# RELEASE GROUPS & DIGITAL COPYRIGHT PIRACY

by

Jonathan R. Basamanowicz
Bachelor of Arts, John Jay College of Criminal Justice, 2008

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

In the

School of Criminology



SIMON FRASER UNIVERSITY

Summer Term 2011

# APPROVAL

**Name:** **Jonathan R. Basamanowicz**

**Degree:** **Masters of Arts**

**Title of Thesis:** **Release Groups & Digital Copyright Piracy**

**Examining Committee:**

**Chair:** **Dr. Neil Boyd**
Professor and Associate Director of Graduate Programs

_____

**Dr. Martin Bouchard**
Senior Supervisor
Assistant Professor

_____

**Dr. Eric Beauregard**
Supervisor
Assistant Professor

_____

**Dr. David MacAlister**
Supervisor
Associate Professor

_____

**Dr. Benoit Dupont**
School of Criminology
University of Montreal

**Date Defended/Approved:** May 17, 2011

# Declaration of
# Partial Copyright Licence

# ABSTRACT

This study uses data gathered from three US Federal policing operations occurring between 2001 and 2005 that targeted *release groups* – organized file-sharing groups that obtain commercial content, remove the copyright protection features, and distribute it – and their illicit networks. This data was used to construct a *crime-script* of these groups' *modus operandi* to discover methods of disrupting their criminal activities. The results indicate that Industry may increase the risk of releasing content through amendments in DRM, and law enforcement may increase the effort through targeting crackers in prominent release groups. As well, data from a sub-operation of Site Down known as Operation Copy Cat was examined to re-construct a 2-mode network of actors and servers that aimed to distribute copyrighted content. The results of this analysis reveal that although only three individuals received a term of imprisonment, there were as many as five other actors in the network with comparable network centrality that evaded this harsh sentence.

**Keywords:** Cyber-Crime; Digital Piracy; Organized File Sharing; Warez; Release Groups; Criminal Networks; Situational Crime Prevention; Social Network Analysis; Crime-Scripts.

.

# ACKNOWLEDGEMENTS

I owe so much of the following work to the help, support, and encouragement of many people. Chiefly, the following were positive influences, and I am grateful to them for their teachings.

**Dr. Martin Bouchard** – Your guidance and assistance in these research endeavours have been invaluable - without your aid, none of this would be possible.

**Dr. Kirk Dombrowski** – Your lectures have shaped my perspective on human behaviour more-so than anyone else.

**Dr. Susan Opotow** – Your support and encouragement to continue learning have steered me to this.

**Angela** – Love you.

-**Thank You**,

Jonathan

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# 1: INTRODUCTION: THE INTANGIBLE'S VALUE

Mark Getty, CEO of Getty Images and grandson of oil-tycoon J. Paul Getty, said in an interview with *The Economist* that "[i]ntellectual property is the oil of the 21st century" (*The Economist*, March 2, 2000). Despite the context of this quote's reproduction, it is often cited by interest groups on both sides of the intellectual property debate as it imbues an inherent truth about the information age: information, in all forms, is a commodity. Seeing that Getty Images reported an annual revenue of more than $850 million in 2007 (Pickerill, Klein, & Oberdorf, 2008), Mark Getty might be onto something. A report by the International Intellectual Property Alliance (IIPA) estimated that copyright industries accounted for upwards of $1.5 trillion, or approximately 11%, of the United States Gross Domestic Product and employed approximately 11.7 million people in 2007 (Siwek, 2009). As these figures increase each year, it is notable that Bill Gates, former CEO of Microsoft, was once quoted in an interview in 1980, saying: "There's nobody getting rich writing software [a form of intellectual property] that I know of…".[1] The former not-rich software-writer's corporation Microsoft reported a revenue growth of an astonishing $7 billion for 2007 (Healy & Liddell, 2007).

With a significant attribute of information being its ease of reproduction, it is no wonder why Getty and others have fancied it as their commodity of choice. One copy can quickly and cheaply become many. This attribute of information is

[1] See <http://features.slashdot.org/article.pl?sid=00/01/20/1316236&mode=thread> Retrieved on February 7, 2011.

both the benefit and burden of Intellectual Property (IP) industries as it is more expensive to construct information than to reproduce it. As such, IP laws operate to curb this phenomenon by granting creators of information exclusive rights over the reproduction and distribution of their creations. Thus, as reproducing information is inexpensive and sometimes cost-less, IP industries are able recoup their losses from developing new information through their exclusive rights to reproduce this information (*Intellectual property rights in an age of electronics and information*, 1986, p. 158-159). Recording industries, for example, are estimated to return the initial cost of production on, at most, 10% of all records sold; thus, more than 90% of all records released cost the industry. However, because of the low cost of reproduction, returns from the 10% of records that do sell make up the losses from the other 90% - and then some (Leyshon, Webb, French, Thrift, & Crewe, 2005, pp. 186-187). IP industries depend on IP laws such as copyright to ensure not only their success but also their survival. Ostensibly, these industries are in the business of controlling information; and with copyright industries producing 11% of the USA's total GDP (Siwek, 2009) - business is good.

There are, however, the unexpected costs of doing business. For IP industries this is represented by infringements on their IP; regarding copyrights, this equates to the unauthorized reproduction, distribution, or sale of their copyrighted works (See Title 17 USC). It is estimated that copyright piracy costs the US economy more than $58 billion and 373,375 jobs annually (Siwek, 2007), and in Europe, it is estimated to cost creative industries as much as €10 billion

and 185,000 jobs annually (Tera Consulting, 2010). Music piracy alone, according to the Recording Industry Association of America (RIAA), results in a $12.5 billion economic loss annually;[2] in 2005, they report that over 5 billion pirated/counterfeited CDs, Cassettes, and music DVDs had been seized (RIAA, 2005). These figures, as well as the seemingly constant warnings by the Motion Picture Association of America (MPAA) and other copyright interest groups, demonstrate the severity and prevalence of copyright piracy. Some scholars even suggested that by 2010 it would be impossible to enforce copyright laws on the Internet (Pouwelse, Garbacki, Epema, & Sips, 2008, p. 711).

Copyright piracy has seemingly become a common occurrence, and with household bandwidth speeds increasing (Internet World Statistics, 2010) and tools of piracy becoming easier to operate (Wang, 2004), it can be expected for these figures to increase. However, pirated materials do not begin in the swarms of torrent networks, but rather from individuals collaborating in a clandestine digital environment actively working to distribute copyrighted materials around the world: called *release groups* (Howe, 2005; Rehn, 2004; Lee, 2002). *Release groups* work to obtain copyrighted content, strip the copyright protections from this content, and distribute it amongst other individuals participating in a global online community, called the *warez scene* (Craig et al., 2005; Goldman, 2004; see CCIPS, *Operation Buccaneer*) or "Warez World" (coined by McCandless, 1997). These groups compete to see who can release the newest content as fast as possible, and they seem very good at it – groups such as 'Drink or Die' have

[2]See <http://www.riaa.com/physicalpiracy.php> Retrieved on February 12, 2011.

released content to the scene as early as two- weeks prior to its commercial release date (Urbas, 2006). All the while, these groups operate under a strict non-profit ethos (Rehn, 2004; Cooper & Harrison, 2001; McCandless 1997), often matched with ideological vigour (Goldman, 2005; Goldman, 2004; Goldman, 2003). In the scene, copyrighted content has no monetary value, but an alternative value scale.

The protection of copyrights is a serious issue to some and a game to others. Interest groups lobby to ensure the enforcement of copyright law. Fortune 500 companies maintain and expand their empire on the comodification of intangible content. Policing organizations have enacted specific task forces and orchestrated elaborate operations to apprehend and disband organized file-sharing groups. Individuals have been imprisoned for distributing and downloading content.

This thesis will shed light on this esoteric community of cyber criminals that satiate the Internets' want of copyrighted content. It will focus on release groups, and it aims to expand literature on their motivations, *modus operandi*, and network architecture – with the end goal of both explaining how these groups operate as well as means of disrupting their activities. Chapter 2 will begin by detailing relevant issues within the copyright debate - describing copyright law's history and current amendments to US copyright law significant to digital piracy. Next, this thesis will outline a brief history of digital piracy, the *warez scene*, and delve into literature pertinent to this study: focusing on Situation Crime Prevention and Social Network Analysis.

Then, chapter 3 will explain the data sources for this study: primarily, court case data from 3 US Federal policing operations targeting these groups - Operations Buccaneer, Fastlink, & Site Down (as well as a sub-Operation of Site Down, known as Operation Copycat). Operation Buccaneer, an 18 month undercover operation ending in 2001, was one of the first federal attempts to police these clandestine networks  and targeted the notorious release group "Drink or Die" (DoD) (Urbas, 2006; US DOJ, Dec. 11, 2001). Operation Fastlink followed, ending in 2004, and targeted groups such as "Fairlight" (FLT) and "MaGe" (US DOJ, Apr. 22, 2004). The next iteration came in 2005 with Operation Site Down, targeting groups such as "RISCiso" (US DOJ, Jun. 30, 2005). A sub-operation of this was Operation Copycat, an undercover operation of a network of sites operating in Northern California (US DOJ, Apr. 6, 2006). In sum, these policing operations have elicited well over 100 arrests and culminated in the largest intervention of federal policing agencies on release groups.

