Company Lawyer

2002

E-commerce, business and crime: inextricably linked, diametrically opposed?

Robin McCusker

Subject: Commercial law. **Other related subjects:** Criminal law. Information technology

Keywords: Computer crime; Computer security; Electronic commerce

***Comp. Law. 3** This paper contends that the e-commerce revolution is a doubleedged sword and that the sharpness and keenness of its blade remains largely untried and seriously underestimated. The clamour for and desire to travel on the internet superhighway has overtaken the issue of whether it is wise to do so. The business community and the world's governments have concerned themselves with the fact that they can and, more probably, must engage in world trade via the internet. They have not dealt appropriately with the question of whether they should so engage and furthermore, they have engaged without considering, evaluating and containing the potential consequences of doing so.*

Ging argues that "[a]s internet companies have plunged headlong into the commercial exploitation of the web, the dangers of fraud to them and their customers have been all but forgotten".[1] To have devised adequate protection within websites for businesses and banks would arguably have led to lengthy delays during which other, less scrupulous competitors might have obtained a market advantage. Business's primary motivation is the creation of profit, and the delay caused by implementing protection for consumers simply reduces that profit margin. In light of the actual and potential growth of the internet, and of the security issues associated with it, the belief system of e-businesses needs to be grounded more firmly in pragmatic reality and less in a profit-driven utopia. In fairness to e-businesses, however, the desire to react unilaterally and ethically to actual or potential threats will invariably be overtaken by a stronger desire to remain competitive within the cyber-business world.

Cerfnoted[2] that the number of internet users grew from 13 million in 1994 to more than 300 million worldwide in 2000. In terms of the revenue that might be generated by on-line shopping, Jupiter Communications estimated[3] that the revenue would increase from US$0.7 billion in 1996 to US$17 billion by 2000 and to US$41 billion by 2002.

The Criminal Investigation Department of the Federal Bureau of Investigation (FBI) noted,[4] following Operation Investnet, that the number of internet users reached 61.4 million in the United States in 1998 and it estimated that that number would grow to 200 million by 2000. It noted that the number of websites was doubling every 37 days and that more than 50 per cent of all U.S. households would have access to the internet by 2003. The University of Texas at Austin's Center for Research in Electronic Commerce noted[5] that the internet economy supported an additional 650,000 jobs in 1999 and that internet revenues increased to US$2.5 trillion. The Center noted, in addition, that the internet economy now supports 2.5 million workers.

Finally, the Gartner Group estimated[6] that American e-tail sales would exceed US$29.3 billion in 2000. That would represent an increase of 75 per cent over 1999's US$16.8 billion in on-line sales which was in itself an increase of 157 per cent on 1998 sales. The Gartner Group further estimated that e-tailing would grow to account for between 5-7 per cent of total retail sales in North America by 2004 from the 1 per cent it represented in 1999.

There is, in short, a recognised, marked and ever-increasing growth in e-commerce, although some commentators have argued that the internet bubble is about to burst. Bywater, for example, noted that "[m]ost dot.coms are operating a frighteningly short-term policy: start the company, get the banner advertising to tide them over, get the hit-rate high enough to build the hype, use the hype to attract the venture capitalists, take the money, and retire".[7] Although this view might be deemed somewhat cynical and exaggerated, it has perhaps been borne out by the rapid decline in stock market prices for dot.com companies and by the decreasing interest or faith in them being expressed by consumers. The stock market meltdown in the United States in April 2000 saw the Dow Jones index falling by 616 points (5.6 per cent) in one day and the infliction of widespread suffering among internet companies as a consequence. Bill Gates' Microsoft stock value was cut by US$11.1 billion and Jeff Bezos, the founder of Amazon.com (regarded, perhaps, as the litmus test of the potential of e-commerce) lost

US$2.4 billion. Even the debut share value of the much-hyped Lastminute.com fell from a floatation peak of 487.5p per share to 240p per share soon after. Whether cynical or not, Bywater's general contention that "[t]his isn't the way to build a commercial or indeed cultural infrastructure"[8] remains sound. The distinction between the media's view of the stock collapse[9] and the more pragmatic business view that the dot.com companies had simply been over-valued from the outset and that they were simply suffering a dip rather than an all-out collapse, is not necessarily the issue. The fact is that dot.com companies have shown themselves to be fragile. The apparent fragility of ***Comp. Law. 4*** the shares in dot.com companies will have a heightened resonation with consumers if the security of the information held by those companies is at all suspect. *Security breaches,* therefore, may well cause the bubble to burst.

