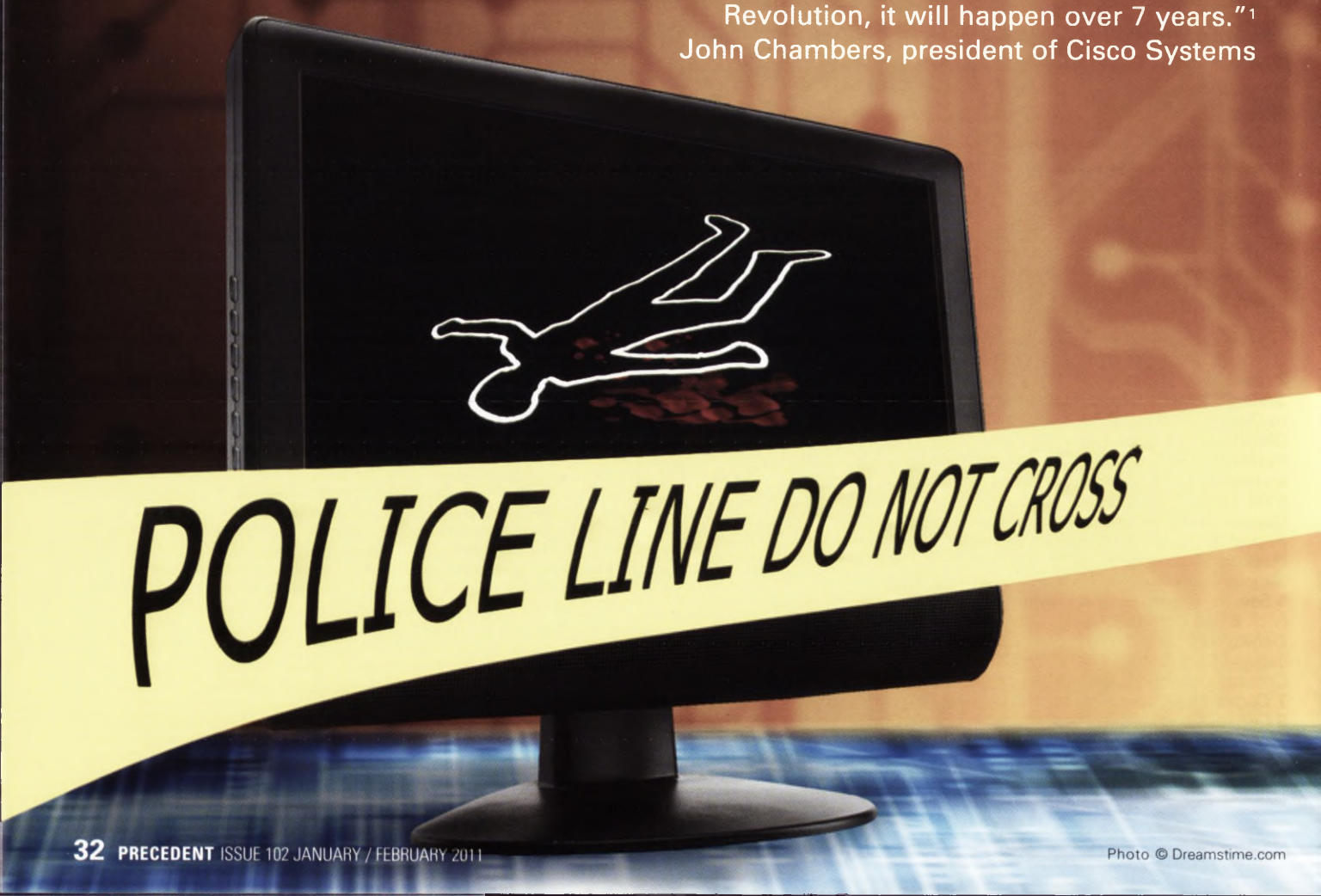
CYBERCRIME

Catching cyber criminals on peer-to-peer networks

By Paul Folino-Gallo

"What people have not grasped is that the internet will change everything ... The Industrial Revolution brought together people with machines in factories, and the internet revolution will bring together people with knowledge and information in virtual companies. And it will have every bit as much impact on society as the Industrial Revolution. It will promote globalisation at an incredible pace. But instead of happening over 100 years, like the Industrial Revolution, it will happen over 7 years."[1]
John Chambers, president of Cisco Systems