These data will be employed to construct a crime script (Cornish, 1994) of the steps required for release groups to successfully release copyrighted content. This crime script will outline details of this process which will elucidate actions that industry and law enforcement may take to disrupt these groups' attempts to release copyrighted content. As well, data gathered from Operation Copycat court cases will be employed to reconstruct a 2-mode network (Borgatti, 2011; Borgatti & Everett, 1997) of users and sites that were distributing content. No studies have been conducted on these illicit networks, and it is unknown if network centrality plays a role in the sentence participants in this crime receive.

# LITERATURE REVIEW

## 1.1 Copyright law

In May, 2010, a number of film production companies, one of which was Voltage Pictures, unleashed a storm of lawsuits targeting tens-of-thousands of individuals for illegally downloading movies such as *The Hurt Locker* (2008). The film, in spite of winning six Oscars (including 2010 Motion Picture of the Year), only grossed approximately $16 million in the US. By subpoenaing Internet Service Providers, individuals who downloaded the film via BitTorrent were identified and threatened with suit to elicit a settlement of $1,500 from each individual. The law firm responsible for the suit reported that they intend to sue over 50,000 individuals for the unlawful downloading of *The Hurt Locker* and other films (Gardner, 2010; Sandoval, 2010). In an interesting turn of events, *The Hurt Locker*'s producers themselves were sued by Master Sgt. Jeffrey Sarver, an army bomb-disposal expert, who has claimed the producers had based the main character off him. Sarver asserts that the screenwriter, Mark Boal, was embedded in his military unit in 2004 and used the information gathered during that time to write an article for Playboy magazine, which was later modified to make the screenplay for the film (Hinds, 2010).

The case of a film studio suing tens-of-thousands of people for stealing a film that's adaptation of the main character may have been stolen from the individual it is based on, besides being saturated with irony, is just one example

which demonstrates the complexity of intellectual property. Since the inception of the 1976 Copyright Act, there have been no fewer than 60 amendments to US federal copyright law.[3] The following section will outline a brief history of criminal copyright law in the US - discussing the first copyright laws through the 1976 Copyright Act. Next, it will detail two recent amendments to copyright law that are significant to the criminalization of digital copyright piracy - the 1997 No Electronic Theft (NET) Act and the 1998 Digital Millennium Copyright Act (DMCA).

### 1.1.1 Brief History of Copyrights

Significant to understanding the rationale of the ideology of release groups, or even end-user piracy, a brief history of copyright may illuminate the perceived unjust nature of these legal protections. The genesis of copyrights are embedded in a setting of ecclesial and government efforts to control the activities of the press in tandem with efforts of publishing guilds to gain control of the book market. In England around the 1500-1600's, the Crown required a means of controlling the book trade to establish order and censure works. To adjudicate this issue, the English government vested the power of granting a right to publish books in the hands of the Stationers Company, a publishing guild, which held a monopoly on the book trade in England. Early English law, thus, required individuals whom wished to publish printed works to receive a publishing right from the Stationers Company. The Crown was able to regulate the book trade

[3] This was established by counting the number of amendments listed on the US Copyright Office's website at http://www.copyright.gov/title17/92preface.html on July 19, 2010.

with the Stationer's executive power, and the Stationers received a monopoly on the English publishing industry.

By 1694,[4] foreign publishers were importing books into England and undercutting English publishers. The Stationers, not wishing to compete, influenced Parliament to resolve the issue with legal solutions, and the answer was the enactment of the *Statute of Anne*, in 1709, which transferred ownership of a copyright from a publisher to an author (Lessig, 2004; Lunney, 2001; Patterson, 1968). This obstructed foreign publishers from printing and importing English works to compete with the Stationers, but it came with a catch – copyrights were limited to a maximum of 21 years (Id.). The statute was enacted as: "[a]n act for the encouragement of learning". By limiting the timeframe of a copyright, transferring ownership from publishers to authors, and creating the concept of the public domain, the Statute of Anne simultaneously placed a check on the Stationers monopoly of printed works and encouraged the creation of new works through a financial motive.

It was these concepts that influenced the drafters of the US Constitution when writing on the powers of the US to grant protections over intellectual property (Lessig, 2004; Patterson, 1968). Article I Section 8 of the Constitution reads: "The Congress shall have Power ... To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries". Though the financial incentive is maintained through various exclusive rights granted by

[4] Note:This refers to the expiration of the *Licensing Act*. Lunney (2001) & Patterson (1968) cite this as 1694, while Lessig (2004) cites this as 1695.

copyright law, an essential distinction that must be made of copyrights in constitutional law is that they are bestowed to authors to encourage the creation of new works first and to reward authors second (United States v. Paramount Pictures, Inc., 1948; Fox Film Corp. v. Doyal, 1932). An issue of controversy that is cited by supporters of copyright reform (Lessig, 2004).

Moving to criminal copyright, under the Copyright Act of 1976, criminal copyright infringement, in section 506, was limited to "[a]ny person who infringes a copyright willfully and for the purpose of commercial advantage or private financial gain". As such, individuals who recorded TV shows or movies on home VCRs or created home mix tapes on cassettes were not liable to criminal charges provided that there was no 'commercial advantage or private financial gain' involved. This is not to say copyright industries agreed with the free sharing of their content. In fact, in a hearing before a Congressional Subcommittee, Jack Valneti - the president of the MPAA at the time - was quoted saying, the now infamous statement: "I say to you that the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone" (*Home Recording Of Copyrighted Works*, 1982). This issue was brought about before the Supreme Court in the case of *Sony Corp. of America v. Universal City Studios, Inc*. (1984), and fortunately for home video collections everywhere, the US Supreme Court saw it differently, and they ruled that if new technology was more likely to be used for legitimate purposes that otherwise, it was fair game (Sony Corp. of America v. Universal City Studios, Inc. (1984)).

Sharing content in the absence of a financial motive, thus, is not a new phenomenon, and the advent of digital copyright piracy was met with similar resistance by industry and law-makers. To redress this issue, digital file-sharing was challenged with two major changes to copyright law in the late 1990s: the 1997 No Electronic Theft Act (or NET act) and the 1998 Digital Millennium Copyright Act (or the DMCA).

### 1.1.2 The NET Act (1997) & The DMCA (1998)

The No Electronic Theft (NET) Act of 1997 was inspired by the case of *USA v. LaMacchia* (1994). David LaMacchia, a twenty-one year-old student at the Massachusetts Institute of Technology, had set up a computer bulletin board system (BBS) under the name of 'Cynosure'. Individuals who had the password to access this system could upload and download copyrighted software free of charge and without the consent of the copyright holders. In April of 1994, LaMacchia was charged with violating a federal wire fraud statute, with the indictment stating that he had caused losses of over one million dollars to copyright holders. The prosecution argued that "LaMacchia subjected himself to the wire fraud statute by advertising infringing software via computer transmission" (Id. p. 542). In a shocking decision, the judge dismissed the charge, claiming that wire fraud cannot be committed with intellectual property. As well, LaMacchia's actions did not meet the requirements of criminal copyright infringement. At the time, criminal copyright infringement was unchanged from the 1976 Copyright Act and required that one must act "for the purpose of commercial advantage or private financial gain" to be punishable. As LaMacchia

did not intend either ‘commercial advantage or private financial gain’, the judge could not foresee how he had committed criminal copyright infringement. Though the judge dismissed the charge, he concluded his opinion stating:

> *This is not, of course, to suggest that there is anything edifying about what LaMacchia is alleged to have done. … Criminal as well as civil penalties should probably attach to willful, multiple infringements of copyrighted software even absent a commercial motive on the part of the infringer. One can envision ways that the copyright law could be modified to permit such prosecution. But, it is the legislature, not the Court which is to define a crime, and ordain its punishment* (Id. p. 545, quotations omitted).

Responding to the proclamation of the judge, lawmakers aimed to rectify this loophole in criminal copyright law by enacting the 1997 No Electronic Theft (NET) act, which criminalized this form of digital copyright infringement. The act redefines ‘financial gain’ to include “… receipt of anything of value, including the receipt of other copyrighted works”. This change, alone, is enough to criminalize traditional file-sharing, providing one can demonstrate that the defence had committed the act wilfully. However, in the case of LaMacchia, the prosecution had alleged that LaMacchia had administrated ‘Cynosure’, but did not demonstrate that he participated in file-sharing himself (Goldman, 2003, p. 372). As such, another clause needed to be included to ensure individuals who enable file-sharing but do not participate may still be liable. The act added a new subsection under section 506 to include wilful infringement “by the reproduction or distribution, including by electronic means, during a 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value or more than $1,000”. The act continues to amend evidentiary rules,

increase penalties for copyright infringement, allows for victim impact statements to be submitted, and orders the US Sentencing Commission to make the sentencing guidelines for criminal copyright infringement stricter (Goldman, 2003).

