relevant case was discussed. Ending the book with extraterritorial jurisdiction made it difficult to conceptualize how it would be applied in the context of the crimes that were discussed throughout the book. Nonetheless, the comparative jurisdictional analysis makes a strong argument that in a world that is increasingly connected and reliant on technology, nations should leverage agreements like the Cybercrime Convention to bring consistency and ease of prosecution to cybercrimes.

I thought this book was an excellent read. It is a technical book, but author's insightful analysis and commitment to a strong organizational structure helped to keep me engaged and interested. I am confident that I came away from reading the book with a good understanding of the principles of cybercrime in large part because of Clough's style and logical reasoning, which was also very well substantiated. I strongly recommend this book to people coming from a legal or high technology perspective who are interested in improving their foundational understanding of cybercrime.