The ITB Journal

Volume 8 | Issue 2 Article 3

2007

Computer Forensics and Irish Law

Anthony J. Keane

Follow this and additional works at: http://arrow.dit.ie/itbj

 Part of the Criminology Commons

Recommended Citation

Keane, Anthony J. (2007) "Computer Forensics and Irish Law," *The ITB Journal*: Vol. 8: Iss. 2, Article 3.
Available at: http://arrow.dit.ie/itbj/vol8/iss2/3

This Article is brought to you for free and open access by the Journals Published Through Arrow at ARROW@DIT. It has been accepted for inclusion in The ITB Journal by an authorized administrator of ARROW@DIT. For more information, please contact yvonne.desmond@dit.ie, arrow.admin@dit.ie, brian.widdis@dit.ie.

This work is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 License

Computer Forensics and Irish Law

Anthony J. Keane, MSc, PhD
Lecturer in Department of Informatics,
School of Informatics and Engineering,
Institute of Technology Blanchardstown

Abstract

They say that ignorance of the Law is not a defence but how many people could really say that they have any idea of the legislation regarding compute use. The answer is not many and therefore most computer users do not know if their activities are considered illegal or illegal, other then the obvious ones that appear from time to time in the news media and normally involve fraud, theft or child pornography. This paper is a short overview and discussion of the Irish legislation that can be applied to computer activities and how "computer crime" is dealt with in Irish law courts.

Introduction

The Internet is a communications system that allows access to resources and people throughout the World. It has been adopted by business as a means of increasing their customer base and improving their ability to provide their service. Criminals have not been slow to take advantage of the anonymity that the Internet offers and to use the Internet to commit fraud and theft in many highly imaginative ways. The mechanism of the Internet is based in technology protocols, many of which are open standard and easily available, so with a little effort in educating one self on the inner working of the Internet, the criminal mind can conceive ways of misrepresenting themselves and trick the remote user into divulging their personal details, financial details, user access codes and passwords. Who hasn't received a spam email asking for bank details, offering to get large amounts of money for a small deposit, and similar type get rich quick schemes. Other tricks are not illegal but border on being so and are defiantly unethical, are the selling of special drugs reporting that they can satisfy some social desire on the part of the customer.

In the 1990s, the business of computers involved moving business practices from paper based systems to computerised networks. This was also the age when security became a necessity to protect the data on computers and ensure its integrity. It was not until the advent of World Wide Web and MS-Windows 95 with built in web browser application that the exponential growth in the Internet took place. Now every business wanted to be on the Web and every user wanted to have email. It is estimated today that they are over 1 billion users on the Internet and many of them are targeted everyday to relieve them of their cash and identity. According to the results of "The ISSA/UCD Irish Cybercrime Survey 2006: The Impact of Cybercrime on Irish Organisations" report[1], Irish organisations are significantly affected by cybercrime where virtually all (98%) of respondents indicated that they had experienced some form of cybercrime with losses of productivity and data being the main consequences.

It is from the explosion of growth in computer use that a new field of computer science has emerged to deal with computer related crime and it is called Computer Forensics. It was initially developed by police enforcement agencies, like FBI where techniques,

tools and best practices were needed for information in a crime to be extracted from computer storage devices and used as evidence in the prosecution of the case. Today the Computer Forensics field has many contributors with propriety application tool kits for analysing storage media, open source tools, academic research groups, professional companies specialising in Security and Forensics and law enforcements agencies.

There are three areas of demand for the services of a computer forensics professional, the criminal area, the corporate requirement, the private / civil area. Here we look at the criminal area and concentrate on the legislation in force in Ireland that is available for prosecution of computer related crimes. We ask the following questions: How is the legislation framed and what computer related activities are considered illegal?

Irish Legislation

Most of the computer crime related offences are handled by the Criminal Damage Act, 1991[2], Section 9 of the Criminal Justice (Theft and Fraud) Offences Act 2001[3] and the European Convention of Cybercrime[4].

Criminal Damage Act 1991, Section 5

(1) A person who without lawful excuse operates a computer—

(*a*) within the State with intent to access any data kept either within or outside the State,

or

(*b*) outside the State with intent to access any data kept within the State,

shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.

(2) *Subsection* (*1*) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.

The unauthorised access to information (data) is handled by the Criminal Damage Act, 1991 and is supposed to safeguard the possibility where a "hacker" has not committed any damage, fraud or theft but has tried or succeeded to gain access to a computer system.

O'Brien[5] has the following interpretations regarding this part of the legislation:

- In procuring a conviction, it is not necessary to establish a mens rea, provided the offender intended to access some data. The actus reus is satisfied when a person interacts with a computer, for example the pressing of the "return key" would be sufficient for the offence to occur, whether or not that person intended to access any authorised data.
- The offence is further expanded by criminalising attempted access regardless of whether any data is successfully accessed, for example an offender has been repealed in their attempt to breach a network security system.

- O'Brien suggests that the scope of this offence is so wide it can encompass any activity involving the use of a computer, for example if an honest user attempts to login to their email account and accidentally input the incorrect password, then under the Act, they have committed an offence.

When a system is damaged, then Section 2 of the Criminal Damage Act, 1991 is used. This creates the offences of intentional or reckless damage to property. While the wording of the Act does not explicitly use computer terms like virus, O'Brien suggests that this offence could be applied to damage caused to a computer system by a virus or similar attack. Reckless damage under section 2 has as the penalties a minimum fine of €12,700 to a maximum imprisonment for a term not exceeding 10 years or both.

Section 6 of the Criminal Damage Act, 1991 deals with the phrase "without lawful excuse". O'Brien interrupts this to mean anyone accessing any type of data from their PC or a network where they have authorised privilege to use, is not committing a crime. In the UK, the courts have ruled that authorised access of some data could not exonerate those who committed an unauthorised access of other similar data, however it still remains to be tested in Irish courts to see if they will adopt a similar approach.