Thus, the NET act criminalized warez trading or, later with p2p networks, more common place file-sharing. However, several issues continued to be a thorn in the paw of copyright industries. Particularly relevant to warez groups is the act of 'cracking', stripping copyrighted materials of their copyright protection software. Under the NET act individuals who cracked software for personal use were not liable to criminal or civil prosecution (Goldman, 2003). As such, lawmakers aimed to amend this issue with the Digital Millennium Copyright Act (DMCA).

The DMCA, enacted in 1998, ratified two 1996 World Intellectual Property Organization (WIPO) treaties. The legislation focused on global and digital copyright issues, and aimed to amend copyright laws for the digital age. Though the legislation modified a number of legal issues, of material concern to the issue of warez groups was the criminalization of the cracking through the "Circumvention of Technological Protection Measures" statute (See DMCA § 1201 at http://www.copyright.gov/legislation/pl105-304.pdf retrieved February 13, 2011). This provision created 17 USC 1201; which reads: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title". Individuals who met the requirements of this law, were subject to civil remedies under 17 USC 1203 and/or criminal remedies under 12

USC 1204 – which included up to a term of five years imprisonment and a $500,000 fine.

In sum, between 17 USC 506 and 17 USC 1201, warez groups faced potential prison terms of upwards of 10 years, with fines as high as $1,000,000 – as noted by Craig et al. (2005), higher than the federal prison term for rape. Not to mention that the application of these charges and aggregation of infringement amount was a legal gray-zone. Perhaps the only saving grace of these groups was the difficulty of prosecuting such a complicated crime, often involving many actors, servers, and legal jurisdictions. However, as evident by many cases of criminal prosecution of these groups, the courts often favoured 18 USC 371 – criminal conspiracy – as the burden of proof was much lower and it carried similar penalties. As well, policing operations of the early 2000s demonstrated law enforcements' ability to police global piracy, despite the complexities of International jurisdictions (Urbas, 2006). The enactment of the 1997 NET act and 1998 DMCA brought about a wave of criminal enforcement and prosecution – bringing the law to the doorstep of these once hidden recesses in the fabric of the Internet.

## 1.2 Digital Piracy, The Scene, & Release Groups

As shown above, copyright piracy is not a new phenomenon (see also Alexander, 2007); however, as new technologies and mediums emerge for protecting content, advanced methods of piracy emerge in tandem (David & Kirkhope, 2004). Many researchers have examined the phenomenon of digital piracy, often employing samples of university students, through a number of

theoretical lenses and methods (Konstantakis, Palaigeorgiou, Siozos, & Tsoukalas, 2009; Cesarini & Cesarini, 2008; Gunter, 2008; Ingram & Hinduja, 2008; Pouwelse, Garbacki, Epema, & Sips, 2008; Hinduja, 2006; Higgins, Wilson, & Fell, 2005). However, many of these studies have examined digital piracy in the form of file-sharing via peer-to-peer (p2p) networks and/or commercial piracy. Though it is the case that these mediums account for the bulk digital piracy that occurs on the Internet (Pouwelse, Garbacki, Epema, & Sips, 2008), they are frequently not the source of the content which they distribute (Craig et al., 2005; DOJ, Jun., 30, 2005). The groups responsible for the acquisition and distribution of copyrighted content on the Internet are known as *Release Groups* (Howe, 2005; Rehn, 2004; Lee, 2002).[5]

Release groups such as "Drink or Die" (DoD) have been described as being highly organized and highly capable groups of individuals who work to strip copyrighted materials of their copyright protections and then to distribute them to other groups within the *warez scene*, sometimes weeks before the content's commercial release dates (Urbas, 2006; see CCIPS, *Operation Buccaneer*). Though there are many release groups, the top few are believed to account for the majority of pirated commercial content released to the warez scene (Goode, 2010; Urbas, 2006), and the DOJ predicts that the top 8 to 10 of these groups are responsible for the majority of pirated content available online (See CCIPS, *Operation Buccaneer*) .

[5] Notably, the term warez group and release group are often used interchangeable in many sources. To clarify for the purposes of this thesis, release groups are a subset of warez groups and will denote groups which actively work to *release* content; thus, excluding courier groups, traders, and abadonware groups – which all exist under the larger category of *warez groups*.

The following section will begin by briefly detailing the history of digital piracy and the genesis of 'the scene'. Next, relevant literature on the warez scene and release groups will be described and their findings discussed. Last, this phenomenon will be framed within the criminological perspectives of Situation Crime Prevention - with specific attention to C*ounterproductive Prevention* (Wortley, 2003; Grabosky, 1996) - and Social Network Analysis.

### 1.2.1 The History of Digital Piracy

Digital piracy dates back to the 1970's when computer clubs would swap and modify software. Computers of the 1970's were bulky and expensive and often users did not own one personally but interacted with one through their work or school. As the 1980's dawned, home computers became more common, and with that, early phone modems emerged as tools to connect users. Employing these early modems, computer users began to set up bulletin board systems (BBS) and newsgroups that enabled users to drop off information at a semi-public digital space for other individuals to view and share. This was the beginning of the warez scene,[6] BBS users would compete to remove, i.e. crack, the copyright protections of games and software and then post the content for others to share. The objective was to release content with the end result of having it proliferate across BBSs and by extension also proliferate one's reputation of being an elite cracker (Scott, 2010; BBS: The Documentary, 2005; Craig et al., 2005). The scene can loosely be defined as a network of sites,

[6] The term *warez* is used to refer to any copyrighted materials which have been stripped of their copyright protections to be copied and distributed - it is a play on the word 'software'.

typically File Transfer Protocol (FTP) servers, and users who operate to aggregate and distribute content.[7]

In a speech given by Jason Scott, an Internet historian, at DEFCON 18 (Scott, 2010), Scott describes the activities of early crackers and members of warez groups. He details the progression of these groups from individuals challenging themselves to defeat copyright protection technology, to groups competing for prestige. Thus, the scene was, and still is, a forum for intellectual competition to see who could defeat the copyright protections of software and games most efficiently, and individuals and groups fight for bragging rights (Id.).

In its early form, the warez scene was moderately safe, as most law enforcement were not technologically savvy enough to police cyber space, and this form of copyright piracy was difficult and expensive to prosecute (Craig et al., 2005, p. 27). The earliest activities of federal law enforcement to police the scene came with *Operation Cyber Strike* in early 1997 (Kornblum, January 28, 1997). Interestingly, though this operation was considered a success and one of the largest organized efforts to curtail Internet piracy at the time (Id.), little can be found on the operation itself. A search of either of the DOJ, FBI, or CCIPS websites reveals no mention of Cyber Strike, a sentiment shared by a representative of the Business Software Alliance in a congressional subcommittee in 2000, testifying:

[7] Content is used as a general term to refer to software, movies, television shows, games, pornography and other forms of digital commercial media and software.

> *We approached the San Francisco FBI office a couple of months ago and said, when is cyber strike 2 coming? They said, what is cyber strike?* (*Implementation of the NET Act*, 2000)

In 1999, ostensibly the most significant change to bring piracy to the mainstream, *Napster* was launched, and within months of its release, it had approximately 50 million users (Kot, 2009, p. 25). *Napster* was one the of the first of a paradigm shift in the distribution of content on the Internet known as Peer-to-Peer (p2p) networks. These new types of networks allowed Internet users to locate and download content from other users in an easy and efficient way. Though *Napster* was shutdown in 2001 due to a lawsuit (See A & M Records, Inc. v. Napster, Inc (2002)), notably citing the case of *Sony Corp. of America v. Universal City Studios, Inc. (1984),* claiming this new technology was more likely to be used for illicit purposes than licit, a slew of copycats soon emerged after. *Kazaa*, *Limewire*, and *Gnutella* – to name a few – all surfaced as easy methods of sharing content, and all suffered the same legal woes that crippled *Napster*. To-date, the most efficient means of distributing content via p2p networks seems to be *Torrents* (Wang, 2004), and because of its hybrid centralized-decentralized architecture – it may be very hard to target by lawsuit or law enforcement action.

Significantly, though p2p networks are the most widely used method of obtaining illicitly copied content for everyday Internet users (Pouwelse, Garbacki, Epema, & Sips, 2008), warez groups opt to separate themselves from p2p networks, and (oddly enough) fight to prevent their own cracked content from

being leaked into mainstream p2p networks.[8] Thus, there is a distinction between mainstream p2p networks, and the clandestine networks of the warez scene. It has been suggested that the content spread on p2p networks to mainstream Internet users originates in the scene, where it trickles down for everyday individuals to access (Howe, 2005; Craig et al., 2005). As well, though much has changed since the beginning of digital piracy in the ways of distribution, release groups' objectives remain the same: obtain commercial content, strip its copyright protection features, and distribute this content to others within the scene (Howe, 2005; Rehn, 2004; Lee, 2002).

