

Regulation of Electronic Theft

*Peter Grabosky, Russell Smith and Gillian Dempsey, **Electronic Theft**,
Cambridge University Press, Cambridge, 2001*

Reviewed by Daniel Stewart

Most definitions of theft involve the dishonest appropriation of property belonging to another with an intention to permanently deprive them of it (Bronitt and McSherry 2001:674). *Electronic Theft* however goes much further in describing the instances in which electronic material and media are involved in forms of unauthorised appropriation. Indeed, much of this book is about recognising new boundaries — in defining ways in which established crimes may be committed, in recognising new activities as criminal and deserving of regulation, and in the development of new conceptions of how that regulation may be achieved. This book attempts to describe the ways in which these boundaries are being shifted, and illustrates the challenges and opportunities facing regulation in this area.

As the book suggests (p. 2), ‘the fundamental principle of criminology is that crime follows opportunity, and opportunities for theft abound in the Digital Age’. Many of these opportunities are not new: electronic media often merely facilitates the carrying out of the forms of acquisition or extends the potential reach or effect of such activities. Thus the ability to steal funds and threaten disclosure of information is increased through the ability to access and manipulate their electronic storage. Similarly, conveying distorted or deceptive information is easier with increased access to new forms of communication and is potentially more profitable due to an increased audience. This book provides many, almost titillating, examples of how the increased reliance on electronic media and storage by private and government bodies has brought with it an increased exposure to fraud, extortion or theft.

Apart from increasing the potential efficiency of criminal activity, electronic media have also contributed to making intangible forms of property an attractive target. Unauthorised, or at least unpaid for, access to computer software, electrical, telephone or internet services has accompanied the development of these facilities, and in some cases required extension of the criminal sanctions available. However the real value of such services is the increased ability to communicate, manipulate and make use of information. The theft discussed in the book largely involves appropriating that ability as much as knowledge of the information itself. The theft of electronic funds often involves access to passwords or other forms of identification or security information, extortion is based on the ability to access information and make it public, deception is premised on ensuring there is inadequate access to or use of accurate information. Protection of the dissemination of information and relationships of confidence through intellectual property has taken on new importance.

Perhaps the most important area exposed through digital media is the privacy of personal information. The ability to collect, collate and take advantage of personal information has been dramatically increased through the large variety of electronic forums in which such information is being gathered. Such information can then be used to permit and encourage theft, provide the basis of extortion or increase the likelihood and value of deception. But it has also given rise to relatively new concerns about the value of anonymity and pseudonymity. Private profiles have become publicly accessible but are still inevitably incomplete and selective, which brings with it the erosion of autonomy and opportunities for discrimination, censorship and unjustified recrimination.

The flip side to any debate about privacy, however, is questions about enforcement, and the ability to identify and locate those who are carrying out regulated activities. Many of the criminal opportunities suggested by the development of digital technology stem from the possibility of at least apparent anonymity. Sophisticated techniques may sometimes track down individuals who break in to computer systems or communicate threats, although the global nature of electronic media means this may often require cooperation between regulatory agencies and countries. But sophisticated techniques are often not practical to prevent less targeted forms of acquisition through deceptive conduct or the misplacing of trust.

Questions of enforcement are just some of the questions involved with the regulation of electronic theft. *Electronic Theft* examines this regulation through the lens of legal pluralism, drawing on an increasing body of scholarship that illustrates regulation as the relationships between various institutions, public and private. Criminal sanctions and government regulation are only two of the influences on behaviour that may be directed towards achieving a regulatory outcome. While traditional forms of public prohibitions and penalties continue to play a role, the government has also recognised the potential effects of providing information and facilitating, perhaps even enforcing, the development of guidelines and codes of conduct. The potential profitability that comes through establishing a reputation and trust in the digital environment has suggested a growing reliance on competitive forces and self-regulation through voluntary codes of conduct and forms of certification. Similarly, many of the features of the new technology that create the opportunities for abuse, such as its accessibility and anonymity, also provide access to encryption and detection technology and other security measures that can help limit vulnerability to electronic crime.