In this regard, it was revealed recently by ZDNet US[10] that in January 1999 an individual stole information on more than 485,000 credit cards from an e-commerce site and then stored them on a U.S. Government agency's website. The credit card companies notified financial institutions but many of the accounts remained, and remain, open because the banks neither closed the relevant accounts nor alerted the customers of the theft. Indeed, Visa officials ordered a "spot check" on 50-100 accounts and then decided that no further action was necessary. More worrying than this, perhaps, is the fact that the theft of information from the 485,000 credit cards had only been discovered by chance when a web administrator (employed by the relevant and unnamed government agency) noticed that a large amount of computer memory was being utilised. Upon further investigation, the employee found the file containing the missing information. This theft, although apparently perpetrated in January 1999, was only revealed in March 2000. Ironically, in November 1999 Visa noted[11] that, although on-line transactions constituted only 2 per cent of its overall business, almost half of the complaints levelled against the company were derived from on-line transactions. A report from e-commerce solutions firm "Cybersource" noted that e-commerce firms were reporting that up to 25 per cent of on-line transactions were fraudulent, the average being 5 per cent.[12] In January 2000, the U.K. Government's official crime figures revealed that internet fraud and forgery had increased by 29 per cent over the previous year.[13] Consumer confidence in the Internet is arguably tainted enough already without being undermined yet further by the apparent complacency displayed, and/or difficulty experienced, by Visa (and, one supposes, other credit card providers) over internet credit card fraud. It was reported[14] recently, for example, that nine out of ten U.K. consumers were uneasy about using their credit cards for e-purchases. Visa discovered that for the European Union as a whole, only 5 per cent of consumers trusted e-commerce.[15] In the United States, a nationwide opinion poll, released by the Information Technology Association of America,[16] showed that 67 per cent of Americans felt threatened by, or concerned about, cyber-crime; 62 per cent felt that not enough was being done to protect internet consumers against cyber-crime and, as a result, 61 per cent were less likely to conduct business on the internet.

Visa, and other credit card providers, have tended to de-emphasise the fraud perpetrated by the direct use of one of its cards or from information derived from it. They note, for example, that approximately eight cents out of every US$100 spent on-line is lost to fraud. The comparative figure for non-cyber-based "landlocked" business is seven cents. Visa argues that even though the on-line figure is greater it is only marginally greater. Furthermore, the perpetrators of the fraud tend in the main not to be "super-hackers" accessing websites but the same opportunist thieves who have traditionally obtained numbers from discarded receipts and bills. Even if they succeed in perpetrating fraud, Visa argue that the U.S. consumer, for example, is limited under U.S. federal law to only the first US$50 lost and that many card issuers rarely seek to recoup that money. The problem is that companies *do* bear the brunt of that fraudulent activity. If the consumer loses money by dealing in e-commerce (even if that loss is then waived by their credit card provider) the likelihood of them purchasing goods or services on-line again is arguably reduced significantly. This has recently been recognised by American Express who have decided to issue free "smartcard" readers to its new card holders which, running via a home computer, convey personal information to the e-business being purchased from. The advantages of the system, aside from speed of purchase, are that American Express will refund customers' accounts in the event of the latter changing their minds about a purchase and that a PIN number, in addition to the credit card number, is required before the card can be used in an e-transaction. Beyond the actual one-off fraudulent activity, there remains of course the likelihood of "identity theft" in which the data derived from the credit card information held by the company[17] is utilised by the thief to obtain new credit, to borrow money or indeed to make further purchases. The pressure upon the e-company *not* to reveal that such losses might be incurred will arguably become increasingly strong given that, without consumer confidence being transposed into consumer spending, the commercial future of the relevant e-commerce companies will be bleak indeed.

