Book Reviews

Electronic Theft: Unlawful Acquisition in Cyberspace

by Peter Grabosky, Russell G. Smith and Gillian Dempsey, Cambridge University Press, Victoria, 2001, 207pp, references 208–225pp, index 226–235pp.

Sarah Holthusen BA (Qld), LLB student, TC Beirne School of Law, The University of Queensland.

The fundamental principle of criminology is that crime follows opportunity, and opportunities for theft abound in the digital age.[1]

Western society is undoubtedly undergoing a transformation with the convergence of communications and computing in the industrial world. Escalating connectivity has unequivocal advantages, but is also accompanied by unprecedented opportunities for crime and acquisition.[2] *Electronic Theft* constitutes the first major international survey of the field, and covers a diverse range of electronic misdemeanours, many of which the legislature is still grappling to encompass in its laws. Computer-related crime is a worldwide phenomenon which transcends jurisdictional borders, and has the ability to impact upon many aspects of our everyday lives. The consequences of these types of crimes are often remarkable in their enormity and impact. *Electronic Theft* highlights the need for universal recognition of the dangers posed by this increasing trend, and for immediate implementation of protective mechanisms. The authors recognise that whilst we may never be able to eradicate these crimes of acquisition, it is fundamental that we, as individuals and as a community, understand the gravity of the threats posed and take adequate precautions and security measures.

I. The authors

Peter Grabosky is Director of Research at the Australian Institute of Criminology and President of the New Zealand Society of Criminology. He has previously conducted and published research in this new and fascinating area, including *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*[3]. Russell G. Smith is a senior research analyst with the Australian Institute of Criminology and the author of several works on crime and the medical professions. He has previously investigated the area of serious fraud in Australia and New Zealand. Gillian Dempsey is a barrister and a senior lecturer in law at the University of Queensland, specialising in information technology, intellectual property law and electronic commerce. All authors are highly regarded as experts in their field and have succeeded in putting together a comprehensive guide to the broad range of crimes of acquisition in cyberspace, and an evaluation of the efficiency of our legal system in protecting us against them. The authors make broad use of international data on electronic crime, from both academic and professional sources. The book is interspersed with fascinating anecdotes of the perpetrators of computer-related crime, their capabilities and the fundamental flaws in their work which often leads to prosecution.

1 Grabosky P, Smith R & Dempsey G, *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Victoria, 2001 at 1.
2 Note 1 at 1.
3 Grabosky P and Smith R, Federation Press, Leichardt, 1998.

II. Content

With estimates that global business-to-business online commerce may amount to US$7 trillion by the year 2004[4], the potential for online crime is increasing enormously. By means of introduction, the authors canvas the meaning of 'acquisition' and the extent to which our understanding of crimes of acquisition has changed with the introduction of technological phenomena, particularly the Internet. They also explain basic principles of criminology and the generally supported theory that crime is linked to opportunity, and our inability to be 'capable guardians' of intangible goods, primarily money, results in an inevitable increase in theft facilitated by technological means.

Traditionally, crimes of acquisition were solely restricted to goods capable of physical asportation, rendering intangible items like telephone lines and electricity incapable of being stolen. The rapid rate of technological developments in more recent years made it painfully evident that the law in this area was in desperate need of legislative change, and it has since become essential to implement technology-neutral laws capable of adaptation to unprecedented technology. Essentially, the authors are endorsing new methods of social control in the digital age which should not be restricted to various legislative enactments. Legal pluralism exists as the theoretical basis for *Electronic Theft*, and is the authors' answer to the challenges faced by the state with the advent of digital technology. Certainly, the capacity of the state in controlling behaviour on all levels is limited and it is becoming evident that non-state institutions are more than capable of exercising coercive power in the fight against crimes of acquisition. It is thus only through a stratum of control mechanisms that we can truly seek to assert control and order throughout the community.