### 1.2.2 The Warez Scene

Current information pertaining to the distribution architecture and social structures of the scene is difficult to come by, as these networks operate clandestinely and have been the target of recent federal policing operations. Despite these difficulties, some scholars have risen to the challenge of documenting the activities of groups and interviewing current or past individuals active in the warez scene. The first academic study that attempted to document the social structure of digital piracy was conducted by Cooper & Harrison (2001), and it was not until shortly after policing operations of the early- and mid-2000s that a wave of scholarly inquiry followed. Authors such as Eric Goldman (2005, 2004, 2001), Gregor Urbas (2006), Sigi Goode (2010, [with Sam Cruise] 2006), and Alf Rehn (2004) contributed to the study of these groups. Additionally, many

[8] In *nfo files* of the warez group Apocalypse Production Crew (aPC), group members express that individuals whom have access to their released content are not to distribute it via p2p networks. See Appendix A.

authors of popular literature contributed to the discovery of the actions of the groups, such as David McCandless (1997), Jeff Howe (2005); Jennifer Lee (2002), and Craig et al. (2005).

In accurately portraying the individuals and groups operating within the scene, there are several levels of analysis that are significant: differences between types of groups/scenes; distribution chain of content; divisions of labour within/between groups; and social categories with respect to prestige. Significantly, there are many semantic differences between both academic and popular literature with respect to labelling phenomena and actors within this world. The following will attempt to bridge these differences, while avoiding redundancy, to describe these issues.

First, authors of both popular literature and academic works have suggested that there are differences between groups with respect to time-frame and type of content that they work with: these divisions are sometimes referred to as different scenes (See *The Game Scene Charts* for an example; also Craig et al., 2005, pp.159-181). With respect to time-frame, divisions exist that categorize groups by the time in which they release content. Cooper & Harrison (2001), for example, describe the difference between *zero-day* groups, which release content on (or before) the day of the content's commercial release date, and *zero-hour* groups, which release content on (or before) the hour of content's commercial release date. Goldman (2005, 2004, 2003), confirms this as well and adds the concept of *abandonware* groups, that trade content which has been discontinued or abandoned and is difficult to find. With respect to type of content,

groups can be divided by the type of content, or media, that they release. This is further specified by the format that the content is traded within. For example, there is both a “DVD Rip” scene and a “HD DVD Rip” scene (See http://scenereleases.info, retrieved February 7, 2011, for more information). This is significant because groups typically compete only within their own respective scene, and often groups may affiliate with other groups or create subsidiaries to diversify their access to content. These group affiliations and subsidiaries shape both the distribution as well as the social structure of the scene. For example, though a group releases DVD content, it may be in their interest to affiliate with an audio group.

Second, it has been suggested by some authors that there is a distribution hierarchy within the scene; along with a ranking scheme that categorizes sites by their speed and access to content. Howe (2005) describes this distribution schedule and the economy that guides it, starting with the apex of the distribution pyramid, the *topsites*:

> *The upper reaches of the network are a "darknet," hidden behind layers of security. The sites use a "bounce" to hide their IP address, and members can log in only from trusted IP addresses already on file. Most transmissions between sites use heavy-duty encryption. Finally, they continually change the usernames and passwords required to log in. Estimates say this media darknet distributes more than half a million movies every day* (Id.).

Both Howe (2005) and Craig et al. (2005) describe how there are only a few dozen top sites worldwide, and the DOJ predicts that files can be distributed globally within minutes (See CCIPS, *Operation Buccaneer*). Below these topsites

are low ranked sites, through which files filter down, and at the bottom of the pyramid are end-user distribution media, such as p2p networks (Howe, 2005; Craig et al., 2005). Significantly, in these networks, content is *quid pro quo*, individuals must contract through group affiliation or trade for access to content using a ratio scheme. As every group is seeking the best access to content, it becomes in their interest to distribute content to top ranked sites first, and use the ratio credits bestowed to gather more content to distribute to lower ranked sites for credit. As well, another noteworthy facet is that distribution schemes may differ between scene, for example, audio and video content which has a higher demand with end users may fast track to lower levels on the distribution hierarchy, whereas niche software or content with less end-user demand, may take longer to trickle down (Craig et al., 2005, pp. 133-137).

Last, the literature describes different divisions of labour within and between groups. Depending on the type of the scene a group may be involved in, different roles appear within the group. Cooper & Harrison (2001) describe these for the audio piracy scene as roles such as *rippers*, *botmasters*, *couriers*, and *leaders* (Id.). Within groups that necessitate the removal of copyright protection features, crackers, are required. Groups that release films within weeks of their box office date often employ *camers*, individuals who film the movie in a theatre with a handheld camera (See http://scenereleases.info, retrieved February 7, 2011, for more information). As well, there are leaders, *senior members,* and *council members* that are responsible for decision making (Cooper & Harrison, 2001). Between groups, there are independent groups that run sites and courier

groups. Lee (2002) describes independent courier groups that compete to achieve the greatest amount of distribution of content. In short, the literature shows a great deal of diversity, role overlap, and organization in the division of labour operating towards a purposive goal – creating an environment that allows for individual interest to often coincide with the collective interest of the group, and the greater scene.

The culmination of the different scenes, the distribution scheme, divisions of labour, and competition results in a complex economy of content, in which the ability to release content acts as a means to reinforce a social hierarchy (Rehn, 2004). This intricate ecology of motivations, divisions of labour, roles, and groups is a unique world, through which criminological concepts may be explored and challenged. The next section will describe two analytical frameworks which will be relevant to the current study: Situational Crime Prevention and Social Network Analysis.

### 1.2.3 Situational Crime Prevention and Digital Piracy

In similar fashion to other industries, copyright industries are involved in an evolutionary digital arms race in the protection of intellectual property (IP) from release groups. In other words, as industry develops new technologies to prevent the illicit copying of their IP, crackers soon develop methods to circumvent these technologies (Goode & Cruise, 2006, p. 173). Scholars have suggested methods of protecting industry from insider leaks of IP (Willison & Siponen, 2009; Willison, 2006; Willison & Backhouse, 2006; Stephenson, 2005), developments in Digital Rights Management (DRM) technologies, tools used to

ensure copyright compliance (Hunter, 2004) to aid in target hardening sourcing routes to release groups and to make it more difficult to copy and distribute content. As well, other scholars have developed formalized theoretical frameworks for studying piracy with the intent to seek methods to reduce opportunities for individuals to offend (Holsapple et. al, 2008; Willison & Siponen, 2009).

Situational Crime Prevention (SCP) is a theory that aims to disrupt purposive offenders attempts to engage in criminal behaviour through amendments in contextual factors, such as changes in the environment (Cornish & Clarke, 2003; Clarke, 1995; Clarke, 1980). Its theoretical roots can be traced to Routine Activities Theory (Cohen & Felson, 1979) and Environmental Criminology (Brantingham and Brantingham, 1981; Jeffery, 1977). An example of SCP in action is study on the theft of scrap metal from construction sites conducted by Kooi (2010). Kooi found 18 techniques which can be applied to reduce the commission of scrap metal theft, such as placing identification on scrap metal to discourage offenders from selecting it (Id.). Thus, by focusing on situational factors that facilitate a criminal event, researchers aim to discover methods of reducing the opportunities for an offender to commit a crime (Clarke, 1995; Clarke, 1980). Currently, SCP researchers argue that by changing situational factors to - increase the effort, increase the risks, reduce the rewards, and/or reduce provocations for an offender to offend and/or remove excuses that enable criminal behaviour - the probability of a successful criminal event

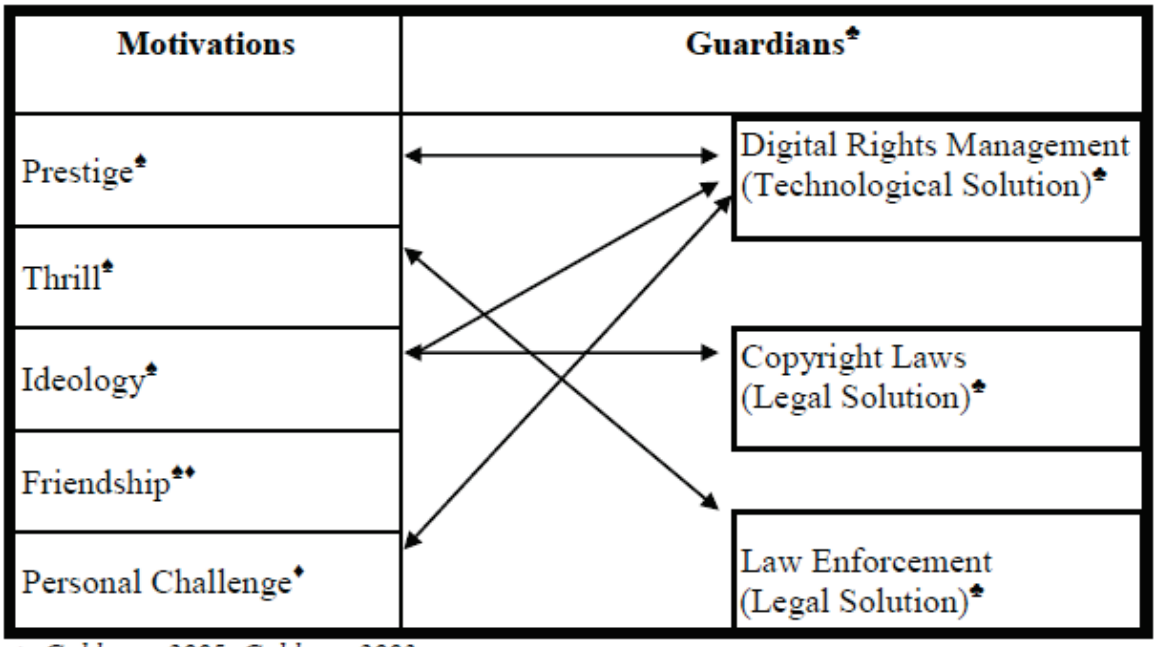
occurring may be reduced (Bullock, Clarke, & Tilley, 2010; Cornish & Clarke, 2003; Clarke, 1995).

