CHAPTER 1

Theft and Cyberspace

The convergence of communications and computing has begun to transform the world. Although this transformation has mainly been located in Western industrial societies, its effects are beginning to be felt globally. As recently as 1990, few people could even envisage what has since come to be known as the World Wide Web, and the possibility that an ordinary individual could communicate with millions of others seemed remote. More traditional telecommunications offered little assistance – without 'the phone book', obtaining a person's telephone number necessitated a laborious, often time-consuming, and increasingly costly call to Directory Assistance. Who would have imagined a desktop link to an electronic white pages, searchable by typing in the name or address of the subject? The idea of making near instantaneous copies of vast amounts of text, much less video, sound and multimedia, was the stuff of science fiction. Our ability to gather and to disseminate information now vastly exceeds our capacity to absorb and to analyse it.

The enormous increase in human potential brought about by the democratization of digital technology, however, has its downside. Information is now being disseminated in such volume that understanding and control by any individual is implausible. Today cyberspace is perceived to be teeming with advertising, vice and (for the time being at least) American content, and critics all over the terrestrial world lament the erosion of traditional values they consider worth keeping.[1]

Beyond its contribution to culture wars, increasing connectivity has been, and will continue to be, accompanied by unprecedented opportunities for crimes of acquisition. The extent to which business transactions are being conducted electronically is increasing enormously. Forrester Research estimated that global business-to-business online commerce could amount to US$2.7 trillion by the year 2004, while the Gartner Group puts the figure closer to US$7 trillion in 2004 (*San Jose Mercury News*, cited in O'Brien 2000). One may expect the growth of electronic commerce to be reflected

in the growth of electronic misappropriation. The fundamental principle of criminology is that crime follows opportunity, and opportunities for theft abound in the Digital Age.

This book will review some of the major crimes of acquisition involving digital technology as the instrument of theft, or crimes involving information as the object of theft. Many of these crimes are not 'new' – rather it is the medium of theft, the transjurisdictional reach of the thief, and the speed with which a transaction may be executed, that are without precedent. Chapters 8 to 10 also discuss some forms of misappropriation whose legal status is contested or evolving, such as the commercial acquisition of personal information, industrial espionage, and various activities relating to digital piracy.

The Criminology of Electronic Theft

Cohen and Felson (1979) observed that all crime can be explained by the intersection of three variables: a supply of motivated offenders, the availability of suitable targets, and the absence of capable guardians – someone to mind the store, so to speak. Crime reduction strategies may be directed at each of these factors: reducing an offender's motivation through moral suasion, or failing that, the deterrent effects of prosecution and punishment; making it more difficult to offend through target hardening; and increasing surveillance in order to enhance the possibility that illegal activities will be detected.

These basic principles of criminology apply to computer-related crime no less than to motor vehicle theft or to shoplifting, and they will be evident throughout this book. As we will note, not all of these factors are amenable to control by governments alone. It follows, therefore, that a variety of institutions will be required to control computer-related crime.

The motives of those who would commit computer-related crime are diverse, but hardly new. Computer criminals are driven by time-honoured motives, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste 'forbidden fruit'. The ability to make an impact on large systems may, as an act of power, be gratifying in and of itself. The desire to inflict loss or damage on another may also spring from revenge, as when a disgruntled employee shuts down an employer's computer system, or from ideology, as when one defaces the web page of an institution that one regards as abhorrent. Much activity on the electronic frontier entails an element of adventure – the exploration of the unknown. The very fact that some activities in cyberspace are likely to elicit official condemnation is enough to attract the defiant, the rebellious, or the irresistibly curious. Given the degree of technical competence required to commit many computer-related crimes, there is one other motivational dimension worth noting here. This, of course, is the intellectual challenge of mastering complex systems. None of the above motives is new. An element of novelty, however, resides

in the unprecedented capacity of technology to facilitate the ability of individuals to act on these motives. Our focus in this book is on theft (in the general sense of unlawful acquisition), so the first of these will figure prominently in the chapters that follow. But there is often more to theft than mere greed, and the reader will notice that many of the illegalities discussed below flow from a variety of motives.

While motives tend not to change, the variety and number of opportunities for cybercrime are proliferating. The exponential growth in connectivity of computing and communications, and their applications to electronic commerce, increase both the number of prospective victims of computer-related crime and the number of prospective offenders. As the Internet becomes increasingly a medium of commerce, it will also become increasingly a medium of fraud.