The advent of the internet and its convergence with digital technology have clearly revolutionised the way in which we communicate and transact with one another on a day-to-day basis. With the emergence of social networking sites, chat applications and peer-to-peer file-sharing systems, information and media are now being produced and exchanged at unprecedented levels online. As technological advancements continue to improve and expand, our reliance upon the internet as a source of information, communication, entertainment and trade has increased exponentially.[2] However, our dependence upon this technology, coupled with the inherent characteristics of the internet, has created vulnerabilities that have rendered cyberspace a fertile ground for criminal activity.[3] Not only can existing crimes be replicated and facilitated in the online environment, but novel crimes that exploit specific features of digital networks have also emerged. It is for this reason that cybercrime presents unique difficulties to law enforcement agencies and the criminal justice system.

Common law jurisdictions shaped by centuries of jurisprudence have been challenged to reconsider well-entrenched principles of law in an attempt to adapt to these rapid developments in the online world. Moreover, the omnipresent nature of the internet has cut across traditional national borders, leaving a quagmire of jurisdictional issues in its wake.[4] Law enforcement agencies have had their mettle tested in attempting to regulate the online environment. The new investigative practices that they seek to engage and adapt present particular challenges of their own. Although this article focuses on remote online searches by law enforcement agencies, it also aims to underscore the importance for lawyers of evaluating and considering the effect that the internet may have on other areas of the law.

PEER-TO-PEER NETWORKS: UNDERSTANDING THE ENVIRONMENT

The trade of illicit material across peer-to-peer networks has become one of many major challenges for law enforcement agencies seeking to regulate online behaviour. The decentralised nature of peer-to-peer networks,[5] coupled with the sheer volume of information exchanged over such networks, make them ideal for the trade in illicit material online.[6] Several studies have suggested that these networks are teeming with contraband material, and a significant amount of traffic relates to the trade of that material, albeit from a comparatively small sub-set of users.[7]

To address the proliferation of illicit material on peer-to-peer networks, law enforcement agencies have developed various suites of software to detect network-users engaged in these illegal activities.[8] As these suites of software are instrumental in gathering evidence and prosecuting offenders, it is imperative for all parties involved in the criminal justice system to acquaint themselves with this technology and understand how it operates, so as to verify the provenance of the evidence derived therefrom and ensure its probative value.

LIMEWIRE AND THE GNUTELLA PROTOCOL

Limewire is a peer-to-peer application that is based around the Gnutella Protocol. Although the Limewire program will shut down in 2011 by reason of an injunction ordered on 27 October 2010,[9] the investigative techniques inherent in the Limewire program are transferable to other peer-to-peer file-sharing programs.

The Gnutella Protocol is a network system that allows a user to connect to other computers without a centralised server. Thus, every computer ('node') in a peer-to-peer network can talk with every other node.[10]

Within that network, there are two types of nodes; the stronger nodes take the part of ultra peers, and the remaining are assigned as leaves.[11] The ultra peers execute searches across the networks on behalf of the leaves, in an effort to minimise traffic on the network.[12] The ultra peer is not involved in the download process, but merely supplies the information necessary to facilitate the download between the leaves (like an introduction service).[13]

THE BASICS OF HASHING

'Hashing' is the process of taking computer data as a string of information, passing that string through an algorithm that converts it to a unique number sequence, referred to as a 'hash value'.[14] The hash value has often been referred to as the DNA or fingerprint of a file. The hash value is a function of the file properties and characteristics.[15] The probability >>

The prevalence of dynamic IP addresses, which can no longer distinguish between physical machines and mobile users, renders them of limited value in investigations.

of a non-contraband file's hash value colliding with a contraband file's hash value is less than 1 in 340 undecillion (340 followed by 36 zeros).[16] So the use of hash values is quite a powerful tool in identifying illicit material without having to forensically analyse the file, even where it has been renamed to avoid detection by authorities.[17]

PEER-TO-PEER INVESTIGATION TECHNIQUES

Methods of gathering evidence using the Gnutella Protocol include the use of search queries, information gathered by 'swarming', the browsing of host files and the downloading of files. Software programs such as the Wyoming Toolkit further enhance the capabilities of file-sharing programs.