SCP has been applied to computer issues such as combating employee theft of IP (Willison & Sipoken, 2009) and reducing opportunity for computer crimes (Willison & Backhouse, 2006). With respect to reducing insider theft of IP, Willison & Sipoken (2009) employed a crime-script approach (see Cornish, 1994) to discover the steps that are undertaken by employee insiders to commit a successful criminal venture. Then, the authors apply Clarke & Cornish's (2003) methods of SCP to suggest ways of disrupting an insider's attempts and find that by taking proactive steps, for example, increasing the effort required to commit theft through employing biometric fingerprint authentication or using passwords, this behaviour may be reduced (Id.).

With respect to release group piracy, the difficultly in prescribing policy to reduce this behaviour is a paradoxical relation between law enforcement/industry efforts and the motivations that encourage it, a phenomenon in criminological literature known as *counterproductive prevention* (Wortley, 2003; Grabosky, 1996). Goldman (2005, 2003) partly described this phenomenon by referencing media reports, release group *nfo* files, and websites to describe the counterintuitive nature of criminalizing copyright infringement. Goldman argued that motivations held by individuals in the warez scene such as stoking one's "ego", "thrill of the illicit", a "software should be free" mentality, and a "sense of community" operates counterproductively to the intimidation tactics imposed by law enforcement (Goldman, 2005, pp. 25-26). Other motivations were empirically

tested by Goode & Cruise (2006) in interviews with crackers, which included questions on initiatives employed by industry, such as DRM technologies. The authors found that the challenge of defeating DRM technologies is a significant motivating force encouraging crackers (Goode and Cruise, 2006, pp. 183-184).

**Figure 1 Counterproductive Relationship Between Release Group Motivations and Guardianship Methods**




♠. *Goldman, 2005; Goldman 2003*
♦. *Goode & Cruise, 2006*
♣. *Holsoppe et al., 2008*

The potential for counterproductive prevention associated with the warez scene is illustrated in Figure 1. The motivations of these groups can be concisely listed as: Prestige, Thrill, Ideology, Friendship (Goldman, 2005; Goldman, 2003), and Personal Challenge (Goode & Cruise, 2006). Figure 1 illustrates the relationship between these motivations that drive release group piracy and the guardianship methods employed to protect copyrighted content suggested by Holsapple et. al

(2008). Motivations, such as prestige, are stoked by being the first and best to defeat DRM technologies. Thrill seeking is further encouraged through the risk of apprehension. Ideology is further stoked by oppressive copyright laws and DRM technologies which do not grant users full access to content, as related to the previous section. Personal Challenge is further encouraged through increasingly difficult DRM technologies.

Thus, this paradox between motivations that encourage release group piracy and the means employed to disrupt their activities is a perplexing issue. Even worse, given the complexity of environment that the crime is committed within, understanding this phenomenon is a difficult task. However, because these individuals acting in these groups are purposive (i.e. make goal oriented decisions), using an SCP framework to interpret their behaviour is fitting: as motivations can be included in the analysis of behaviour.

### 1.2.4 Social Network Analysis

With a significant characteristic of the Internet being the interconnectivity of users and fiction-free access to information,[9] a network approach to the study of cybercrime seems particularly apt. A Social Network Analysis (SNA) framework permits researchers to map out the connections within a social network - defined in its simplest form as "... a finite set of actors and the relation(s) that define them" (Wasserman & Faust, 1994, p. 20) - and to employ mathematical tools to determine characteristics and patterns within the network

[9] The concept of 'Friction Free' markets (See Chapman, 1996 for more) is often cited on both sides of the copyright debate. For example, the film *Steal this Film II* (King, 2007), claims: "Friction free markets and friction free piracy run in tandem" (Id.).

(Hulst, 2009; Morselli, 2009; Borgatti, 2006; Wasserman & Faust, 1994; Scott, 1988; Tichy, Tushman, & Fombrun, 1979). Through an SNA framework, researchers may gain a unique perspective which allows them to: bridge micro- and macro- characteristics which affect behaviour and/or network architecture (Papachristos, 2009; Patacchini & Zenou, 2008; Burt, 2005; Granovetter, 1979); discover methods of optimally disrupting a network or optimally disseminating resources within a network (Hulst, 2009; Borgatti, 2006); and organize data regarding social structure(s) (Scott, 1988; Tichy, Tushman, & Fombrun, 1979). As such, an SNA framework has been lent to understand a number of social issues - from the spread/distribution of AIDS in needle-sharing networks (Dombrowski, Curtis, Friedman, 2007) to locating and mapping child exploitation websites (Frank, Westlake, & Bouchard, 2010).

SNA spawned from traditional sociological methods of analysing social structure and relations within and between groups, such as sociometry (Moreno, 1937; Tichy, Tushman, & Fombrun, 1979), and progressed through developments in mathematics, such as *Graph Theory* (Scott, 1988). Within the field of Criminology, scholars have suggested that it may be a useful investigative tool to study organized criminal behaviour (Hulst, 2009; Morselli, 2009). Relevant to the current study, copyright piracy is an innate crime of distribution, and as such, understanding the network architecture is essential to understanding the operations of these groups. Three SNA-related concepts are relevant to the study of warez groups: the “security vs. efficiency trade-off” (Morselli, 2009, pp. 63-71); social capital (Burt, 2005); and locating *key-players* (Borgatti, 2006).

First, though it has been suggested that organized criminal ventures are similar to their licit counterparts in many ways (e.g. Levitt & Dubner, 2005), criminal networks differ in that they must operate clandestinely to avoid disruption by law enforcement (Morselli, 2009; Baker & Faulkner, 1993). Since organized crime involves the collaboration of multiple actors and can result in complex relations between actors, SNA allows researchers to visually graph the relations between actors and to organize data in a comprehensible and meaningful way. For example, in a study by Baker & Faulkner (1993) of price-fixing in industrial equipment manufacturers, the authors employed an SNA framework to examine network structure in relation to role in the conspiracy and amount of prison time served. They discovered that in networks that operated with their leaders in peripheral locations within the network, leaders of the conspiracies received lighter sentences. Conversely, in networks where the leader was highly centralized, leaders of the conspiracies received higher sentences (Id.). The authors employed the data to demonstrate a phenomenon in criminal networks research know as the “security vs. efficiency trade-off” (Morselli, 2009, pp. 63-71), in which illicit networks must maintain a balance between operating clandestinely and operating efficiently (see also Bouchard, Beauregard, and Kalaczska, in press). Though no studies have been conducted on the subject, as warez groups operate as an illicit network of actors and sites, they must remain invisible to law enforcement while at the same time must operate to distribute their content between other members of the group and other groups. The DOJ predicts that within minutes these groups can distribute content globally (See

CCIPS, *Operation Buccaneer*); all the while, the crime these groups engage in can carry a prison term of five years. Actors in these networks must operate efficiently to stay competitive in the scene, but equally, must remain invisible to law enforcement.

Second, another concept that helps explain the relation between actors in SNA research is *social capital* (Burt, 2005; Burt, 1997; Burt, 1995). Though the concept has been used outside of SNA, social capital within the SNA framework stems from research conducted by Mark Granovetter's (1973) study on the value of weak ties – social connections that bridge into new resource pools. In his study, he finds that people are more likely to find new employment through social contacts with which they are loosely associated. Granovetter suggests a framework that may aid social scientists by bridging micro and macro levels of analysis (Id.). Portes (1998), for example, explains that social capital "...stands for the ability of actors to secure benefits by virtue of membership in social networks or other social structures" (Id., p. 6). An example of social capital in action is the concept of *brokers* (Burt, 2005). Brokers bridge network gaps, or put differently – position themselves in *structural holes* within a network (Id., p. 7). In the warez scene, it may be that individuals position themselves in powerful structural gaps in the network to reap the rewards, or that individuals positioning themselves in structural holes may enable the group to succeed. Applying the concept of social capital to release groups may enable researchers to better understand success and failure. For example, high ranking top-sites that

distribute content in the scene only remain highly ranked so long as they have access to the newest releases (Lee, 2002), as Craig et al. (2005) write:

> *Topsites demand that all of the groups affiliated with them pre-release directly to their site. ... Piracy is a cutthroat world and a topsite's status lasts only as long as it receives every release first*. (Id., 128)

Thus, groups or individuals with greater social capital may be able to better operate a site or negotiate deals for their site; while others without social capital will struggle to find groups to affiliate with their site.

