PAPER:

# SEARCH AND SEIZURE OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

By **Charles Leacock,** Q.C., LL.M (Lond), Director of Public Prosecutions, Barbados

## Introduction

The rapid development in computer technology in the past two decades has focused attention by countries on the need to modernize and update their legal and administrative capabilities. The advent of digital evidence has become commonplace as people and entities respond to legitimate business transactions. The prevalence of abuse has focused attention on the development of mechanisms to respond to cyber crimes and computer related interferences. Digital evidence may be considered any information of a probative nature that is stored, transmitted or retrieved in a binary form. The format of digital evidence consists of ones and zeros of electricity. As such, digital evidence is beyond the conventional computer based information, extending to the analogue format of audio and video productions, although all are rapidly becoming digital as well.

The International Narcotics Control Board[1] has repeatedly cautioned that committing a crime in an electronic environment (cyber crime) is easy. Few resources are required to obtain access to and use the internet. The personal dangers for the criminal and the likelihood of detection are reduced, because cyber crimes are difficult to investigate and prosecute. The use of digital evidence has proliferated in the past decades. Courts have permitted prosecuting authorities to obtain access to e-mails, digital photographs, word documents, instant messaging, spreadsheets, internet browsers, hotel electronic door keys, automatic teller machine slips and global positioning schedules. The reality is that new rules have not developed at a sufficient pace to cope with the existing realities. Accordingly, existing rules designed for physical and conventional investigations are applied and stretched to cover the reception of digital evidence.

## Authentication

All evidence, including digital evidence, demands that a proper foundation must be presented for its reception. Courts are overtly interested with the reliability of digital evidence. In the 1977 eighth circuit case of *United States of America v Scholle*,[2] Henley, J suggested that 'the complex nature of computer storage' called for authentication of digital evidence to have a 'more comprehensive foundation'. However, by 1982 as the reception of digital evidence had become commonplace, Clark, CJ of the fifth circuit in *United States of America v Vela*,[3] reiterated a comment made in *Rosenberg v Collins*, 624 F.2d at 665, that 'this court has previously held that "computer data complications ... should be treated as any other record of regularly conducted activity."'.

Authentication measures allow network operators and regulatory authorities to trace electronic routes, although they cannot identify persons, for which see the successful defence in the German cases of OLG Köln, 19 U 16/02; LG Konstanz, 2 O 141/01 A; AG Erfurt, 28 C 2354/01,[4] in these 3 related cases, the seller was not able to prove that the buyers were the ones that entered into the contract on-line. However, biometric measurements may serve to authenticate individuals through the capture of unique data characterizing physical features of a person. Examples include a persons' finger or palm print, a laser scan of the retina and a voice point.

## Record keeping

Electronic record keeping in e-commerce transactions provides a helpful service for suspicious activities in cyberspace. Information on the nature of network traffic allows the understanding of broad trends in how people

[1] *http://www.incb.org/incb/index.html.*
[2] *553 F. 2d 1109, 1 Fed. R. Serv. 1374.*
[3] *673 F. 2d 86, 10 Fed. R. Evid. Serv. 333.*
[4] *Reported in the Digital Evidence and Electronic Signature Law Review 2 (2005) 105 – 106.*

obtain access to web sites. Record keeping is achieved through service logs, which register the trail of on-line transactions, the duration of on-line sessions and the identification of network address for business transactions. Basic information would be subjected to profiling techniques whereby patterns of transactional activities may be detected.

## Search and seizure

The case of Vladimir Levin,[5] in which computer hackers in St. Petersburg, Russia hacked into Citibank computers in the USA and transferred substantial funds, illustrated the new reality of digital evidence. This was a modern day bank theft that required no physical attendance, weapons, masks or a get-away vehicle. The fact that Levin was able to use his computers via several intermediaries and transfer substantial funds, shows innovative solutions are demanded. A collection of all related computer information for a search encounters challenges. Evidence collection is frequently interrupted, as few ISP administrators maintain comprehensive log records and registers. Invariably, records considered routine are deleted, as storage space is critical to network speed and capacity. Fraudsters are known to target intermediary computers that maintain inadequate or no record. Such lax records retard investigations and prosecutions of cyber offending.

