Cyber Criminals on Trial

Russell Smith, Peter Grabosky and **Gregor Urbas** look at the challenges of criminal cases involving cybercrimes.

Over the past three decades, cybercrime has come a long way. The earliest cases were directed at telecommunications and electronic accounting systems with curiosity or the challenge of defeating security protocols as the usual motives (Grabosky and Smith 1998, Grabosky, Smith and Dempsey 2001). Very few instances were prosecuted, often owing to investigative and legislative weaknesses, resulting in those involved rarely appearing before the courts, and almost never going to prison.

More recently, cyber criminals have extended their horizons and, driven by economic and political motives, have committed a wide variety of crimes and caused considerable hardship globally—both financially and personally. Following legislative reform, more and more cases have entered the judicial process. These cases have posed some familiar challenges for prosecutors and judges, but also created many new ones.

In *Cyber Criminals on Trial*, we examined some 240 publicly-reported cases involving cybercrimes that have been determined in the courts—principally in Australia, the United Kingdom, the United States, Canada, New Zealand and Hong Kong. Of these, 164 cases involved a conviction or the accused pleading guilty and sentencing outcomes were available in respect of 139 of these (Smith, Grabosky and Urbas 2004).

Although the research encompassed cases adjudicated in courts from around the globe, the manner of responding to cybercrime in different jurisdictions has many common features, as offences of this nature are often committed for similar motivations of greed, curiosity, or revenge. Offenders from different countries also tend to have similar characteristics, often being well-educated, middle-class, young and male. As digital technologies become more prevalent, however, it is to be expected that this profile will alter and that individuals from different social and educational backgrounds will become involved—as too will female users of digital technologies.

Three principal questions are addressed in the book.

Does cybercrime raise unique problems?

First, we found that the prosecution and judicial disposition of cases involving cybercrime does, indeed, raise certain considerations that make these cases different from those involving conventional crime. Prosecutors have been presented with some truly novel arguments in these cases, such as the computer addiction defence. Difficult and unresolved evidentiary issues have also been raised concerning the admissibility of evidence obtained when hard drives have been copied and both relevant and irrelevant data are unable to be differentiated.

On the other hand, many cases raise conventional issues that face prosecutors in other complex cases involving financial fraud or dishonesty. It seems, for example, that a similarly high proportion of offenders plead guilty in cybercrime cases, making it unnecessary for full and protracted criminal trials to be conducted. Were this not the case, the difficulties associated with prosecution and trial would be exacerbated greatly.

Over the last decade, a number of legal problems have emerged which have created difficulties for the successful prosecution of cybercrimes. Their nature has sometimes been remarkably simple, such as the omission of laws that proscribed deception of computers as opposed to human actors—thus making ATM-related fraud sometimes difficult to prosecute (Kennison v Daire (1986) 160 CLR 129). As these problems grew, a variety of solutions was adopted. This has created problems itself as laws are now variable and conflicting across different jurisdictions.

The problem of cybercrime for prosecutors, however, needs to be placed in context. Although cybercrimes often involve voluminous information and data trails, so do other crimes. Similarly, prosecutors have had to deal with international criminals for many years in cases involving piracy on the high seas, illegal immigration, drug trafficking, and smuggling of contraband, not to mention serious fraud. Although these cases can often be protracted and slow, the mere presence of computers in the commission of the offence can hardly be said to raise new matters of jurisdiction and procedure with which courts are unfamiliar.

Are there differences of approach between jurisdictions?

It appears that the prosecutorial and judicial responses to cybercrime have been remarkably similar in North America, Britain and Australasia. Where differences between these countries exist, they have largely arisen from the presence of other legislative and procedural factors—rather than the fact that computers are at stake. For example, the different

sentencing regimes that exist in the United States with its sophisticated system of sentencing guidelines, and that which exists in the United Kingdom and Australia where appellate court guideline judgments exist (although not, as yet, for cybercrime cases), is likely to be more responsible for any perceived differences in sentencing practices in cybercrime cases. As our brief consideration of the sentences imposed in child pornography and hacking / vandalism cases showed, there seem to be few obvious differences in the ways in which courts in different countries approached these matters—all generally treating the possession and distribution of child pornography as warranting more severe sentences than cases of hacking and computer vandalism.

Are cybercrimes treated more seriously than conventional crimes?

There is little conclusive evidence that the presence of computers in the commission of crime enhances the severity with which courts deal with those convicted of these crimes. Of course there are instances of extremely serious offences being facilitated through the use of computers, such as the possession and dissemination of child pornography and the spread of malicious code which can disable computers across the globe in hours or days. But the fact that digital technologies have been used does not seem to result in increased sentences being imposed.

In fact, in some cases, the commission of crimes electronically could be said to decrease the seriousness with which courts view this conduct. Stalking a victim through the use of e-mail, for example, could be said to impose less of a threat then actually waiting for one's victim outside their house. Similarly, engaging in sexually provocative discussion with a child in a chat room, would seem to be less serious than engaging in physical sexual relations with a child—although some sexual encounters can be initiated on the internet.

In the end, cases that come before the courts in the twenty-first century are likely to demonstrate many aspects of life as those of us in developed nations currently know it—activities that are heavily dependent on digital technologies; activities that involve participants in multiple countries; and activities that take place with an undue emphasis on speed. Prosecutors and courts need to be equipped with training and resources to respond effectively to such cases which, it may confidently be predicted, will become a regular feature in daily court listings. In order to maximise the efficiency of judicial processes, and to guard against the problem of history repeating itself, prosecutors and judges need to be made aware of the latest cases immediately they come to light. Technology, which itself is deeply involved in the commission of modern crimes, it seems, will provide the best means of achieving such an objective. A century ago, the philosopher Santayana said: "those who cannot remember the past are condemned to repeat it." In today's digital environment, it may be said of prosecutors and judges that those who fail to anticipate the future are in for a rude shock when it arrives.

■

Russell Smith *is Principal Criminologist at the Australian Institute of Criminology.* ***Peter Grabosky*** *is Professor in the Regulatory Institutions Network at the Australian National University and a Fellow of the Academy of the Social Sciences in Australia.* ***Gregor Urbas*** *is a Lecturer in Law at the Australian National University.*

References

Grabosky, P. N. and Smith, R. G. (1998), *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Transaction Publishers, New Brunswick / Federation Press, Sydney.

Grabosky, P. N., Smith, R. G. and Dempsey, G. (2001), *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

Smith, R. G., Grabosky, P. N., and Urbas, G. F. (2004), *Cyber Criminals on Trial*, Cambridge University Press, Cambridge.