Last, SNA may operate as a method to discover important individuals within a network, known as *key-players* (Borgatti, 2006). Research on how to discover these individuals within networks has led to a number of questions. For example, Borgatti (2006) describes the relation between targeting key players and the objective of the research (i.e. to disseminate information or to optimally disrupt the network). If one were examining a network to discover the most well-connected individual, thus to distribute a resource to as many nodes as possible or to gather a resource from as many nodes as possible, then targeting a node with a high *degree* (number of links) would be best. However, if a researcher were looking to discover a way to disrupt or fragment the network most optimally, then targeting an individual with a high *betweeness* (node through which many paths travel) would be optimal (Id). This concept is significant to warez research as it may enable law enforcement to better prioritize targets. For example, are the administrators of the warez groups truly the most important players within the

network, or do players occupying specialized positions (e.g. crackers) more central and important to target?

## 1.3 The Current Study

Warez groups, in general, offer an interesting challenge to criminologists. These individuals operate in organized groups (Urbas, 2006; Craig et al., 2005) in an odd ecology of motivations (Goode & Cruise, 2006; Goldman, 2005). As well, the diversity in roles between/within scenes (Cooper & Harrison, 2001) coupled with these individuals' goal-driven behaviour creates an odd economy, where the value of content is not related to its commercial retail value (Rehn, 2004; McCandless, 1997), but something else. These groups often involve individuals of varying ages, well outside the scope of traditional criminal involvement and are typically well educated and successful (DuBose, 2006).

To date, very little research has been conducted on warez groups and the scene in which they are embedded, and to the researcher's knowledge, no research has been conducted on the network architecture of these groups. Additionally, few studies have been conducted with the objective of disrupting these groups' activities. As these groups are composed of purposive offenders, acting in concert, through a series of clandestine networks, the analytical frameworks employed to better understand this behaviour will need to reflect this set of circumstances. Thus, both an SCP (to interpret their behaviour and seek methods to disrupt their aims) and SNA (to map the connections between individuals and servers that enable the criminal venture) framework seem a good fit for this thesis.

The current study aims to examine release groups through these two perspectives. Through an SCP framework, the study will employ a crime script approach (Cornish, 1994) to discover the necessary steps of a warez release. It will employ a dataset constructed of 93 court cases of convicted individuals who engaged in the warez scene whom were apprehended in three major FBI operations: Operations Buccaneer (US DOJ, Dec. 11, 2001), Fastlink (US DOJ, Apr. 22, 2004), and Site Down (US DOJ, Jun. 30, 2005). Using an SCP framework, opportunities to disrupt release groups will be examined with the focus being efforts employed by industry and law enforcement. Through an SNA perspective, the study will map out the connections between sites and individuals employing a two-mode network constructed with UCInet using data from court cases from one federal policing operation, Operation Copy Cat (US DOJ, Apr. 6, 2006), for which there was especially detailed data. Using an SNA framework, the network architecture will be examined in relation to sentences doled out by the courts for the conspiracy. The analysis will aim to answer whether or not a relation exists between centrality and sentence. Specifically, are the most culpable individuals also the most well connected? As well, are there other actors in the network that are central or well-connected who were over-looked by the courts?

# 2: DATA & METHODS

## 2.1 Data

The following section will describe the data employed in this study: court case data retrieved from a public domain database, and secondary sources.

### 2.1.1 Court Case Data

The court case database was constructed by searching news reports and DOJ press releases for arrests of warez members tied to federal law enforcement operations. The three most prominent operations were chosen – Operations Buccaneer, Fastlink, and Site Down. Operation Buccaneer was an 18 month undercover operation conducted by US Immigration and Customs Enforcement (ICE) targeting the prominent warez group Drink or Die (DoD) (US DOJ, Dec. 11, 2001). Operation Fastlink was an undercover operation targeting a number of groups, some of which were Apocalypse Production Crew (aPC) and Fairlight (FLT) (US DOJ, Apr. 22, 2004). Operation Site Down was the culmination of three separate policing operations conducted by the FBI, targeting RISCiso and warez groups using servers located in Northern California (US DOJ, Jun. 30, 2005).

Data input into the database were gathered from court cases stemming from these operations and was collected from the US Courts' Public Access to

Court Electronic Records (PACER) database.[10] PACER is a public domain database which allows users, for a small fee, to access federal court case records. Varying degrees of information are available via this database. Each individual found in a DOJ press release tied to a warez operation arrest was searched in PACER and court documents which yield information on the facts of the cases were downloaded and analyzed. Additionally, court cases often created snowball-samples, where one court case led to the discovery of others. Though the available amount of information varied from cases to case, a prerequisite for inclusion into the database was a complete and available Docket Report, which listed the defendants name, charge, and sentence. In almost every case, the defendant's Indictment or a Bill of Information was available, which listed the charges and facts of the case. In ideal cases, the defendant had an Indictment or Bill of Information; Plea Agreement or Statement of Facts; US Sentencing Memorandum; Defendant Sentencing Memorandum; Letter(s) to the Court; and the case's Judgment. Out of the documents that were available, the following data were gathered in order to provide background information on the participants at each stage of the script : number of indictable counts, number of charges, type of charge, district, sentence, year of judgment, infringement amount determined by the plea agreement, residence, group affiliation, role, and age of defendant.[11]

[10] See http://www.pacer.gov/

[11] In many cases the defendant's age and/or residence was not listed in the court documents. If this was the case, then this information was gathered via DOJ press releases, which often cite age and residence. Age was adjusted to be relative to 2004 in arrests tied to Fastlink and Site Down and to 2001 in arrests tied to Buccaneer.

Though many of the data gathered was straight forward, in the case of role and criminal history research decisions were made. First, role was difficult to determine in some cases, as some files did not report role (n = 35) and ones which did often reported multiple roles per defendant. Role, as such, was first split into primary role and a dichotomized multiple role (0 = no; 1 = yes) variables. In the presence of multiple roles, multi-role was coded 1, and if the defendant had an administrative position in the group (leader/senior member/council (1), or site operator/administrator (2)) the highest ranking of these was selected. If not, then primary role was selected by being the most prominent role suggested in the court case files (supplier (3), cracker (4), tester/packager (5), Courier (6), and No Role Listed (7)). Second, many of the cases did not specifically disclose the criminal history of the defendant; however, in sentencing memos and judgments, the "Criminal History Category" of the defendant was listed. Though this does not specifically describe previous offenses, it does rate the accused on a point scale based on presence or absence or previous offenses. For the purposes of this database, defendants listed with a Criminal History Category of I were coded with no criminal history (0); if the defendant had a Criminal History Category of II or more, they were coded as having a criminal history (1).

Of the reported roles of the 93 defendants, site operators / administrators were the largest group (19), followed by suppliers (16), then leaders/senior members/council (listed as "group admin" in Table 1; 11), crackers (5), couriers (5), and tester/packager (2). In 35 cases role was not determinable. Although most defendants were under 30 years, age nonetheless ranged from 17 to 51.

The two individuals with a primary role of Tester/Packager had the highest mean age (40.5), and individuals with a primary role of Cracker had the lowest mean age (23.3). There was little variation between roles regarding mean number of charges, and just under one third (31 percent) of respondents were sentenced to prison (mean of 17 months). There was an interesting variation between roles and sentence meted out. Of individuals imprisoned, it should be noted that both Testers/Packagers were sentenced to imprisonment, serving on average a term of 15.5 months—it is the only role in which every individual was dealt a prison term, though no pattern can be established from two cases. Group administrators had the second highest imprisonment rate (n=7; 64 percent) and served the longest mean terms of imprisonment (22 months), while none of the five crackers were sentenced to prison.