Thus, the e-company that suffers a security breach is in a somewhat invidious position. To reveal that the breach has occurred enables the effects of that breach to be mitigated because, for example, consumers and credit card providers can be notified and the requisite action taken. However, revealing that a security breach has indeed occurred undermines public confidence in the e-company in particular and in e-commerce in general. In addition, it may also sap the confidence of other businesses with which the compromised e-company has dealt. Businesses exist to make money. The e-commerce revolution is unlikely to take corporate prisoners. The likelihood of security breaches becoming known in the public or business sector, therefore, will be slight. A study[18] by the Computer Security Institute and the FBI, which surveyed 643 computer-security professionals at large corporations, revealed that 70 per cent of them had detected unauthorised use of their computer systems in the previous year. Only 273 of the 643 respondents were prepared to quantify the amount of money lost. However, the losses revealed by those 273 *alone,* amounted to US$266 million for the year. Criminologists dealing with criminal statistics have to be aware of the “dark figure” of crime, that is to say, those crimes that tend to be under-reported or unreported. The dark figure of e-commerce crime is also believed to exist and it is its existence that arguably threatens the future of e-commerce more than the criminal activity itself. The UN has ***Comp. Law. 5*** also suggested[19] that the dark figure of crime, in the context of cyber-crime, refers to its relative invisibility. Such invisibility may be attributed, *inter alia,* to the sophistication of computer technology, the relative lack of expertise of law enforcement agencies and the victims' lack of preparedness against such crime being perpetrated against them.[20]

However, there are those commentators who argue that the response of the media and governments to internet security breaches is an over-reaction in which, what sociologists term, a “moral panic” is created. Rather like the way in which the fear of crime arguably causes greater consternation than the crime itself, it is argued that the fear of security breaches, in terms both of the likelihood and consequences of their occurrence, far outstrips the *actual* likelihood of such breaches occurring, and, furthermore, overestimates the effects of such breaches. Thus, for example, Senator Conrad Burns noted that “we now live in a world where malicious criminals can bring large parts of the nation's critical infrastructure to a grinding halt”.[21] As Stewart observed, “[a]s an assessment of Internet security, the senator's statement is a wild departure from the available evidence. As an expression of moral panic, it's pitch perfect.”[22] From February 7 to February 9, 2000, a number of major e-commerce companies' websites[23] were so inundated with requests for data that the sites' servers overloaded and could not deal with legitimate requests for information for a number of hours. These “denial of service” attacks were reported in the media in alarming tones.[24] As Stewart observed, however, “no consumer or proprietary information was stolen or even at risk. Rather, they were akin to petty vandalism, public nuisance or civil disobedience.”[25] How real a threat, therefore, is the hacker[26] to e-commerce?

The “Love Bug”[27] was described by one computer security expert as “the most damaging and the most widespread virus outbreak ever”.[28] It certainly caused consternation and disruption. The losses incurred in terms of lost work hours are estimated to be in the amount of US$10 billion. Eighty per cent of all U.S. federal agencies, including the State and Defense departments, were infected by the bug. The bug emanated from Quezon in the Philippines and spread successfully throughout Asia, Europe and the Americas. Once opened as an innocuous looking e-mail, the bug installed itself on the computer's hard drive, replaced itself with a copy of itself, and sent infected e-mails to the addresses logged in the Outlook Express folder. The fact that Microsoft Windows runs on nine out of ten computers made the bug particularly powerful. The use of e-mail attachments is of course not new[29] but the Love Bug was particularly malevolent. A month after Love Bug, the U.S. Government's National Infrastructure Protection Center revealed that the FBI was investigating another potentially disruptive e-mail virus. Network Associates, a software company, noted that the virus “has the potential to create e-mail storms leading to network performance slowdowns and has the ability to install extraneous content on users systems that can significantly deplete system memory”.[30] The infiltration by hackers by means other than e-mail is also becoming an issue. In June 1999, hackers caused the web pages of the FBI, the U.S. Senate and, ironically, that of the National Infrastructure Protection Center (which posts warnings about hackers and viruses) to move off-line. Bugtraq, an internet-based group that collates and disseminates information about security loopholes in software, noted recently[31] that approximately 60 new vulnerabilities were being discovered in software every month. Cerf argues[32] that, as a result of such viral attacks, “we will depend in larger and larger measure on the network's functioning reliably. Making this system of millions of networks sufficiently robust and resilient is a challenge for the present generation of Internet engineers. Failure could portend an increasingly fragile future.” Research commissioned by nCipher argued that many e-businesses are open to hacking by dint of the fact that they share web servers. Rather than