It is in describing how government, non-government and individual actions have all been used to regulate the potential for electronic theft that this book makes its most important contribution. Through pulling together examples from various primary and secondary sources on a wide variety of topics, the authors illustrate the way in which various elements of the conduct being discussed is regulated through one or more of the mechanisms presented.

For example, the chapter on industrial espionage sets out the way in which digital storage, access and communication increases the vulnerability of organisations to breaches of confidence. Outsourcing of technological functions

or specialisation of employment roles increases any exposure. The chapter summarises the way in which relationships of confidence can be protected through the courts, and in some jurisdictions such as the US through criminal sanctions, but emphasises how organisations themselves have the motivation and the means to better establish and protect confidential information. Thus compiling an inventory of confidential information, restricting access, contractual clauses, marking information as confidential and the selection, screening and socialisation of those with access can all assist in maintaining the value of confidential information. But within any organisation this can not be an unqualified objective, and other sometimes-conflicting goals such as efficiency, trust, morale and creativity also have to be sought. The chapter also briefly considers some normative issues about the extent to which confidential information should be protected, given the possible interference with the flow of information available to others and the creation of value through contextualising the information. However, the extent to which these issues can be resolved or even investigated in a principled way given the present interaction of the plurality of regulatory mechanisms is largely beyond the scope of the book.

Clearly the examples presented by the authors are not intended to be comprehensive or detailed. Many more specific forms of analysis are referred to in the text, including some important contributions by one or more of the authors. However, those presented are sufficient to illustrate a number of issues that remain to be explored before any normative analysis of this pluralistic approach to regulation can be undertaken. In discussing legislative responses the authors suggest the need for technologically neutral language and point out the inevitable delay in reactive legislation, but do not explore the pro-active ability of principle-based rather than proscriptive legislative drafting. The capacity of other forms of judicial if not criminal redress, such as trespass and assault, to adapt to digital environments is also not considered in detail. The difficulties of jurisdictional boundaries are pointed out, but while there is clearly scope for greater cooperation among regulatory agencies, the achievements so far, further impediments and the possible disadvantages of extra-territorial legislation are not always consistently addressed. The relationship between privacy and enforcement, and how boundaries can meaningfully be drawn between them, is not discussed to any great extent.

Any book that draws on the rapidly changing nature of its subject matter for some of its conclusions is itself vulnerable to changes in the regulatory and technological landscape. Since the book was written the *Privacy Amendment (Private Sector) Act 2001* (Cth) has been passed, the Australian High Court has seemingly opened the door to a more general right of privacy being developed in Australia while limiting its application to corporations (*Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) HCA 63) and the first charges have been brought in the US for circumventing a technological protection measure. The authors could consistently have used these and many other recent events within their discussion, but the examples also emphasise the unresolved issues inherent this area. The difficulties of establishing limits for privacy

protection and accountability of the means of enforcing those provisions, the uncertain role of the courts in responding to new technologies and protecting relationships of confidence, and what limits should be placed on the ability of individuals and organisations to prevent access to information and expression are issues that are merely raised by the authors.

Electronic Theft highlights the inadequacy of trying to examine the issues confronting regulation of electronic media without considering the interaction of the various forms of regulation involved. As the authors suggest, there is much to be done in cataloguing the various forms of institutions, public and private, and the influence that they have. 'We must now inquire what institutional form, or, even more appropriately, what blend of institutional forms, is best suited to a given task' (p. 206). Perhaps even more important is the development of new methods to determine the effects, limitations, accountability and equity of those blends. *Electronic Theft* may not push many boundaries of research or analysis, but it clearly illustrates new opportunities for the regulation of electronic technology.

Reference

Bronitt, S. and McSherry, B. (2001) *Principles of Criminal Law*, LBC Information Services, Pymont, N.S.W.

Daniel Stewart is a Lecturer in the Faculty of Law at the Australian National University.