In common law jurisdictions such as England and Wales, both prior to and after the passing of the Police and Criminal Evidence Act 1984, it has been trite law that the police may not ransack a person's home to look generally for evidence against him. A lawful entry into premises for a search and seizure must always relate to a specified purpose, and the search must be consistent with the stated purpose. In the USA, the Fourth Amendment prohibits unreasonable searches and establishes a reasonable expectation of privacy in the conduct of all searches.

The collection of digital evidence is paramount once the electronic trail leads to the offending computers. Digital evidence specialists have developed routine procedures on the seizure of an offenders' computer. Usually the machine is taken away from the location for examination. The justification for off site inspection is based on practical considerations. Most computers have large hard drives of 20-60 gigabytes. Even a routine examination would take considerable time, since most files may be suspicious or mislabeled to conceal their content. At the computer examination, forensic analysts could create a bit stream or mirror image of the hard drive. The bit stream copy is an exact duplicate and not mere files. Each bit and byte stored on the hard drive is duplicated for accuracy. The forensic examiner would use the copy for interrogation thereby preventing the original from damage.

A broad range of techniques may be employed by the analyst. For example, a string search may be executed for particular extensions or phrases including text links to the search. Secondly, all files with similar characteristics may be opened or sampled for the object of the search. Any nexus to the suspect will be explored from the hard drive to incriminate or link the offence to the suspect. In *United States v Grey*,[6] child pornography was found during a search under a warrant. The items were held admissible although the defendant argued that the files marked with JPG extensions were presumptively pictures and not related to the subject of the search. The courts ruled that hackers frequently mislabel files and the FBI was not required to take file names at face value.

The existing rules of criminal procedure have been developed over the years to cope with physical realities such as murder, rapes, burglaries and thefts. Current rules of collection of evidence cater largely for eye witnesses, what is seen, observed, touched and felt. As such the rules on search and seizure in common law jurisdictions have limited the scope of evidence collection. Searches are confined to persons and places. For example, police officers cannot require an individual to undress in public regardless of any suspicions they may have. Searches when authorized, especially by warrants, are circumscribed by consent, statutory authority or the existence of reasonable suspicion based on objective criteria. Seizure involves a meaningful interference with the possessory interest in property of another and is justified in certain circumstances. Collection of abandoned property is not seizure. Time limitation on such interference of property is crucial in the determination of its justification for seizure.

## The third party

The advent of the digital environment has spawned new realities that challenge the existing structure. The collection of digital evidence from third parties has opened interesting opportunities for law enforcement and regulatory bodies. In the United Kingdom, the

[5] *R v Governor of Brixton Prison, Ex p Levin; sub nom Levin (Application for a Writ of Habeas Corpus), Re [1997] A.C. 741.*

[6] *78 F.Supp.2d 544.*

 

Interception of Communications Act 1985, Drug Trafficking Act 1994, Security Services Act 1989 and recent prevention of terrorism legislation invariably make provision for the collection of intelligence on an ex parte basis. Review is subject to the judiciary, but intercepts of electronic communications exist for justifiable causes of national security and prevention of crime. Various threshold requirements must be satisfied that aim to balance privacy concerns. However, the result is that a subpoena, court order or interception order can be used to obtain digital evidence from a third party. ISP administrators are generally cooperative, as they are innocent third parties providing a service. The abuse of the electronic platform for offending removes any reasonable expectation of privacy from the offender. Moreover, no issue of self-incrimination as incorporated in the Fifth Amendment of the Constitution of the USA arises. ISP administrators may find it easier and less burdensome to comply by handing over the entire file with thousands of unrelated correspondences.

Generally, internet users store a good deal of private information on remote servers. Such information is easily accessible to ISP administrators who could read private e-mails, stored files and examine access logs that record the surfing of individuals on the World Wide Web. The ability to produce disclosure from the ISP can be equal to viewing the entire private world of an individual on-line. Such disclosure can relate to multiple accounts of subscribers without their knowledge or consent. As a result, investigators in the digital world can obtain disclosure of the entire profiles and surfing sites of individuals. The employment of subpoenas, court orders or intelligence interception orders without consent once statutory justification exists, is permissible.