maintaining their own hardware storage facilities for important financial data, nCipher maintain that many e-companies "rely on third party operators to maintain their business security".[33] In a world in which the potential consequences of infiltration of financial and personal information held on the Internet are enormous, such a myopic viewpoint borders on the reckless.

Businesses, Stewart maintains, "have an interest in minimising their security weaknesses, and that makes for an ambivalent relationship with the security panic. It may bring unwanted government intervention and customer concern, so businesses are inclined to play down the threat."[34] If blame for e-crime can be levelled at faceless hackers rather than at the door of the poor security of the e-commerce companies themselves, then, theoretically, the likelihood of direct government interference in, and regulation of, e-commerce will be reduced. The effects of such masterful misdirection by e-companies (whether intended or not) may, however, for a variety of reasons, be rather short-lived. First, although the focus at the present time is upon ensuring that on-line credit card transactions remain secure (or at least as secure as "land-locked" transactions), ultimately, new forms of electronic payment (such as digital cash) will become increasingly utilised. The consequential potential for money-laundering is a very real one. Given that governments regulate money-laundering activity (at least in principle) in the "land-locked world", it seems inconceivable that they would not wish to ***Comp. Law. 6*** attempt to do so in the cyber-world. Secondly, the use, or propensity for the use, of the internet for a wide range of criminal activities, including terrorism, makes it extremely unlikely that governments will be able or willing to leave the Internet unregulated and/or unobserved for any definite period of time. Such a line of thought was recently pursued by the National Security Council's Director for Information Protection, Jeffrey Hunker, who has been charged with the task of encouraging law enforcement agencies, government intelligence agencies and the private sector to pool their collective knowledge and expertise. He maintains that, although companies may once have dealt with security breaches unilaterally, this approach was "totally inappropriate when we're dealing with a world where what you're experiencing might be one facet of a much larger intelligence or terrorist or national security threat".[35] This viewpoint is indicative of the problem law enforcement agencies are deemed to face when they endeavour to confront cyber-crime. The United Nations (UN) recently noted[36] that controlling cyber-crime was problematical because it took place in an electronic environment (which is difficult to police uniformly or effectively), that that environment was borderless (allowing crimes of a truly transnational nature to occur) and that it facilitated the creation of so-called "data havens"[37] in countries in which there was little or no criminalisation of computer misuse. Foresight's Crime Prevention Panel has noted in this regard that "[a]s the global reliance upon interconnected computer systems increases, so will the need to instigate protective measures against failure and malicious attacks. Consumerism, rather than communitarianism, is expected to be the predominant social philosophy."[38] Unfortunately, the expectation or anticipation of international co-operation in the area of cyber-crime is seemingly predicated upon the belief that it *already* exists in the context of other non-cyber criminal activities. However, in the case of terrorism, for example, which is increasingly becoming both technologically advanced in its application and international in its execution, and for which, consequently, there needs to be concerted and uniform international law enforcement effort, no single, universally accepted definition of terrorism has been accepted by the United Nations or exists in any multilateral treaty. Similarly, the activity of money-laundering is one that already constitutes an international problem and is one which, with the advent of electronic payment technologies (EPT), is likely to become a major cyber-based activity. The eradication, or at least reduction, of money-laundering is the primary role of the Financial Action Task Force (FATF), established by the G7 Summit in Paris in July 1989. Its membership comprises of 26 governments (including both the United Kingdom and the United States) and two regional organisations (the European Commission and the Gulf Co-operation Council). These members are undoubtedly doing their utmost to comply with the 40 recommendations to combat money-laundering laid down by the FATF. However, the FATF's recent annual report noted that there had in recent years been a "considerable increase in the number of jurisdictions which offer financial services without appropriate regulation or control, coupled with very strict banking secrecy".[39] Clearly, the difficulties presented by a crime which will increasingly occur in the borderless realm of the internet will be exacerbated when the definition of the crime either remains undefined at all, or poorly and/or unilaterally defined. If the FATF are experiencing regulatory difficulties in non-cyber money-laundering, one has to question the likelihood of the same cyber-based activity being thwarted.