The third basic factor that explains computer-related crime is the absence of a capable guardian. Capable guardianship has evolved over human history, from feudalism, to the rise of the state and the proliferation of public institutions of social control, to the postmodern era in which employees of private security services vastly outnumber sworn police officers in many industrial democracies. Here again, it may be instructive to compare computer-related crime with more conventional types of crime.

Guardianship against conventional crime involves preventive efforts on the part of prospective victims, contributions by members of the general public or commercial third parties (such as insurance companies and private security services), and the activities of law enforcement agencies. Indeed, it is often only when private efforts at crime prevention fail that the criminal process is mobilized. So it is that owners of motor vehicles are encouraged to lock their vehicles at all times, that insurance contracts may offer premium discounts for crime prevention measures such as theft alarms, and that some car parks have video surveillance or private security guards in attendance. Often it is only when these systems fail that the assistance of law enforcement is sought. So it is in cyberspace as well.

Law and Technology

It has become trite to suggest that law and policy often fail to keep pace with technological change. The most robust legal systems are those that can adapt to changing technological circumstances without continuing repeal and reenactment of legislation – so-called technology-neutral laws. By contrast, in some jurisdictions around the world, the existing law of theft has only limited application to intangible property. For instance, at common law in both England and Australia, larceny is the unlawful taking or conversion of anything capable of being stolen (Fisse 1990: 197). Because larceny could only be committed in respect of something capable of being asported (physically removed), the intangible nature of items such as telephone services rendered successful prosecution as larceny impossible. For instance, in *Low v. Blease*

([1975], 119 Sol J 695 Crim LR 513), the English Queen's Bench Divisional Court held that electricity does not constitute property within the meaning of s. 4 Theft Act 1968 (Eng). Accordingly, electricity could not be stolen by switching on the current.

This definitional problem has largely been resolved in Australia by the introduction of various statutory definitions of theft which include intangible items of property such as electricity, thus bringing the unauthorized use of a telephone service within the definition of theft – at least of the electricity consumed (in Australia, see *Crimes Act* 1900 [NSW] s. 154C; *Criminal Law Consolidation Act* 1935 [SA] s. 154; Queensland Criminal Code s. 408; Western Australia Criminal Code s. 390; Tasmanian Criminal Code s. 233). But the value of the electricity used in a telephone call is not necessarily representative of the value of the service being provided, so more specific criminal regulation is required.

Protection for intangible property, however, has typically centred on laws proscribing the obtaining of various forms of advantage by deception. For example, in Australia, section 29A of the *Crimes Act* 1914 (Cwlth) proscribes (with a maximum sentence of ten years) obtaining from the government with intent to defraud or by false pretence 'any chattel, money, valuable security or benefit'. The use of such laws to prosecute digital theft is by no means simple, however. Prosecuting larceny in the area of computer crime is complicated by the necessity of proving that the property was taken without the victim's consent. Where a computer alone, rather than a human actor, has been deceived, this lack of consent can be difficult to establish (see Grabosky and Smith 1998). In the Australian case of *Kennison* v *Daire* ((1986) 160 CLR 129, 20 February 1986), the High Court of Australia upheld the conviction of a man who had exploited a loophole in the Savings Bank of South Australia's automated teller machine (ATM) system. Kennison had closed his account with the bank but retained his card, one of the conditions of use of which was that his account was in sufficient credit to accommodate a withdrawal. The ATM had been programmed to permit up to $200 to be withdrawn by any person using a card and its correct personal identification number (PIN). Knowing his account to be empty, he used the card while the ATM was not connected to the bank's central computer. The conviction was upheld because Kennison had acted fraudulently with intent permanently to deprive the bank of $200. Kennison's argument, that the bank had consented to the withdrawal of the money by providing a machine that permitted the transaction to take place, was rejected.

To avoid any potential for misunderstanding, some risk-averse jurisdictions now include deception relating to a computer system expressly within the terms of financial crimes. For example, section 17.1 of the Australian Model Criminal Code defines deception as 'conduct by a person that causes a computer system or any machine to make a response that the person is not authorised to cause it to do'.