Making search queries in Limewire using words associated with illicit material is a method often employed by law enforcement agencies to develop leads in cybercrime investigations.[18] In the peer-to-peer context, this often involves typing specific search terms that are commonly used to locate and download illicit material. The search query is sent through the ultra peers. The ultra peers then return a set of results to the investigator's computer. The results page sets out the file names that best match the search query, along with the IP address of the leaf that is storing that file.

From the titles of the media file names returned through Limewire, the direction for further investigation of certain files will often be self-evident.

Once illicit material is suspected to be contained in returned results, an investigator may then:

- uncover the hash value of the suspicious file and cross reference that hash value with a database of known contraband; or
- connect with the target leaf offering the suspicious file and query the full set of files that the leaf is sharing.

Both of the aforementioned steps require the remote access of the target leaf by the investigator's computer. Upon evaluation of the contents of the files on that leaf, however, an investigator will often be able to negate the accidental download of contraband material.[19]

The investigator is able to remotely access the target leaf and initiate a download of the file that is suspected of containing illicit material. In so doing, the source leaf that is offering the file will notify the investigator of other users on the peer-to-peer network that are sharing that same file.

This feature was designed by file-sharing programs to speed up the downloading process by facilitating the downloading of parcels of information from various leaves with the identical file. These identical files are recognised by the hash value. From an investigative standpoint, this process (referred to as 'swarming') provides a useful tool to uncover groups of people engaged in sharing illicit material across a peer-to-peer network.

Upon selection of the desired file, the investigator's computer connects with the host leaf directly, and the target leaf transmits the file and content to the investigating computer. In the decision of *US v Willard*,[20] the US District Court of Virginia set out how Limewire and the Gnutella Protocol are ordinarily used by law enforcement agencies in cyber investigations:

> 'An undercover agent working for the . . . FBI conducted a keyword search on a peer-to-peer file-sharing network using terms known to be associated with child pornography. Her search revealed a file from internet protocol ('IP') address 24.125.166.216. The agent conducted a search of other files available at this IP address and downloaded seven files, three of which depicted child pornography. Special Agent Howell of the FBI subsequently viewed the images and confirmed that they depicted child pornography.'[21]

LOCATING THE PHYSICAL LOCATION OF THE TARGET LEAF

Where the filename or content of the file give rise to a reasonable belief that it contains contraband material, the investigator may require a subpoena issued to the internet service provider (ISP) so as to ascertain the physical location of the computer that is storing the contraband material.

The widespread use of dynamic host configuration protocol (DHCP), mobile networking and computer viruses has diminished the value of IP addresses in cybercrime investigations. More computers are using dynamic IP addresses that make the location of computers more difficult to ascertain. The inability of IP addresses to distinguish between physical machines and the difficulty in following a mobile user moving across a number of IP addresses thus renders the IP address of limited value in investigations. However, the location of the computer, coupled with evidence of the material gathered through the peer-to-peer investigation will ordinarily be enough to establish the reasonable suspicion to justify a search warrant.

DOES LIMEWIRE EXAMINATION CONSTITUTE A SEARCH?

To date, there has been very little judicial consideration in Australian courts as to whether peer-to-peer examination of a target leaf's computer constitutes a search. Yet the answer to this question is of great importance to the admissibility of the evidence derived from a search of this kind in the absence of a warrant.

A great number of legal commentators and courts have considered this question in the American context. Though not directly on point, there is some recognition that the Fourth Amendment of the US Constitution did reflect the state of English law at the time it was drafted.[22] What is often neglected when comparing the laws of Australia with the

US in this context is the significant change to the way that the Fourth Amendment has been interpreted by the courts following the decision of *Katz v US*.[23]

In *Katz v US*,[24] the Supreme Court ruled that a search would be considered unconstitutional under the Fourth Amendment only where a person expects privacy in the thing searched, and society believes that expectation to be reasonable.

Notwithstanding this divergence between the US and Australian law, an examination of US law as it relates to peer-to-peer investigations is a useful starting point in divining an answer to the seemingly straightforward question.