In a separate report, the FATF identified 15 countries where there were "serious systemic problems".[40] In short, the countries that refuse to regulate against money-laundering rapidly become the facilitators of money-laundering and thereby undermine the attempts by the FATF to tackle and it is hoped eradicate the issue. It is against this non-co-operative backdrop that the likelihood of

success of international efforts against the rise of cyber-crime must be assessed. In essence, there seems to be a lack of global commitment to tackling the issues raised by this new form of criminality. Whether this is due to intransigence or genuine practical difficulties on the part of respective countries, is not necessarily clear. In reality, of course, the reason for the difficulty is academic. The consequences of non-co-operation remain abundantly clear. As a report of the President's Working Group on Unlawful Conduct on the Internet recently noted, "[w]hen one country's laws criminalise high-tech and computer-related crime and another country's do not, *co-op* eration to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible".[41]

The UN has noted in this regard that "[l]aws, criminal justice systems and international *co-op* eration have not kept pace with technological change. Only a few countries have adequate laws to address the problem, and of these, not one has resolved all of the legal, enforcement and prevention problems."[42] In essence, their review observes that there is no agreed typology of computer-related crime and no international definition of what constitutes criminal conduct. In addition, there is relatively little technological expertise on the part of law enforcement agencies and inadequate legal powers to facilitate the investigation of, and access to, computer systems. Investigatory difficulties are further exacerbated by differences in respective jurisdictions' procedural laws governing investigation of computer-related crime. Finally, there is deemed to be a lack of extradition and mutual assistance treaties, and of co-ordinated law enforcement procedures, both of which would enhance the likelihood of international co-operation occurring and being of assistance.

Despite such obvious difficulties, the U.S. Attorney-General Janet Reno said in April 2000 that the public and private ***Comp. Law. 7*** sectors "have a common goal--to keep the nation's computer network secure, safe and reliable".[43] E-businesses seemingly recognise that consumer confidence is a prerequisite for the continued expansion of e-commerce. E-businesses maintain that such security can only be attained through the use of encryption.[44] As the British Chambers of Commerce recently observed, cryptography "provides the basis for data protection and privacy and is also the key mechanism for identifying the parties to transactions, for authenticating data and for providing the digital signatures that are widely seen as an essential basis for electronic transactions".[45]

In 1999, the U.S. Congress introduced the Cyberspace Electronic Security Act (CESA). Acting Attorney-General Jon Jennings argued that "the same encryption products that help facilitate confidential communications between lawabiding citizens also pose a significant and undeniable public safety risk when used to facilitate and mask illegal and criminal activity".[46] The Act provides, *inter alia,* law enforcement agencies with the right to gain access to, and then decrypt, encrypted information (which may be being utilised by a criminal element) into plain text (*i.e.* readable text) for the purposes of pursuing an investigation.

In the United Kingdom, the government has introduced the Regulation of Investigatory Powers Act (RIPA).[47] The Act deals with four main areas,[48] including the right to access encrypted data. Section 49(3) of the Act provides that disclosure of encrypted information must be made if it is in the interests of national security, for the purpose of preventing or detecting crime or in the interests of the economic well-being of the United Kingdom. Certainly, encryption is deemed to be an inevitable facet of the successful expansion of e-commerce. The fact that criminals may utilise encryption in their own communications raises a concomitant need for law enforcement agencies to be able to intercept and decipher coded e-traffic.