Having explained the context of their approach, and canvassing what is meant by 'electronic theft', the remainder of the book is concerned with identification and exploration of specific forms of misappropriation using digital technology. Electronic theft of funds represents 'the clearest and arguably most lucrative' forms of acquisition in cyberspace.[5] Chapter Two examines a number of growing concerns with the advent of electronic payment systems, including direct debit, EFT, home-banking systems, card-based systems and electronic cash. Manipulation of these systems is increasingly common, and are fast discouraging the community from making use of convenient and fast purchasing over the Internet. Security flaws in these systems represent the major problem, and it is only through identification of these flaws and increased security mechanisms that one can seek to restore the community's faith in such systems.

The practice of mass extortion is inevitably facilitated by digital technology.[6] In the third Chapter this fascinating and intriguing area of computer crime, which asserts the potential to cripple billion dollar organizations the world over, is investigated. Extortion, a close cousin to robbery and bribery,[7] is not a remarkably new crime but its boundaries have rapidly expanded with the advent of digital technology. Extortion threats to damage information systems, identify security flaws or publicize private information can, for example, be directed to a large corporation in America by an extortionist in Iceland, within seconds using electronic mail. Payments to that extortionist can be carried out equally as quickly using electronic funds transfer which may secure anonymity and reduce the probability of an arrest. Privacy laws and trans-jurisdictional barriers also offer marked advantages to extortionists. Despite most existing laws embracing extortion facilitated by these means, the greatest challenges posed to the law enforcement community are the tasks

4 According to the Gartner Group, Note 1 at 1.
5 Note 1 at 15.
6 Note 1 at 44.
7 Note 1 at 34.

of detection and investigation. Statistics collected by the authors indicate that extortion is a growing phenomenon which we cannot afford to ignore.

As governments experience increased connectivity, opportunities to electronically defraud the system are increasing dramatically. The authors turn their attention to this problem in Chapter Four, an area which incorporates crimes of misappropriation of government funds, social security fraud, evasion of payments, manipulation of salary systems and espionage. Governments are not unusual targets, since they possess large financial resources; not surprisingly, many crimes against governments are perpetrated by actual employees, hence the authors emphasise a need for screening processes and internal control measures. The actual losses sustained by governments in this area are uncertain as this information is rarely made public so as not to encourage distrust in the system. However, a 1999 KPMG study revealed that 62% of government agencies surveyed experienced fraud in the preceding 2 years.[8] These crimes obviously pose grave threats to the integrity of our political system and adequate security and control mechanisms are an absolute necessity.

Chapter Five discusses telecommunications fraud, including misappropriation of telephone and Internet services. In some instances, telecommunications crime is simply a matter of falsification of identity or evasion of payment: such misdemeanours require little or no technological knowledge. In other cases, electronic manipulation of information systems is required to obtain services free of charge. Telecommunication hackers ('phreakers') also pose threats to telecommunications companies, and the existence of the Internet means perpetrators are able to share their knowledge with others, thereby encouraging such activities. Whilst most jurisdictions have laws specifically prohibiting telephone-related fraud, companies are more inclined to self-police than to seek out the help of the law enforcement community in the interests of preventing bad publicity. Companies have inexorably been forced to develop sophisticated internal security measures, such as software and skilled investigative capacity.

'Finance is the bloodline of an economy. . .and security markets are integral to a nation's economic system'.[9] In the following Chapter, the authors undertake a detailed examination of online securities fraud, an area in which the consumer is often the victim due to fraudulent and misrepresentative advertising practices, market manipulation and insider trading. The impact of new technologies has led to global transformation of the securities market, which has had both positive and negative consequences. Access to stocks online, without employing an intermediary such as a stockbroker, means trading securities is faster than ever before, but inherently more risky. The challenge to investors, faced with an unprecedented mass of information is to distinguish useful information from hype or blatant falsehood. The challenge to legal authorities is to preserve the integrity of capital markets and maintain public confidence, whilst identifying and punishing the perpetrators of fraud.[10] International cooperation, investor education and a self-regulated industry are identified as fundamental to prevention of these practices.