**Table 1 Characteristics of Defendants in Court Case data by Primary Roles.**

| Primary Role | n | Age Mean (STD) | # of Charges Mean (STD) | # Imprisoned n (percent) | Months Imprisonment Mean (STD) |
|---|---|---|---|---|---|
| Group Admin | 11 | 29.9 (11.1) | 1.3 (0.5) | 7 (64) | 22.0 (14.9) |
| Site Op/Admin | 19 | 29.1 (7.7) | 1.6 (1.0) | 9 (47) | 17.4 (9.8) |
| Supplier | 16 | 25.2 (7.1) | 1.3 (0.5) | 4 (25) | 18.0 (17.4) |
| Cracker | 5 | 23.3 (6.0) | 1.6 (0.9) | 0 (0) | 0.0 |
| Tester/Packager | 2 | 40.5 (9.2) | 1.0 (0.0) | 2 (100) | 15.5 (3.5) |
| Courier | 5 | 26.8 (5.2) | 1.2 (0.5) | 2 (40) | 4.5 (5.0) |
| Unknown/Not Reported | 35 | 26.1 (7.6) | 1.3 (0.5) | 5 (14) | 12.1 (16.3) |
| Total | 93 | 27.4 (8.2) | 1.4 (0.6) | 29 (31) | 16.7 (13.0) |

### 2.1.2 Operation Copy Cat – SNA Data

After aggregating and organizing the 93 case court dataset, it was discovered that the specific law enforcement operation, Operation Copy Cat, offered the opportunity for examination through an SNA framework. Operation Copy Cat was a subsidiary of Operation Site Down, targeting a group of warez sites located in the Northern District of California (US DOJ, Apr. 6, 2006). Unlike the larger dataset of 93 cases, the court cases of individuals apprehended for Copycat are almost entirely tried in one district, the Northern District of California, and have a uniform operationalization of role ascribed by the court. These definitions of role are outlined in the case of USA v Fish et al. (2008) in the

Indictment Report of David L. Fish (See Appendix B, for a copy of this page of Fish's Indictment Report that defines role). As well, most cases have the same amount and types of documents available, which are constructed and outlined almost entirely uniformly. Most importantly, besides these uniformities of data presentation, various documents have outlined **specific** connections between defendants and servers, as well as the **types** of connections. As such, the court case data for this specific policing operation afforded the unique opportunity to construct a weighted 2mode network of Operation Copy Cat.

The operation Copy Cat dataset was constructed by extracting court documents from 33 defendants found in DOJ Press Releases and news articles. These were examined in similar fashion to the larger dataset; however, there were four notable differences between the construction of this dataset and the larger one. First, because the dataset enabled weighted connections between individuals and servers, connections were weighted on an ordinal scale from lowest to highest based on culpability suggested by court documents, as: [0] no connection; [1] Leech; [2] Ratio; [3] Site Op/Admin. Leeches were described by the court as individuals who had access to download content but were not required to upload content in exchange. Ratio users were individuals who had to upload content to the site in order to earn credits equivalent to a proportion of the content they upload to the site (typically 1:3 Upload:Download). Site Operators/Administrators had a degree of control over the site which they connected to (See See USA v. Fish et al, Case Number 5:05CR00445. N.D. CA,

2008). Significantly, every connection, with one exception,[12] established in UCInet was specifically denoted in a court document. In most cases (28), a defendant's relation was further explained by the type of access the individual had to the server, i.e. Leech or Ratio. In only a few cases were individuals described as connecting to a server without explaining the level of connectivity. In these cases, the lowest level of culpability was assumed; thus, they were coded as a [1] Leech.

Second, an attribute dataset was constructed based on individuals' roles. As opposed to the larger dataset of 93 cases, role was broken down into seven dichotomized variables: "Supplier", "Cracker", "Test/Pack", "Courier", "Group Administrator", "Scripter", and "Broker". This was changed because it afforded a greater range of testing and allowed for multiple roles to be accounted for more accurately; however, this amendment was only possible because of the uniformity between court cases in Operation Copy Cat. As well, because relation between users was accounted for through link weight, the role of Site Operator/Administrator could be removed.

Third, inclusion in this dataset differs from inclusion in the larger dataset in that inclusion is defined by: the ascription of arrest under Operation Copy Cat,

[12] Brian Verhoeven is specifically listed as connecting to a server named "Wasted Time" – the headquarter server for a group of the same name. Another individual, Ali Ghani, is specifically described as the leader of this group; however, the courts vaguely claim that he connected to 'servers'. The decision was made that it would be incredibly likely that Ghani would have access to this server. However, keeping in line with the other parameters of the methods, as the type of access is not denoted in court documents, it is left at Leech access.

the presence of a docket report,[13] and information which demonstrates activity in the network.[14] This allows a fuller view of connections between servers and defendants within the Operation Copy Cat networks. In sum, 32 individuals were located out of the 40 total arrests noted by DOJ press releases (US DOJ, May 14, 2008). These 32 cases were the only ones located through the search efforts – this may be because some conspirators were under the age of 18, and their records were sealed.

Finally, a database was also constructed that employed identical operationalization as the 93 case dataset with regards to sentencing and demographic data. One significant difference between sentence in the larger dataset of 93 cases and the copycat sentence dataset, is that Operation Copy Cat began to include restitution to the MPAA, BSA, and ESA on top of regular fines as part of their sentence imposed to convict warez conspirators. The value of these restitutions imposed by the court are vastly larger than fines imposed in previous cases. Fines operationalization for this dataset is the sum total of restitution and fine. Significantly, there are three cases that are exceptions to this operationalization (Fish, Veyna, and Patel). These individuals were sentenced to very high restitutions, but these values were paid in part by other participants in the conspiracy. Thus, the actual value that these three individuals were required

[13] One individual, Oscar Martinez, was apprehended during Operation Copy Cat and had valuable information regarding his connections to servers and his role. However, this individual had no sentencing data, as it is believed he fled the country soon after his bail hearing (See Oscar Martinez in USA v Nunez et al., Case Number 5:05CR00734, N.D. CA, 2007).

[14] One defendant was not included, Josh McAleer, because his 'Indictment Report' and 'Sentencing Memorandum' does not suggest that he aided in installing a server, but was not actually involved in the conspiracy (See Josh McAleer in USA v Soares et al., Case Number 5:06CR00246, N.D. CA, 2008).

to pay was the difference between restitution paid by other actors in the conspiracy and their total restitution value. All other actors' fines in the Operation Copy Cat dataset are the values that each of their judgements report.

### 2.1.3 Secondary Data

By relying on court data, we are limited to the perspective offered by defendants under threat of punishment. In other words, motivations and/or explanations of behaviour are disclosed in defence sentencing memoranda and letters to the judge that mitigate culpability. This bias was partially reduced through the use of secondary sources. These were: *Software Piracy Exposed* by Craig et al. (2005); DOJ press releases; websites with interviews of warez group members; warez group nfo files and scene release charts found at http://www.defacto2.net; and magazine articles. These documents were gathered in the course of searching for relevant court cases and conducting a review of available literature on release groups. Of these sources, most significant in structuring this research was the work of Craig et al. (2005). Their text details their year-long research project examining the warez scene and contains numerous in depth interviews with insiders of the warez scene, details the internal structure of the scene, and details distribution chain of content. In these interviews, participants explain how they operate, their motivations, and ideological perspective on piracy and copyright law. Examples of other sources, such as interviews with warez group members found online, are two interviews

with Hew Raymond Griffiths, the former leader of DoD, before[15] and after his apprehension,[16] and a blog thread lead by a former warez scene courier.[17]

## 2.2 Methods

The following section will describe the methods employed in this study: a crime script (Cornish, 1994) analysis and a descriptive 2-mode Social Network Analysis.

### 2.2.1 Crime Script Analysis

Script analysis began in the field of cognitive psychology as a way of understanding behaviour (Gardner, 1985, p. 165). Researchers Roger Schank and Robert Abelson (1977) describe *scripts* as: "... a predetermined, stereotyped sequence of actions that define a well-known situation." (Id., p. 41). Scripts are written sequentially, comprise of multiple steps, comprise of multiple roles, and, traditionally, must be written from a point of view (Id., pp. 41-42). In the cognitive sciences, script analysis is useful for understanding goal driven and purposive behaviour, and as Rational Theories, for example Routine Activities Theory (Cohen & Felson, 1979), rely on similar postulates (See Williams III & McShane, 2004, pp. 235-251), script analysis is an apt fit for understanding criminal behaviour.

[15] See BanDido Interview retrieved November 1, 2010, from http://www.defacto2.net/legacy/apollo-x/bandido.htm

[16] *Lateline* Interview with Hew Raymond Griffiths retrieved on November 9, 2010 from http://www.youtube.com/watch?v=3jkz19yGfEQ

[17] See Interview with former scene courier retrieved November 7, 2010 from http://www.reddit.com/r/IAmA/comments/ckIx3

Derek B. Cornish (1994) is accredited for introducing the concept of scripts to the criminological limelight, and since, this method has been lent to a number of criminological issues, from understanding organized car theft (Morselli & Roy, 2008) to discovering methods to prevent sexual assaults on children by sexual predators (Beauregard, Proulx, Rossmo, Leclerc, & Allaire, 2007). The crime-script approach is a useful method of understanding criminal behaviour for a number of reasons. First, crimes may often involve multiple actors, performing multiple roles, during multiple stages of a criminal event. As such, this method grants researchers the opportunity to organize data about varying actors, roles, and steps in a meaningful way (Cornish, 1994).

Second, crime-scripts may operate at varying levels of analysis that allow researchers to illustrate criminal events in a comprehensive way. For example, Cornish (1994) uses the example of a car theft, as this type of crime could be analysed as "... theft of property (metascript), through robbery (protoscript) and robbery from the person (script)" (Id., 162). Each varying level may prove useful for analysis, and researchers may organize this complicated data into a comprehensible format, without losing valuable nuanced information (Id.).