To complement the respective domestic legislation, the Council of Europe introduced, on April 24, 2000, its draft Convention on Cyber-Crime.[49] The Council anticipates that the Committee of Ministers should be in a position to adopt the text (following widespread consultation) and present it for signature by autumn 2001. It seeks to provide for "the co-ordinated criminalisation of computer hacking and hacking devices, illegal interception of data and interference with computer systems, computer-related fraud and forgery".[50] In terms of enforcement, the draft Convention obliges all signatories, *inter alia,* to "empower their national authorities to carry out computer searches and seize computer data …"[51] U.S. Attorney-General Janet Reno, arguing in support of the draft Convention, noted that "[s]ome countries have weak laws, or no laws, against computer crimes, creating a major obstacle to solving and to prosecuting computer crimes. I am quite concerned that one or more nations will become 'safe havens' for cyber-criminals."[52]

One suspects that in the area of cyber-crime, in which there is not necessarily universal business and public support for governments' right to intercept and decrypt encrypted data (in the pursuit of justice), to hope to get such a wide-ranging and detailed convention universally adopted and applied is bordering on the utopian. If the pattern of money-laundering control,[53] for example, is any guide (and

of course money-laundering will become an increasingly key facet of cyber-crime), the problem of computer-based crime will become a major disruption to public life as well as to e-commerce developments. The U.K. and U.S. Governments have sought to justify their respective pieces of legislation on the fact that the very *possibility* of the utilisation of encryption by criminal groups justifies the right of the governments to acquire access to the plain text of those otherwise hidden communications. However, if governments cannot hope realistically to co-operate at the level, and with the urgency, necessary effectively to thwart global cyber-crime, then are the powers they possess in relation to encryption justified on anything other than a national level?

The British Chambers of Commerce (BCC) argued that the RIPA was “likely to create a legal environment which will inhibit investment, impede the evolution of e-commerce, impose direct and indirect costs on business and the consumer, diminish overall trust in e-commerce, disrupt business-to-business relationships, place U.K. companies at a competitive disadvantage, and create a range of legal uncertainties which will place a growing number of businesses in a precarious position”.[54] It is a position that the U.K. Government has challenged.[55]

The BCC's chief concern, perhaps, lies in the provisions concerning cryptography, which it maintains “is now universally seen as a critical technology on which e-commerce will depend”.[56] Cryptographic technology, however, is only as good as the security under which the keys which unlock the coded language are kept. The RIPA provides[57] that a notice requiring disclosure by the key holder of encrypted information may be given on reasonable grounds. It is further provided[58] that, where there appears to be more than one person in possession of the key, notice will not be given. ***Comp. Law. 8*** However, the Act also provides[59] that in “special circumstances” those subsections will not apply. Disturbingly perhaps, what those circumstances are, or could be, is *not* disclosed. The BCC argues that this lack of clarification places businesses in a difficult strategic position. The BCC notes that “[w]here a security risk can be quantified, a business decision can be made on whether the level of risk is tolerable or whether steps need to be taken to counter it. But when such a risk is of unknown extent, security decisions have to err on the side of caution by planning on the assumption that it is a much larger risk than it may turn out to be.”[60] The propensity for small fledgling e-businesses to rely on third party operators[61] is deemed by the BCC to be a crucial issue in the future development of e-commerce. For the e-businesses and their consumers alike, the presence or perception of secure websites will be essential. As the BCC note, “a hosting company will not only have to manage its own keys but also the keys of many of its clients. This is an enormous security challenge in its own right but the addition of a requirement that all such keys might have to be supplied to U.K. Government authorities could easy turn a difficult job into an impossible one.”[62] The BCC proceeds to argue that, for e-commerce to grow, there has to be a high degree of mutual trust between business, the consumer and government. Consequently, the BCC argues, the release of encrypted information to outside parties, whether in plain text or coded with decryption keys, will serve only to erode that trust.