In the US, the starting point of any discussion involving a search and seizure is the Fourth Amendment, which reads as follows:

> 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'[25]

Some legal commentators from the US have confused the focus on a reasonable expectation of privacy with the plain view doctrine. The confusion stems from the idea that most peer-to-peer systems freely advertise shared content among users and, therefore, the files observed in search results are clearly in plain view.[26]

However, the US courts have proceeded on the basis that a search is deemed to have occurred only when the government conduct has transgressed a citizen's subjective manifestation of a privacy interest; and the privacy interest invaded is one that society is prepared to accept as legitimate. This 'reasonable expectation of privacy' test has come to be the means used for determining the scope of the Fourth Amendment's protections.[27]

In the cases of *US v Borowy*[28] and *US v Ganoe*,[29] the Ninth Circuit Court of Appeals held that the access and seizure of material through the Limewire software did not qualify as a search, as it did not violate a reasonable expectation of privacy as guaranteed against under the Fourth Amendment of the US Constitution. In both instances, the courts held that the expectation to privacy did not survive the decision to install and use file-sharing software, thereby opening a computer to anyone else with the same freely available program. It was on this basis that the courts in the US have admitted evidence acquired through Limewire investigations and the use of the 'Wyoming Toolkit'.[30]

It appears that the weight of US authority is directed to the reasonable expectation of privacy as opposed to whether the computer constituted a search.

THE LAW OF SEARCH AND SEIZURE IN AUSTRALIA

In Australia, a search may be conducted only by operation of statute, by consent, or exigent circumstances.

The first step is to determine whether a search has taken place. This may be a question of fact to be determined according to the level of interaction between the investigator's computer and the target computer.

There is a paucity of cases that deal with the definition of a search in the Australian context. In *Darby v Director of Public Prosecutions*,[31] the court was directed to the authorities from the US. That judgment spoke to the issue of what constitutes a search. The Court of Appeal was split as to whether the use of drug detection dogs constituted a search, with the majority holding that it did not. Though confining its reasons to the term 'search' as it applied to the *Drug Misuse and Trafficking Act* 1985 (NSW), the Court held that a search involved the examination of a thing for the purpose of finding out whether it contained contraband. His Honour Ipp JA (with whom McColl JA agreed) held that, as the drug dog had been trained to follow the scent of cannabis, the dog was not used for the purposes of searching the defendant; the dog knew where the drug was. It was the police officer who searched the defendant for the purposes of locating the drug on the defendant's person.

There are several points of interest when seeking to apply the drug detection dog analogy to the *Darby* case. >>

Our dependence on the internet, coupled with its inherent characteristics, has created vulnerabilities making cyberspace a fertile ground for criminal activity.

The drug detection dog is operating in a public space, and although it is in that public space with a direct purpose of detecting illicit substances, the scent of cannabis is something that can be perceived by the dog. Is this the same as launching a broad search in cyberspace without any underpinning reasonable suspicion and receiving back a list of results of potential offenders? On one construction, it may be argued that cyberspace constitutes a public space; that the search results would be analogous to a scent detectable in the public and thus, at that stage, no search had been carried out. On another construction, however, the search query actually constitutes thousands of contemporaneous searches, providing back results after the files of the nodes are sifted by the program.

Supposing that the former construction is adopted, and that the search query is analogous to the drug detection dog walking down the street, what of the subsequent acts performed by law enforcement agencies using the peer-to-peer network? Is the direct connection by law enforcement to the target computer for the purpose of examining other files contained therein a search?

It has been suggested that the Fourth Amendment of the Constitution of the US encompasses the common law position of England.[32] If the corollary of this point is that decisions from the US should be followed in Australia, then the fact that the Limewire user under investigation does not have a reasonable expectation of privacy over shared files would militate against the finding that the remote access to a computer in these circumstances constitutes a search. However, adoption of the precedent from the US should be tempered, as His Honour Olsson J presciently noted in *Questions Reserved No. 3*:[33]

> 'It is true that some limited authority can be found in the United States which attaches a wide construction on what constitutes a search. However, these are very much a reflection of specific concepts written into the constitution of that country by the so-called Fourth Amendment — which, *inter alia*, focus on reasonable expectations of privacy.'

The Court of Appeal in *Darby* did not agitate the issue of reasonable expectation of privacy. Rather, it held that once the dog had identified the suspect, any ensuing trespass perpetrated to examine the person to determine whether there was contraband would require a reasonable suspicion to have been formed by the investigating officer (implicitly accepting that this would constitute a search). The focus was on the trespass to the person or thing being searched, rather than an enquiry as to the expectation of privacy.