Moreover, the use of prospective surveillance has allowed for the search of an individual suspect that accords with constitutional and statutory justification. The use of an intermediary through whom a hacker has passed is justifiable. As for example, in the *Levin* case, the fact that the hackers invaded several intermediary computers could result in a trail placed to monitor him in the future. The fact that the systems of innocent parties might be violated by hackers, enables the installation of monitoring filters with the consent of the third party to identify and trace future unwarranted incursions.

Existing surveillance monitors can identify the type of traffic, such as e-mails or messages. Filters could identify specific words or phrases along with internet addresses. However, filters cannot make judgments or exercise discretion as to what is private or public information. The binary characters of internet information in zeros and ones challenge not merely the technology but the ability to deduct its content. The context of the information along with the identification of the sender and receiver are usually not susceptible to affirmative proof. This provides an added challenge to the protection afforded by the law against unreasonable searches and seizure. However in *Halford v United Kingdom*,[7] Article 8 of the European Convention on Human Rights was held to protect the telephone calls made on a telephone specifically provided for personal use from the business premises at Merseyside Police Headquarters.

## Safeguards

The seemingly unchartered right of investigators to compel disclosure in search and seizure powers for digital evidence must be addressed. Claims for privacy and civil liberties as afforded by the constitutional and statutory powers have a role in the digital world. The tradition in common law jurisdictions is that searches must be executed when authorized within a reasonable time. For digital evidence there is no such implication, but it is relative due to the volume of documents and files to be scanned. Seized property must be returned if there is no charge filed or offence committed. In cases of physical evidence, courts have affirmed the need for fairness in the absence of search warrants. Usually a search warrant may be obtained upon sworn information. There is no need for a charge to be filed. Real evidence arising from a search may provide justification for a charge to be filed.

In *AG v Williams*,[8] the Judicial Committee of the Privy Council emphasized that the judge or magistrate who issues a search warrant must be satisfied that the applicant for such a warrant has reasonable grounds for suspicion. The magistrates must satisfy the appropriate legal threshold prior to the issue of a search warrant.

Further evidence obtained in pursuit of the specified object of the search warrant may be excluded if not relevant. The plain view exception as applied in the USA gives investigators wide latitude to obtain evidence of other crimes once the search was consistent with the execution of the warrant. Digital evidence is no different, and allows for even intrusive and wide ranging searches of hard drives over prolonged periods. The test

[7] *(1997) 24 EHRR 523.*
[8] *(1997) 51 WIR 264.*

of relevance for admissibility in criminal proceedings is equally applicable in the digital world.

However, some courts have begun to take a more measured view of digital search and seizure. Emphasis is being placed on the nature and extent of the information needed rather than on the location of the evidence. The content of public and private spaces for searches is immediately relevant for physical searches.

By contrast, searches and seizures of digital evidence has less to do with public and private location but rather the purpose of the information. In the case of *In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*,[9] Magistrate Judge Schenkier refused the government's request for the unchartered search of a home computer. The law enforcement authorities were required to undertake to follow a pre-approved protocol in a tax fraud case. The court reasoned that the absence of such approval would confer a license to roam through everything on the computer without limitation and appropriate standards. The need for a pre-approved protocol was justified on the basis of four conditions:[10]

> First, it is frequently the case with computers that the normal sequence of "search" and then selective "seizure" is turned on its head. Because of the difficulties of conducting an on-site search of computers, the government frequently seeks (and, as here, obtains), authority to seize computers without any prior review of their contents.
>
> Second, that is significant in this case because of the substantial likelihood that the computer contains an "intermingling" of documents evidencing the alleged tax fraud, with documents that the government has no probable cause to seize.
>
> Third, we consider the extraordinary volume of information that may be stored even on a home computer. ..... The capacity of the computer to store these large quantities of information increases the risk that many of the intermingled documents will have nothing to do with the alleged criminal activity that creates the probable cause for a search and seizure.
>
> Fourth, while computers present the possibility of confronting far greater volumes of documents than are typically presented in a paper document search, computers also present the tools to refine searches in ways that cannot be done with hard copy files. ..... computer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity. These methods include limiting the search by date range; doing key word searches; limiting the search to text files or graphics files; and focusing on certain software programs. See Carey, 172 F.3d at 1276. Of course, these are not the exclusive means of focusing a computer search, and they are not the means that might be appropriate in every case. But, the existence of these tools demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents in a file cabinet.