The chapters that follow examine a wide variety of circumstances in which benefits are able to be obtained illegally and improperly by individuals making use of digital technologies. Some clearly fall within traditional conceptions of theft; others may give rise to civil or administrative consequences, while others again may have primary relevance to personnel management in the workplace. Using a government computer for personal use during working hours might, for example, technically amount to theft, but it is unlikely that a criminal prosecution would be undertaken; rather, the matter would probably be dealt with internally. Transferring $1 million from a business bank account to a private individual's personal account, however, would usually (though not invariably) result in the matter being reported to the police and a prosecution ensuing. Economic crime in cyberspace, therefore, comprises a diverse range of behaviour with a variety of legal and social consequences.

Theoretical Context

It has long been recognized that the criminal justice system is a very imperfect means of social control, and that effective crime prevention requires the contribution of families, schools, and many other institutions of civil society. Moreover, as environmental criminologists and exponents of situational crime prevention will attest, the design of public space and the 'engineering out' of criminal opportunities can make a significant contribution to crime control.

The same principles apply to white-collar and sophisticated crime. It is now also increasingly acknowledged that effective business regulation is beyond the capacity of governments alone and requires the involvement of many other institutions. Two decades ago, Bardach and Kagan (1982: 33) maintained that most regulation was already 'in the hands not of government officials but of the myriad individuals employed in the private sector'. Teubner (1983) has spoken of how, instead of imposing direct substantive controls on behaviour, states might structure mechanisms for self-regulation. He refers to the fostering of a 'regulated autonomy' based largely on private orderings. The state facilitates the development of these self-regulating systems rather than engaging in direct intervention. Indeed, in some areas the state plays an even more passive role, deferring to private institutions. A decade later, Ayres and Braithwaite (1992) envisaged a tripartite regulatory system, embracing monitoring by government agencies, self-regulation by companies and industry associations, and surveillance and lobbying by public interest groups. These three types of institution would play an active regulatory role, strengthening the self-regulatory initiatives of regulated industries and complementing the activity of government regulatory agencies. Shearing (1993) views regulatory systems in an even wider perspective, speaking of 'regulatory space' as comprising a variety of institutional orderings and

regulatory mechanisms. Grabosky (1994, 1995a) has discussed the quasi-regulatory activities of commercial institutions, observing that in certain settings the influence they have wielded was far in excess of what government agencies were able or willing to mobilize. In some instances, resources outside the public sector may be consciously harnessed by government in furtherance of regulatory objectives. In other cases, institutional orderings may arise more or less spontaneously, but with significant regulatory effects. The prevention of crimes of acquisition in cyberspace provides one of the best illustrations of how this diversity of regulatory activity may function.

This notion of legal pluralism provides the theoretical basis for this book. It is a perspective that sees law as having its analogues in various other social institutions, or where official and unofficial forms of ordering coexist in an interactive relationship (Merry 1988). Observers as long ago as Ehrlich (1912) began to see law as but the top stratum from which a web of quasi-legal rules and controls ordered everyday life. More recent scholars began to focus on the relationship between state law and private forms of social control and conflict resolution (Fitzpatrick 1984). Today there is growing realization that the capacity of the state to control both individual and corporate behaviour has limits. The nature of digital technology, combined with the ambivalence of many governments about the extent of their role in the economy and society of the twenty-first century, makes legal pluralism a useful lens for viewing the ordering of cyberspace.

One of the seminal thinkers of the late twentieth century, Michel Foucault, made a number of perceptive observations about government and society, two of which are especially germane to this book. Although he made them before the world entered the digital age, they apply no less to matters of social control in cyberspace than they do to terrestrial affairs. The first of these notes the trend towards a less central role for the state and for law in the ordering of relationships. Foucault sees overt enforcement of law as but one element in what might be called a web of constraint, some strands of which are barely discernible, and many of which are non-governmental. He refers to law as 'partial' (1980: 141) and 'not what is important' (1979: 13), observing that the real practice of government was not the imposition of law but rather working with and through the constellation of interests, institutions and interpersonal relations that are part of civil society. Burchell (1991: 127) adds further texture to Foucault's outline when he refers to 'governing in accordance with the grain of things'. Foucault saw power in modern society no longer centralized in the Sovereign, but rather dispersed. He uses the terms 'capillary power' and 'micro-physics of power' (Foucault 1977: 139) as metaphors for the partial displacement of law by other orderings. At the same time, Foucault acknowledges that law is not isolated from these microstructures of power but rather interacts with them. In this way he echoes Donald Black's (1984) theory that law varies inversely with other forms of social control.