In applying the NSW Court of Appeal's approach to the instant case of peer-to-peer investigation, the pivotal question is whether the remote access of a computer constitutes a trespass. If the answer is 'yes', the access must, by implication, constitute a search. This was indeed the position in respect of wiretapping cases until the decision of *Katz*, and finds support in the decision of Sir Robert Megarry V-C in *Malone v Commissioner of Police of the Metropolis* (No. 2) [1979] 2 All ER 620.

Of course, the open view rule may be invoked to advance the proposition that no search has taken place, despite the remote access of the target computer by the investigator. The plain view rule has implicitly been accepted by the courts in Australia. The premise of the plain view doctrine is that where an item can be sensed or perceived without committing a trespass, that item is said to be in open view.[34] Things in open view are exposed to the public, and the perception of a thing in open view does not constitute a search.[35] Of course, the plain view doctrine was formulated before the advent of the internet, yet whether the courts apply a broad application of the doctrine remains to be seen. Whether there is a requirement for a trespass to be committed for the Courts to find that a search has been conducted is also a problematic issue when considering the difficulties that tort law has had in dealing with trespass to digital products.[36]

In the case of *Darby*, however, the majority decision of the Court of Appeal referred to O'Keefe J's reasons at first instance,[37] where His Honour summarised the various meanings of 'search', as provided by a number of dictionaries.

The common theme from the definitions of search could be distilled to two fundamental elements:

- the examination of a person or thing;
- with the view of finding something that is hidden.

This definition eschews the need to stretch the plain view doctrine and grapple with trespass. If this definition of search is to be applied to the instant case, the remote access of computers through the peer-to-peer investigations constitutes a search.

A corollary of this finding is that the search must require a warrant unless express consent to be searched has been given or a statutory right to search the target computer exists. Alternatively, investigators may be entitled to search a computer remotely where there are exigent circumstances to justify such action being taken.[38]

THE EFFECT OF A WARRANTLESS SEARCH ON THE ADMISSIBILITY OF EVIDENCE IN AUSTRALIA

Without express statutory provisions authorising law enforcement to conduct a search using a file-sharing program, it would appear that peer-to-peer investigations of this nature would constitute an impropriety or unlawfulness so as to warrant the intervention of s138 of the *Evidence Act* 1995 (Cth). It may be that in exercising the court's discretion to exclude evidence, it would find that the desirability of allowing the evidence to be admitted outweighs the impropriety of the warrantless search. The arguments

successfully advanced in the US – that any incursion on privacy brought about by this type of investigation is far outweighed by the desirability of protecting the more vulnerable classes of society from exploitation – are likely to carry some weight. This is particularly so when having regard to the inherent difficulties already experienced by law enforcement agencies commissioned to detect and prosecuting those who engage in this type of behaviour.

CONCLUSION

The idea that those who use peer-to-peer networks may be subject to clandestine searches may also be repugnant to civil libertarians. To others, to argue that civil liberties should prevail over the fight against cybercrime may seem equally abhorrent.

The need for clarity on the issue of whether peer-to-peer investigations constitute searches, and the legality of those searches, is self-evident. So, too, is the need to ensure that law enforcement agencies act within the confines of the powers they have been given to prosecute cyber criminals.

Where those powers are deemed insufficient to adequately detect and prosecute cyber criminals, these types of investigations should be legislated for so as to ensure that there are checks and balances in place to protect ordinary citizens, while at the same time ensuring that evidence derived from these operations remains admissible at trial. ■