In conclusion, it seems that the business and law enforcement communities, respectively, occupy polarised positions. For business, encryption is deemed to be the most reliable method of protecting consumers against internet crime. Any compromise, therefore, over encryption security will, according to business, serve only to deter on-line transactions and stifle the growth of e-commerce. Conversely, law enforcement agencies maintain that unbreakable encryption will simply provide a conduit along which information concerning drug trafficking, terrorism and other crimes can flow unimpeded. Behind both positions, however, lies a further conundrum. Can the internet *per se* be controlled and regulated by the unilateral actions of national governments or indeed through the power of collective international agreements?[63] The very nature of the internet's computer network makes it extremely difficult to impose any practical notion of territoriality upon cyberspace. Given that fact, it seems unlikely that any one state could realistically hope to regulate the internet. As Buhrer of Interpol argues, “[w]e've got to reach the stage where we're not comparing apples with oranges, but apples with apples”.[64] If the internet is truly global of course, then arguably regulation is a *global* not *national* issue, and, as with all global issues, solvable only through global co-operation. Ironically, although the internet is an illustration of what can be achieved when global economies decide that e-commerce is the way ahead, the governments who promote e-commerce, and the businesses which facilitate and sustain its growth, seem unwilling, or unable, to compromise on the issue of encryption. The absence of encryption may indeed lead to breaches, or the perception of breaches, in the security of e-businesses and to a diminution in growth of e-commerce as a consequence. Equally, however, the presence of encryption, without access being granted to law enforcement agencies to the encrypted data, may facilitate the increased growth of cyber-crime, and *that* may in turn undermine e-commerce to an irretrievable degree. By that juncture, the current fear of security breaches and of subsequent consumer boycotts will seem idyllic by comparison.

Robin McCusker *Senior Lecturer in Law, University College Northampton*

Comp. Law. 2002, 23(1), 3-8

---

1. P. Ging, “Dark Side of the Web”, www.bbc.co.uk/news, May 27, 2000.
2. V. Cerf, “What Will Replace the Internet?”, *Time,* July 3, 2000, pp. 66-67 at p. 66.
3. M. Krantz, “Click Till You Drop”, *Time,* August 3, 1998, pp. 40-45 at p. 45.
4. www.fbi.gov/majcases/investnet/investnet.htm.
5. The Internet Economy Indicators, Indicators Report, June 28, 2000.
6. *E-Commerce Times,* June 28, 2000, www.ecommercetimes.com.
7. *Daily Telegraph,* January 20, 2000, www.telegraph.co.uk.
8. *ibid.*
9. See, for example, S. Jagger, “Investors Hit Panic Button on Tech Shares”, *Daily Telegraph,* March 31, 2000, www.telegraph.co.uk/et?.ac.
10. www.zdnet.co.uk/news/2000, March 17, 2000.
11. www.zdnet.co.uk/news/2000, November 24, 1999.
12. *ibid.*
13. www.zdnet.co.uk/news/2000, January 20, 2000.
14. www.bbc.co.uk/news, November 19, 1999.
15. *ibid.*
16. www.globalarc.t.com, June 19, 2000.
17. The information is held on a “cookie”, a small (4K at most) file that a web server can store on the consumer's machine.
18. *Fortune,* www.library.northernlight.com, May 15, 2000.
19. “International Review of Criminal Policy, Nos. 43 & 44 (Manual on the Prevention and Control of Computer-Related Crime)”, www.ifs.univie.ac.
20. *ibid.*
21. S. Stewart, “Anxiety Disorder”, www.thestandard.com, May 15, 2000.
22. *ibid.*
23. Amazon.com; Buy.com; CNN.com; eBay, E-Trade, Yahoo and ZDNet.
24. The *Wall Street Journal* 's front page, for example, said that the Internet was “Under Siege” and the lesser known *Charlotte Observer* 's front page noted that “Hackers' Assaults Stir Chaos on Internet”.
25. Stewart, n. 21 above.
26. The word “hackers” is used as a generic term throughout the paper and should be deemed to encompass “crackers” who are the malicious hackers who seek to bring down computer systems rather than simply infiltrate them. This recognised distinction is outlined in “A-Z: Hack Attack”, www.bbc.news.co.uk, February 11, 2000.
27. A generic name for a virus which was disguised as an e-mail message proclaiming “ILOVEYOU”.
28. G. Hodges, President and CEO of McAfee, in L. Grossman, “Attack of the Love Bug”, *Time,* May 15, 2000, pp. 25-30 at p. 28.
29. Other attachments include the Morris Worm, Michelangelo, WordConcept, Wazzu, Melissa, ChernobylVirus, Explore.Zip and BubbleBoy; Hodges, n. 28 above, p. 28.
30. www.bbc.co.uk/news, June 20, 2000.
31. M. Ward, www.bbc.co.uk/news, May 31, 2000.
32. Cerf, n. 2 above, p. 67.
33. *ibid.* See also p.7 below in which the dangers inherent in continuing business opposition to access by law enforcement agencies to encrypted business data are discussed.
34. Stewart, n. 21 above.
35. V. Beiser, “Only You Can Prevent Cybercrime”, www.wired.com/news/politics, July 7, 1999.
36. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, Austria, April 10-17, 2000, “Crimes Related to Computer Networks”, www.uncjin.org/Documents/10thcongress.
37. *ibid.,* p. 1.
38. Crime Prevention Panel, “Just Around the Corner”, www.foresight.gov.uk, p. 5.
39. Financial Action Task Force, *Annual Report 1999-2000,* June 22, 2000, www.oecd.org/fatf/reports.htm, p. 18, para. 76.
40. Financial Action Task Force on Money Laundering, “Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures”, June 22, 2000, www.oecd.org/fatf/reports.htm, p. 12, para. 64.
41. “The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet”, March 2000,