The second of Foucault's observations which is of concern to us here is the relationship between knowledge and power. His celebrated work *Discipline and Punish* (an unfortunate translation of the original *Surveiller et Punir*) (1977) describes the transition from physical punishment as an expression of political power to surveillance and control through observation, record-keeping, monitoring and inspection. These two basic ideas converge. Not only are the surveillance capabilities of governments in Western industrial societies without precedent, but non-state actors, from large multinationals to insurance companies to parents, are all able to command formidable knowledge, and thereby control, over individuals. Chapter 10 of this book will cite some examples of the knowledge and power held by commercial interests.

So it is that states often seek to co-opt private institutions in furtherance of law enforcement and regulatory objectives. The assistance of Internet service providers (ISPs) can be helpful, or even essential to the investigation of computer-related crime. At the same time, we see private institutions seeking a market niche. A vast information security industry has grown up to complement, if not largely eclipse, whatever role government law enforcement and regulatory agents may wish to play. Rose and Miller (1992) refer to this as 'governing at a distance', using 'new technologies of government' that harness energies residing outside the public sector to advance public policy.

This line of argument has been popularized in the very influential North American book *Reinventing Government* (Osborne and Gaebler 1992). Recognizing that government as traditionally configured has its constraints and limitations, the authors advocate that governments adopt the role of facilitator and broker rather than that of commander. They suggest that governments 'steer' rather than 'row', and that they structure the marketplace so that naturally occurring private activity may assist in furthering public policy objectives. Osborne and Gaebler (1992: 280) use the term 'leverage' to refer to this approach.

The notion of legal pluralism is very salient in the digital age, where the limits of the state have become increasingly apparent. Throughout this book, we will see examples of non-state institutions and market forces exercising power no less coercive than that available to governments.

Lessig argues that behaviour in cyberspace is already controlled primarily not through legislation but through other codes: the programming and architecture of information systems. To Lessig, technology, not law, is the predominant regulatory institution of cyberspace. 'Code can, and increasingly will, displace law as the primary defense of intellectual property in cyberspace.' His emphasis is on 'private fences, not public law' (1999: 126). He observes a shift in effective regulatory power 'from law to code, from sovereigns to software' (1999: 207).

Just how 'code functions as law' is illustrated by the unique identifier that is created with every MS Word document, and by digital content (text, sound, visual, or multimedia), which can be programmed to degrade if and when it

is copied. Lessig (1999: 160) contends that protection of privacy will be achieved through systems that will allow users to 'articulate their preferences and negotiate the use of data about them'. Similarly, Rochlin (1997: 13) refers to the 'hegemony of design' as constituted by 'new modes of organizational control, indirect and diffused', disguising 'the imperatives of compliance as no more than a set of operating rules'.

Much as Molière's Bourgeois Gentilhomme, who remarked that he had been speaking prose all of his life without realizing it, Lessig and Rochlin speak the language of legal pluralism. Code, market forces, and to a lesser extent social norms, have eclipsed law as the major institutions of social control in cyberspace. As Foucault did, they regard the relationship between these various elements as interactive.

Transformation of Social Relations

It was not that long ago, even in the industrialized world, that commerce was largely based on personal relationships, deals were sealed with a handshake, and 'a man's word was his bond'. The Internet has indeed brought about significant changes in human interaction. Instead of a face-to-face relationship with our local bookseller, we are just as likely to deal with a digital bookseller such as Amazon.com. But trust is the foundation of commerce in cyberspace, just as it is on the ground. The difference is that whereas in real life trust is based on personal relationships, online trust is based on confidence in processes. The establishment of trusted processes in cyberspace is the key to commercial success, and so it is that online merchants seek to create an environment in which a prospective customer can be relaxed and confident about any prospective transactions.

Although commercial transactions in cyberspace are completely depersonalized in the sense that one does not deal directly with a sentient being (other than in some real-time interactive environments), technology now enables an online bookseller to 'remember' precisely what books you have been buying, at what price, and when. This may be advantageous, as when you are automatically advised of new publications on a topic that appears to have interested you in the past, but it may be less so if information is disseminated to other merchants, to government agents, or to anyone else with an interest in your private life.

As we will see in Chapter 6, ordinary investors are now able to buy and sell shares online without dealing through intermediaries such as underwriters, brokers and investment advisers. While this may enhance the efficiency of securities markets, it also provides opportunities for criminal exploitation. But the fundamental criminality is still reducible to the basics: misrepresenting the underlying value of a security at the time of the initial public offering; or market manipulation during secondary trading of a security, through the dissemination of false information, or by engineering a deceptive pattern of transactions to attract the attention of the unwitting investor.