Notes: **1** Cited in T Friedman, 'Foreign Affairs, Internet Wars', *New York Times*, 11 April 1998, accessed 17 November 2010 < http://www.nytimes.com/1998/04/11/opinion/foreign-affairs-the-internet-wars.html. **2** P Grabosky, R Smith, and G Dempsey, *Electronic Theft; Unlawful Acquisition in Cyberspace* (2001, Cambridge University Press). **3** S Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law,' (2001) 8(2) *Murdoch University Electronic Law Journal* <http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82nf.html. **4** D Johnson, and D Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) *48 Stanford Law Review* 1367; See also U Kohn, *Jurisdiction and the Internet* (2007, Cambridge University Press). **5** D Wall, 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace,' (2007) 8 *Police Practice Research* 2. **6** C Steel, 'Child pornography in peer-to-peer networks'. (2009) 33 *Child Abuse and Neglect* 560; See also D Hughes et al, 'Supporting Law Enforcement in Digital Communities through Natural Language Analysis' (2008) in N Srihari and K Franke, (eds) 5158 *Lecture Notes In Computer* Scienc,e p122. **7** D Hughes, J Walkerdine, G Coulson and S Gibson, 'Peer-to-Peer: Is Deviant Behavior the Norm on P2P File-Sharing Networks?' (2006) *IEEE Distributed Systems Online* 7, 1-11. **8** *Ibid.* **9** *Artista Records and 10 ors v Limewire LLC and 4 ors* (2010) NY District Court, 06 Civ 05936. **10** P Makosiej, G Sakaryan & H Unger, 'Measurement study of shared content and user request structure in peer-to peer Gnutella Network' *Design, Analysis, and Simulation of Distributed Systems* (2004, pp115–24), Arlington, VA. **11** J Lewthwaite, and V Smith, 'Limewire Examinations' (2008) *Digital Investigations,* The Proceedings of the Eighth Annual DFRWS Conference. **12** B Loo, R Heubsch, I Stoica, and J Hellerstein, 'The Case for A Hybrid P2P Search Infrastructure' (2005) In G Voelker and S Shenker, *Lecture Notes in Computer Science* Vol. 3279/2005. **13** R Matei, A Iamnitchi, and P Foster, 'Mapping the Gnutella Network' (2002) 6 *Internet Computing,* 50. **14** B Schneier, *Applied Cryptography* 30 (1996 2nd ed). **15** SJ Wang, 'Measures of retaining digital evidence to prosecute computer-based cyber-crimes' (2007) 29 *Computer Standards & Interfaces,* 216. **16** RP Salgado, 'Fourth Amendment Search and the Power of the Hash' (2006) 119 *Harvard Law Review,* 38. **17** R Losey, 'Hash: The New Bates Stamp' (2007) 12 *Journal of Technology Law and* Policy,1. **18** D Hughes et al, 'Supporting Law Enforcement in Digital Communities through Natural Language Analysis' (2008) Proceedings of the 2nd international workshop on Computational Forensics. **19** M Liberatore et al, 'Forensic investigation of peer-to-peer file-sharing networks' (2010) 7 *Digital Investigation,* 95. **20** *US v Willard* 2010 WL 3784944 (US District Court for the Eastern District of Virginia 2010). **21** *Ibid.* **22** D Schlansky, 'The Fourth Amendment and Common Law' (2000), 100 *Columbia Law Review* 1739. **23** *Katz v US* 389 US347 (1967). **24** *Ibid.* **25** *United States of America Constitution* Amend IV. **26** M Liberatore, B Levine, and C Shields, 'Strengthening Forensic Investigations of Child Pornography on P2P Networks,' (2010) in ACM Conference on Future Networking Technologies (CoNEXT). **27** R Julie, 'High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age' (2000), 37 *American Criminal Law Review,* 127 (2000). **28** *US v Borowy* 595 F.3d.1045 (9th Cir. 2010). **29** *US v Ganoe* 538 F.3d 1117,1127 (9th Cir. 2008). **30** So-called because it was developed by the Wyoming Internet Crimes Against Children (ICAC) Task Force. See also P Luehr, 'Real Evidence, Virtual Crimes: The Role of Computer Forensic Experts', (2005) 20(2) *Criminal Justice,* 14. **31** *Darby v Director of Public Prosecutions* (2004) 61 NSWLR 558. **32** D Schlansky 'The Fourth Amendment and Common Law' (2000), 100 *Columbia Law Review* 1739. **33** *Questions of Law Reserved (No. 3 of 1998)* (1998) *71 SASR 223.* **34** K Tronc, C Crawford and D Smith, *Search and Seizure in Australia and New Zealand* (1996, Lawbook Co), p25. **35** *Malone v Commissioner of Police (No. 2)* [1979] 2 All ER 620. **36** *Hoath v Connect Internet Services* [2006] NSWSC 158. **37** *Director of Public Prosecutions v Darby* [2002] NSWSC 1157. **38** *Bunning v Cross* (1978) 141 CLR 54 at 79.

Paul Folino-Gallo *is a barrister working from the Third Floor, Wentworth Chambers, Sydney.* **PHONE** *(02) 8915 2810*
EMAIL *pfolino-gallo@wentworthchambers.com.au.*