Accordingly, a new method may arise in which search and seizure of digital evidence may be subjected to time limits, such as, for example, 30 days or shorter periods as warranted. Moreover, the approach of law enforcement and regulatory authorities to retain seized computers and equipment for prolonged periods may be ending. Time limits as well as the need to return property in a useable manner after timely investigations should become the new standard.

Further, the retention of bit streams and copies of the hard drives of suspects should be governed by a new regime. Physical evidence is required to be returned and samples taken such as fingerprints or DNA tissues should be destroyed. Such destruction is common, although not in the UK, especially when suspects are exonerated or eliminated from an investigation. In most cases, copies of digital evidence are retained after the conclusion of an investigation. The existing rules are applied to physical evidence from a propriety point of view. Copies of digital evidence are not considered as such once the original hard drives, discs or CDs are returned to the owner. As such, enhanced protocols are needed to address the current realities in the digital area.

## Reforms

The search and seizure of digital evidence raise added concerns about the technical and resource challenges presented by computer encryption. Encryption is largely designed to ensure privacy and freedom of expression as a basic civil rights issue. The future of search and seizure of digital evidence should be marked by the following conditions:

[9] *321 F.Supp.2d 953 (N.D. Ill. 2004).*
[10] *321 F.Supp.2d 953 (N.D. Ill. 2004), at 958-959.*

 

(1) Public education such as information on web sites and the media on the harmful effects of financial crimes, child pornography and narcotics related substances.
(2) Development of software programs to track electronic transactions whereby an audit trail would be established for on-line commerce.
(3) Alliances must be forged by law enforcement and regulatory authorities with the private sector to combat high-tech crimes to ensure confidence in the market.
(4) Widespread adoption of model legislation for cyber crimes such as European Convention on Cybercrime and the United Nations Convention against Corruption.
(5) Enhanced investigative techniques such as prospective surveillance through innocent parties whose system was violated, for example a public library or museum.
(6) Effective compliance and oversight of law enforcement and regulatory authorities to report to courts or supervising bodies in order to minimize over-intensive surveillance.

## Conclusion

The existing rules of evidence collection, especially the search and seizure regime, is largely designed for physical evidence and eyewitness accounts. The advent of digital evidence has seen innovative measures to adopt existing rules to the electronic frontier. The result has been mixed, with measured success and outright violations that constitutional and statutory protections were designed to confer. A new ethos is required with the accent away from proprietary interest to the nature of the information sought and the technology in use to obtain it. The current review of the electronic world in much of the Anglophone world must address three major themes:

(1) The extent to which existing laws on search and seizure are sufficient to cope with unlawful conduct on the internet.
(2) To what extent new technologies, tools, capabilities or legal authorities could be used for effective investigation and prosecution of cyber conduct, especially the search and seizure regime.
(3) The role of education and public awareness to reduce cyber offending and enhance the reception of digital evidence.

The existence of digital evidence is a reality in 2008. There must be wide support for self regulation and the development of cyber ethics by ISPs and web hosts. Such self-regulation will lead to greater compliance with evolving standards and uniform conduct. As such, information will become more accessible and reduce the level and intensity of invasive monitoring and intrusions into civil liberties. The rules on search and seizure for digital evidence would, in reality, become routine and standardized as the existing regime relating to physical evidence.



*Charles Leacock graduated from the Hugh Wooding Law School, Trinidad and Tobago (1983) with the Certificate of Legal Education, having previously obtained the LL.B (Hons) from the University of the West Indies (Cave Hill Campus) (1981). He was awarded the LLM degree in Criminal Justice from the University of London (1993).*

[7] *(1997) 24 EHRR 523.*
[8] *(1997) 51 WIR 264.*