In Chapter Seven, curiously entitled 'Electronic "Snake Oil"' the authors investigate the extent of deceptive and misleading online advertising practices, identified in the previous chapter as a major problem for the online securities market. Like most forms of electronic theft, this type of acquisition is easily perpetrated from remote or untraceable locations, and includes non-delivery of products and services, pyramid schemes, provision of Internet services, and false or misleading advertisement of sexual services and 'miracle' health products. The defrauding of consumers online is remarkably easier than in the traditional marketplace, and the response from law enforcement bodies has been that of

8 Note 1 at 52.
9 Note 1 at 81.
10 Note 1 at 12.

hard regulation and rapid endorsement of preventative strategies. Globalisation is an important influencing factor in this area and emphasises the need for international cooperation of consumer protection bodies, since investigation and prosecution is becoming exceedingly difficult.

Chapter Eight deals with theft of intellectual property, a rapidly expanding and important area considering that 'copyright law has suffered the greatest impact from the information revolution'.[11] Digital technology permits near-perfect reproduction and rapid dissemination of print, graphics, sound and multi-media combinations, and the temptation to infringe others' copyrights so as to obtain material free of charge has proved irresistible to billions of people. The recent mass of MP3 litigation in America by the recording industry exemplifies the enormity of this widespread crime. An important question in this context is whether free distribution hinders artists' creativity, or rather increases availability and therefore popularity. Whilst there are impassioned defenders of the holders of these property rights, there are also many fighting for a liberal approach to intellectual property and maintain that such information should be free and available to all. In any event, the authors recognise that this is yet another area which requires legislative neutrality, as most traditional copyright laws were designed without any intention of their applicability in this area.

Increasing connectivity places companies at unprecedented risk of losing valuable proprietary information such as trade secrets. Interception technologies, hacking tools and surveillance equipment inevitably magnify this risk. In Chapter Nine the authors focus on industrial espionage, recognising that high staff turnover in big international companies also means increased accessibility and decreased trust. Frequently, employees or 'insiders' are the perpetrators of these crimes. Responses to industrial espionage are often aggressive; indeed, to be effective they need to be.

Chapter Ten focuses on the electronic misappropriation and dissemination of personal information through electronic means. Erosion of privacy in the digital age is a mounting trend, which threatens to transform our lives; increasing connectivity is accompanied by increasing vulnerability. The potential for theft of personal information, facilitated by digital technology of course, is greater than ever before. The challenge to legislators is to strike a balance between adequate protection mechanisms and controlled usage of personal information which has immense value for marketing and research purposes. The authors propose that the solution to this may be economic: individuals are far more likely to reveal personal information in exchange for monetary reward.[12]

Each of these Chapters represents a specific examination of a particular avenue through which crimes of acquisition can be perpetrated in the digital age, yet the authors do not attempt to give an exhaustive list and acknowledge the enormity of this area of the law. General themes which run through the book include the contested legal status of many 'new' crimes of acquisition, such as theft or misuse of personal information, industrial espionage and digital piracy. A diversity of responses is endorsed by the authors in relation to various types of crime, as the legal system alone is often incapable of providing a viable solution.

III. Recommendation

Electronic Theft: Unlawful Acquisition in Cyberspace is a comprehensive guide to the extent and magnitude of implications the digital age is having on our legal system and the industrial world. Computers have undoubtedly become a fundamental necessity to many aspects of our lives, and it is impossible to imagine a future without them. Yet in some

11 Note 1 at 131.
12 Note 1 at 177.

respects the Internet is a monster of our own creation which is fast stretching beyond our control. *Electronic Theft* canvases a fascinating range of issues relating to computer-related crime and highlights the importance of legal pluralism in minimising this type of crime in society. This book is essential reading for anyone interested in intellectual property and the implications of fast paced technological growth on the industrial world. The incidence of electronic crime is undoubtedly going to increase rapidly in the future as a result of the proliferation of electronic devices. Knowledge, awareness and self-regulation remain fundamental objectives in the quest to minimise such crimes which often threaten to compromise our way of life.