Computing and communications technologies make such activities both easy to carry out and difficult to detect.

The issue of trust surfaces again in the context of electronic cash, and the possibility of 'private money'. Before the nationalization of currencies a century ago, many individual banks issued their own notes. Banks differed in terms of their viability. Some issued currency that turned out to be worthless, while others' paper was 'as good as gold'. To the extent that the nature of money changes in the digital age, trust in private institutions will become even more salient.

The Limits of Government

Even where the law, through interpretation or amendment, comes close to keeping abreast of both technology and the 'disintermediation' that characterizes new commercial relationships, its use may be limited. Despite the fact that new technologies allow us to do more things more quickly than ever before, they pose challenges to governments which are not unlike those that plague many other areas of social and political life.

Perhaps the most prominent of these entails the limits of the law or indeed, government efforts generally, as instruments of public policy. To be sure, digital technologies enable a degree of surveillance that would do George Orwell proud. But not all states today are preoccupied with social control, either in cyberspace or on the ground. Those that are often realize that control can be gained or kept at a prohibitively high cost in terms of the contentment and creativity of the public and the health and vibrancy of the economy.

As we will see throughout the chapters that follow, many governments lack the capacity to control behaviour in cyberspace, on the part of their own citizens or those of other countries. This is also reflected in the limited ability of governments alone to protect personal property in the digital environment. Law enforcement resources are constrained, and there are relatively few skilled computer crime investigators and forensic accountants. The rarity of suitably trained investigators generates competition for scarce investigative resources. This effectively forces a choice between concentrating efforts on protecting property interests or focusing on areas that have attracted greater concern from the general public such as Internet child pornography and the information to facilitate the illicit production of drugs or explosives.

As far as traditional property crime is concerned, there are, in terrestrial space as well as cyberspace, very real limits to what the state can do to protect a citizen's assets. In English-speaking societies at the very least, the capacity of public police is now acknowledged to be limited. Most victims of residential burglary are aware that they stand little chance of recovering their lost possessions; they harbour few illusions that 'their' offender will eventually be brought to justice. The role of the police is often limited to that of legitimizing insurance claims and providing a few kind words (and perhaps

some crime prevention advice) to the victim. Individuals are, to an extent that few wish to acknowledge openly, their own best chance of crime prevention. The result is that those who can afford the expenditure tend to acquire sophisticated alarm systems, live in 'gated' communities, and fit their motor vehicles with sophisticated locking and disabling devices.

Compounding this is the global nature of cyberspace, where crimes may be committed over vast distances and across national frontiers. Although it may be legally possible to prosecute offenders who are alleged to have committed electronic theft in various jurisdictions, even internationally, significant problems may arise in detecting such illegality and in proving allegations successfully. As long ago as 1986, an OECD paper discussing the problems of prosecuting international computer crime observed:

> For international cooperation to be effective there must be agreement as to what is criminal at the national level and what sanctions should attach to a given offence. Extradition treaties need to be adequate to deal with offences committed in various jurisdictions. There are also problems of differing laws as to search and seizure, service of documents and the taking of testimony or statements of persons. (OECD 1986: 68)

These issues are no less problematic today than they were at the dawn of the digital age. The legal challenges lie not so much in attempting to create uniform legislation internationally, which is unlikely ever to occur, but rather in ensuring that individual countries are able to prosecute those offenders and offences that occur within their own geographical boundaries.

The necessity of self-reliance in crime control is no less in cyberspace than in one's terrestrial neighbourhood. This raises the fundamental issue of what forms of cyber-theft are sufficiently threatening to warrant the full application of the criminal law, and which might be more effectively and efficiently controlled by prevention or by conferring enforceable civil property rights on the 'owner'.

New Instruments of Social Control in the Digital Age

Just as technology has brought about unprecedented opportunities for crime, so it has wrought new means of preventing and controlling crime. Security technology, including mechanisms of access control and authentication, are the equivalent of deadlocks and back-to-base alarm systems for safeguarding terrestrial property. It is these technologies of self-help, rather than any state presence, that will provide the basis for secure electronic commerce.

As an alternative to conventional law enforcement, governments may seek to confer entitlements and allow citizens to enforce their own rights. Private redress is of course not a perfect solution. Within a developed society, access to justice is unevenly distributed. Microsoft can protect its interests much more effectively than most private individuals can protect their interests. The