One of the problems with the legislation is the poor definition of computer terms, for example data and computer. The reason given for this approach is to prevent the legislation from becoming obsolete by the rapid advancement of technology. However the range of meaning of data could lead to a scenario outlined by Karen Murray[6];

"The Criminal Damage Act 1991 has sought to avoid ambiguous definitions by avoiding a definition at all. This may have bizarre results; the human memory is undoubtedly a "storage medium" for 'data'; if a hypnotist causes a person to forget something, have they committed criminal damage?"

Murray argues that such vagueness may be subject to a Constitutional challenge in Ireland under the doctrine where *"the principle that no one may be tried or punished except for an offence known to the law is a fundamental element of Irish and common-law system and essential security against arbitrary prosecution".*

In other words, if there is no way of determining what the law is, there is no crime" .

Criminal Justice (Theft and Fraud) Offences Act 2001, Section 9

(1) A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

(2) A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

In the year 2000, the Electronic Commerce Act was signed into force by the President of Ireland and created the legislation framework for conducting commercial transactions online. This was soon followed in 2001 by the Criminal Justice (Theft and Fraud) Offences Act in which section 9 has provision for "unlawful use of a computer".

However, O'Brien claims the scope of the offence is too broad having the possibility of criminalising anyone who made a gain by the use of a computer. He said that it "*may be impossible to know where free-market capitalism ends and dishonesty gains begin*". However he also prises the Act for use to combat hacking activities like denial of service attacks where a loss of business is possible.

The European Convention on Cyber-Crime[7]

Since 1995 the EU has been trying to get a consensus on how to tackle cross-border Internet related criminal activities. In 2001 it finally got an agreement to what has become known as the Convention on Cybercrime. Ireland became a signature to it in 2002 but it only came into force on 1st July 2004. The cybercrime convention represents the first international attempt to legislate for cross-border criminal activity involving computers. In the broad definition of computer crime, the term cybercrime is viewed as a subcategory and generally associated with the Internet. The Convention on Cybercrime covers the following three broad areas:

- All signatures criminalise certain online activities
- States should requires operators of telecommunications networks and ISPs to institute more detailed surveillance of network traffic and have real-time analysis
- States cooperate with each other in an investigation of cybercrime by allowing data to be shared among them "but with an opt-out clause if investigations of its essential interests are threatened".

As the legislation reflects the needs of law enforcement rather than public interest groups, opponents of the Convention have cited the lack of privacy issues and forced cooperation clause as endangering the right to privacy for citizens in the EU.

Some Closing Comments

Before leaving you with the Tsunami case to ponder, it is evident that from this paper that cyber criminals and ordinary computer users can be prosecuted under various Acts but the success of the case may depend on the interruption of the law to that particular crime, at that time, *"Laws which are not specifically written to prohibit criminal acts using computers are rarely satisfactory*"[8].

The Tsunami Case

In 2005 a college lecturer and security consultant, Daniel Cuthbert was moved by the devastating images of the Asian Tsunami disaster and donated money via a charity website. He entered his personal details like name, home address and credit card details but after a few day he became concerned that he had given his details to a spoof phishing site run by criminals. In an attempt to find out more about the site he did a couple of very basic penetration tests. If they resulted in the site being insecure as he suspected, he would have to contact the authorities. The first test he used was to type the (dot dot slash, 3 times) ../../../ sequence into his web browser. This is part of a command to exploit a bug in some web servers that allows you to see parts of the site that are not normally available to the public. As this is not a complete attack as that would require a further command, but merely a light "knock on the door". Having tried this twice and received no response, he assumed the site was ok and went about his

normal work. There were no warnings or dialogue boxes showing that he had accessed an unauthorised area but he had triggered a intrusion detection system (IDS) at the company that ran the site and they called the police. A few weeks later he was arrested at his place of work and had his house searched. He was prosecuted under the UK Computer Misuse Act 1990[9] and the relevant section of the Act is Section 1 states:

(1) A person is guilty of an offence if –
   a. he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
   b. the access he intends to secure is unauthorised; and
   c. he knows at the time when he causes the computer to perform the function that this is the case.

Due to the wide scope of the Act, the Judge, with 'some considerable regret' had no option but to find Daniel Cuthbert guilty under the Computer Misuse Act 1990 and he was fined. He was also dismissed from his job. While this is English law and we don't have an equivalent Irish case, as yet, it does highlight the care needed when performing a penetration test if you are to be confident that you are not acting illegally.

References

1. "The ISSA/UCD Irish Cybercrime Survey 2006: **The Impact of Cybercrime on Irish Organisations"**, http://www.issaireland.org/cybercrime
2. Criminal Damage Act 1991. http://www.irishstatutebook.ie/1991/en/act/pub/0031/index.html
3. Criminal Justice (Theft and Fraud) Act 2001 http://www.irishstatutebook.ie/2001/en/act/pub/0050/index.html
4. **European Convention on Cybercrime** http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
5. Rory McIntyre-O'Brien, **"**Slipping Through the Net: Hacking Offences in Ireland", ***Cork Online Law Review*** VIII, 2005
6. Karen Murray, "Computer Misuse Law in Ireland", May 1995 Irish Law Times 114
7. Adrian Bannon, "Cybercrime Investigation and Prosecution – Should Ireland Ratify the Cybercrime Convention", ***The Galway Student Law Review***, Vol 3, 2007
8. Dennis Kelleher and Karen Murray, ***Information Technology Law in Ireland*** 1997 Dublin ; Sweet & Maxwell p.253.
9. Computer Misuse Act 1990 http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm