

Chapter 10

Music, Video and Software Piracy: Do Offenders See Them as Criminal Activities?

ABSTRACT

Of all the types of cybercrime considered in this book, piracy, illegal file sharing and/or other types of copyright infringement are probably the offences that members of the general public are most likely to have committed. Yar (2007) indicates that piracy activity seems to be very widespread, including individuals from various social classes, although there seems to be a disproportionate number of young people engaging in the activity. This chapter aims to determine if those involved in piracy and online copyright infringement activities see themselves as criminals. It also aims to examine how such offenders justify their actions and how they can be dissuaded from such acts. Definitions of key terms in the area will be presented, along with some examples of real events relating to illegal file sharing. A description of some of the methods used during illegal file sharing and piracy will be provided, along with a historical view of how copyright infringement has developed over time. The known current prevalence rates and costs of offending will be considered, along with arguments presented from industry and academia regarding the effects of file sharing on legitimate sales. Similarly, the problem of trying to estimate the true cost of piracy and illegal file sharing will be highlighted. The psychology of offenders will be considered, and in particular, the phenomenon of the lack of insight of offenders into their own criminality will be investigated. In particular, the roles of self-control, social learning and justifications in illegal file sharing will be analysed. Some potential solutions for these crimes will be considered, including the determination of appropriate punishments and the development of suitable educational campaigns. Finally, potential future trends and research will be described.

DOI: 10.4018/978-1-61350-350-8.ch010

BACKGROUND

There have been several high profile cases of online file sharing websites in recent years.

Yar (2007) describes the case of a file-sharing service called Napster. When using this service, individuals registered online and downloaded the Napster software, which would then scan the user's computer for any digital music files (such as MP3 files). The software then sent a list of the music files on the computer to the Napster server. If another user then searched for a specific song, Napster would inspect its members' computers for copies of it, while also checking which of these computers were currently online. Napster then allowed the searcher to ask the file owner for permission to download a copy of the file for themselves. Eventually approximately seventy million individuals were using the system. In late 1999 the US recording industry took Napster to court, suggesting that the file sharing website had facilitated illegal downloading of copyrighted material. Napster eventually paid \$36 million to the recording industry (Yar, 2007, p. 98).

Jewkes (2010) describes the case of 'The Pirate Bay' (p. 534). This Sweden-based website allowed people to post music, films and software, and directed users to media files available elsewhere on the Internet. 'The Pirate Bay' did not store the content or index itself, and so circumvented anti-piracy laws. Nevertheless, in 2009, the four owners of 'The Pirate Bay' were found guilty of breaking copyright law, were fined and were sentenced to a year in prison each.

In October 2010, a New York district court issued an injunction which forced 'LimeWire', a large file-sharing website, to disable some of its functions, including searching, downloading, uploading and file-trading (BBC News, 2010a).

Definitions and Key Terms

There are a large number of terms which are used in conjunction with the illegal distribution of copyrighted material. Bryant (2008) distinguishes between 'illegal filesharing' and 'commercial music piracy'. The former involves the transmission of files, while the latter involves the use of physical materials such as CDs and DVDs. However, many researchers use the term 'piracy' to refer to illegal filesharing as well. For example, Hill (2007) defines digital piracy as "the purchase of counterfeit products at a discount to the price of the copyrighted product, and illegal file sharing of copyright material over peer-to-peer computer networks" (p. 9).

Yar (2006) indicates that it has proven to be difficult to settle upon a precise and agreed definition of 'piracy', but that legal and economic uses of the term are based in Intellectual Property (IP) law and protection (p. 65). Stephens (2008) describes Intellectual Property Rights (IPR) as "encompassing the privileges accorded to the creators and owners of creative work (intellectual property, or IP) including inventions, designs, software, music, films, and written works" (p. 121). Stephens indicates that copyright does not require a registration process, and in most cases the copyrighted work can only be reproduced and used with the copyright holder's permission. If it is otherwise used, the holder has a legal right to stop the copyright breach and to seek compensation.

There are complications in defining the legality of copyright infringement. Stephens (2008) indicates that some consumers argue for 'fair use' of the content, suggesting that they should be entitled to make copies of the content for personal use. For example, a person may buy a music CD. They may then wish to make a copy of the CD to leave in their car. They may also want to copy the CD to mp3 format so that they can listen to it

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/music-video-software-piracy/60689

Related Content

Probabilistic Evaluation of SMS Messages as Forensic Evidence: Likelihood Ratio Based Approach with Lexical Features

Shunichi Ishihara (2012). *International Journal of Digital Crime and Forensics* (pp. 47-57).

www.irma-international.org/article/probabilistic-evaluation-sms-messages-forensic/72324/

Evidentiary Implications of Potential Security Weaknesses in Forensic Software

Chris K. Ridder (2009). *International Journal of Digital Crime and Forensics* (pp. 80-91).

www.irma-international.org/article/evidentiary-implications-potential-security-weaknesses/3910/

A Simulation Model of IS Security

Norman Pendegraft and Mark Rounds (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 214-227).

www.irma-international.org/chapter/simulation-model-security/60950/

An SOA-Based Architecture to Share Medical Data with Privacy Preservation: An SOA-Based Architecture to Share Medical Data with Privacy Preservation

Mahmoud Barhamgi, Djamal Benslimane, Chirine Ghedira and Brahim Medjahed (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 310-324).

www.irma-international.org/chapter/soa-based-architecture-share-medical/60956/

Evidentiary Implications of Potential Security Weaknesses in Forensic Software

Chris K. Ridder (2009). *International Journal of Digital Crime and Forensics* (pp. 80-91).

www.irma-international.org/article/evidentiary-implications-potential-security-weaknesses/3910/