www.cybercrime.gov/unlawful.

42. "International Review of Criminal Policy--United Nations Manual on the Prevention and Control of Computer-Related Crime", www.ifs.univie.ac.at.

43. Stanford University Law School Conference on Cyber-Crime, April 5, 2000, reported at www.bbc.co.uk/news, April 8, 2000.

44. Encryption, also referred to as cryptography, is the "use of mathematical or other methods to hide the content of messages or files". This definition was extracted from "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet", A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000, www.cybercrime.gov/unlawful.

45. "The Economic Impact of the Regulation of Investigatory Powers Act", British Chambers of Commerce, June 12, 2000, p. 12, www.britishchambers.org.uk/news and policy.ict/ripActsummary.

46. www.bbc.co.uk/news, August 20, 1999.

47. The Act may be seen as a companion to the Electronic Communications Act 2000 which seeks, *inter alia,* to facilitate the use of electronic communications and data storage.

48. The Act deals with the interception, acquisition and disclosure of communications data, surveillance and covert human intelligence sources, investigation of electronic data protected by encryption and the scrutiny of investigatory powers and functions of the intelligence services.

49. Draft No. 25 of the Convention was produced on December 22, 2000. The Convention was formally adopted by the Committee of Ministers on November 8, 2001 and was signed on November 23, 2001.

50. "Draft Convention on Cyber-Crime", www.conventions.coe.int/treaty/EN/projets/cybercrime.htm.

51. *ibid.*

52. D. McCullagh, "Cybercrime Solution Has Bugs", www.wired.com/news/politics.

53. See p.13 above on the challenge faced and only partially met by the Financial Action Task Force.

54. "The Economic Impact of the Regulation of Investigatory Powers Act", n. 45 above, p. 1.

55. See www.homeoffice.gov.uk/oicd/bcc.

56. *ibid.,* p. 12.

57. s. 49(2).

58. s. 49(5) and (6).

59. s. 49(7).

60. "The Economic Impact of the Regulation of Investigatory Powers Act", n. 45 above, p. 12.

61. See p.4 above.

62. "The Economic Impact of the Regulation of Investigatory Powers Act", n. 45 above, p. 13.

63. Freenet, for example, which has been designed to operate without any form of centralised control. See J.L. Shenker, "The Infoanarchist", *Time,* July 17, 2000, pp. 44-45, for an evaluation of its potential threat to, *inter alia,* intellectual property rights.

64. U. Sautter, "To Catch a Thief", *Time,* June 19, 2000, pp. 67-69 at p. 69.