Third, crime-scripts are useful for documenting the decision making of offenders as well as characterizing innovation in criminal ventures (Cornish, 1994, p. 171). As rational actors seek optimal means to an end, rational criminals engaging in purposive crime may adapt their methods to better suit their aim. A study conducted by Lacoste & Tremblay (2003) demonstrates how innovation in criminal ventures may yield greater financial gain. By examining the *modus*

*operandi* of check fraudsters, Lacoste & Tremblay discovered that even though the total number of check frauds that were occurring were reducing, the amount of money being earned per fraud was increasing.

Last, and significant to the following study, crime-scripts may illuminate previously overlooked crucial occurrences in the commission of a criminal event that may aid in constructing prevention schemes (Cornish, 1994). Seeing as situation crime prevention is seeking contextual factors which may aid in the disruption of criminal events, scripts are a fruitful method of discovering nuanced *triggers* (Cornish, 1994, p. 172), or perhaps *preconditions* (Schank & Abelson, 1977, p. 49) in the case of goals/motivations, which initiate a crime-script or step within the script. For example, in the case of computer-fraud, Robert Wilison (2006) employs a crime-script to discover situational controls that may be enacted to disrupt the commission of computer fraud by industry insiders. Regarding the current study, why was a crime-script approach favoured over other options? As discussed in the literature review, release groups contain a variety of roles and perform a variety of tasks, making analysis and description of their activities in a concise manner difficult. Take, for instance, Cooper & Harrison's (2001) study of audio piracy: the authors describe an environment of inter-related actors trading and releasing content, describing a division of labour, divisions of status, and divisions of scenes (Id.). Employing that descriptive approach, besides demonstrating the tangled-mess that this behaviour can seem, makes discovering situational controls for disruption difficult. However, a crime-script approach will allow for these nuances to be characterized and

modelled; thus, organizing data through this method will highlight situational controls that may aid in disruption efforts.

The crime-script was constructed by reviewing court case documents from the dataset of 93 cases and secondary sources (See Appendix B for an example of Indictment Report). These sources detail the process by which these groups acquire and release content within clandestine networks. The crime-script was constructed to describe: steps within the release process; the actions performed to complete each step; the roles of individuals who perform these steps; the requirements needed to perform a role; the motivations found for each individual role; and the visibility to industry and/or law enforcement.

Significantly, in some cases there were disparities between sources on steps that occur. To discover the steps that would be examined in this script, only **steps that were material to the release of content** were included. Thus, though the "testing step" is sometimes combined with other steps (See CCIPS, *Operation Buccaneer*), it is considered a separate step in this script because it is a significant action that must be performed separate of other actions for the success of the criminal venture. As well, these steps were generalized across scenes. This may be a limitation in the sense that nuances from *protoscripts*, for example "release of cam'ed movies", may have variations; however, the benefit for this larger, *universal script*, is that these sub-sets may be substituted. Thus, though "release of cam'ed movies" may not employ a *cracking* step – they do employ an *encoding* step, which performs a similar function, stripping the

identification tags from films that allow investigators to know the theatre in which the film was recorded.

As well as documenting the material steps that must occur, the roles that accompany these steps are documented. Thus, in the case of the Indictment Reports  or Sentencing Memos, these documents explain the individual's role(s) in the release group and explain their function to the group. Secondary sources elaborate on this; for example, a forum thread found online documents the activities of a 'courier' (See Footnote 18). Much like the limitation of the construction of steps, many roles were found; however, only roles material to the release process were included in the script. For example, in Operation Copycat, court case documents describe roles such as *scripter* and *broker*; though these roles serve a necessary function to groups, they were not included because they are not crucial to the release script. That is to say, content could still be released in the absence of these roles, and with respect to these two roles, they are more significant to the structure of distribution, which the SNA results will describe. In addition to documenting these roles, the requirements necessary to fill these roles were examined. This was relevant to the analysis as it aids in discovering disruption opportunities. For example, if individuals in the release steps are highly instrumental and difficult to replace, targeting these individuals may aid disruption efforts.

Finally, though not traditionally included in a crime-script analysis, each step within the release process was examined for visibility to law enforcement.

This was determined by whether or not an activity in the script required a behaviour which was illegal and noticeable by law enforcement.

### 2.2.2 Social Network Analysis

As discussed in the literature review, SNA is an analytical framework that enables researchers to visually map out the connections between nodes and employ mathematical tests to illuminate patterns in the graph (Hulst, 2009; Morselli, 2009; Borgatti, 2006; Wasserman & Faust, 1994; Scott, 1988; Tichy, Tushman, & Fombrun, 1979). In the current study, data gathered from Operation Copy Cat will be visually graphed in a 2-mode (Borgatti, 1997; Borgatti, 2011) weighted network. 2-Mode networks, or affiliation networks (Wasserman & Faust, 1994, pp. 291) are defined as relations between actors of differing types (Id.), or in other words of actors of differing levels of analysis. Borgatti & Everett (1997) describe and demonstrate these types of networks through a 2mode network analysis of a sociological study conducted by Davis et al. (1941). In this study, Davis et al. examined the attendance of social events (Id., p. 245); and in Borgatti & Everett's re-examination of this study, they graph the attendance of participants to social events in a 2mode network. In other words, as opposed to a network in which the actors are of equal levels of analysis, the actors are of differing levels of analysis, in this case, between **individuals** and **social events** (Borgatti & Everett, 1997). By employing a 2mode network approach one gains the vantage point of traditional SNA methods on, otherwise, ungraphable data.

2-mode networks have been employed in a few criminological works. For example, Morselli & Roy (2008) employed a script analysis in conjunction with a

2-mode network approach to examine the dynamics of a car theft ringing operation. In another study, Bouchard (2010) employ a 2-mode network analysis between individuals and positions within a drug distribution chain. He found that the variety two-mode centrality measures had different implications for identifying which position was central and this, which position was the most interesting target for law enforcement.

In constructing the UCInet 2-mode network, several rules were followed. First, only cases of Operation Copy Cat were examined, other court cases which were not associated with Copy Cat were not included. Second, only cases where the defendant was connected to the network in some way were included. This only affected one case (See Josh McAleer in USA v. Soares et al., Case Number 5:06CR00246. N.D. CA, 2008), as the individual was arrested for aiding the conspiracy through installing servers, but was not accused of accessing them. Third, links were only ascribed if they were specifically denoted in court documents (See Footnote 13 for exception). If a document lists a connection but does not explain the type (i.e. leech or ratio) then leech access was chosen.

Next, Actor and Server's centrality scores (Degree, Betweenness, and Eigenvector Degree) were aggregated with UCInet. 2-mode degree is a measure of the number of connections a node holds in relation to the rest of the network. Betweenness is a measure of number of paths that travel through a node, in

relation to the number of paths that do not - relative to the total network.[18] Eigenvector centrality is a measure of how well-connected a node's immediate links are (Borgatti & Everett, 1997).

To systematically test which nodes were most central to the network, UCInet's "Core/Periphery Analysis" tool was used. The method is analogous to well-known cluster analysis methods, as it attempts to create groups of similar characteristics – in this case – groups of actors and servers with similar connections between each other. This method uses a genetic algorithm to cluster actors and servers together, aiming to achieve an optimal fitness, in which there are two groups for each axis in the matrix: the core and the periphery (Hannenman & Riddle, 2005). If optimal fitness is achieved, it means that the "Core" group will have a density of 1 (i.e. total connectivity); while the "periphery" group will have a density of 0 (i.e. no connectivity at all). Using this method, researchers can locate core actors in a network who account for most of the network's connectivity. This method will be used for both the weighted network and a dichotomized version of the network, which hold the same placement and number of links, but denotes connections as 1 and absence of a connection as 0.

[18] More specifically, Borgatti & Everett (1997) defines it as such: "Betweenness may be roughly defined as the number of geodesic paths that pass through a given node, weighted inversely by the total number of equivalent paths between the same two nodes, including those that do not pass through the given node." (Id., p. 256)

# 3: RESULTS: CRIME-SCRIPT ANALYSIS

In line with SCP, the objective of the crime-script was to discover the steps that were necessary for release groups to complete a successful *release* of content and isolate data that would yield methods of disrupting their aims. After examining both the court case data and the secondary data, five necessary steps to a warez release were examined (supply, crack, test, package, distribute) overseen by individuals acting as decision makers (administrative function). Table 2 describes the function of each step, the role required to complete it, who is capable of fulfilling that role, and whether or not it is visible to law enforcement. A release begins with a supplier acquiring the content through one of three means (*Skill*, *Social Position*, or *Legal Purchase*), and then transmitting it to the group's cracker. The cracker removes the copyright protections from the content and gives it to the tester to ensure it works properly. Once the tester has confirmed that the content has been successfully cracked by the cracker, the content is transmitted to the packager, who labels and divides up the content into the right sizes for the couriers. Then, in the distribution steps, the couriers spread the content to the groups affiliated sites. The following section will explain each step with greater detail and reference specific court documents and secondary data, beginning with the administrative step, which oversees the group's actions.

**Table 2 Crime-Script of Release Process**

| |----------| Administrative Function |----------| ***Decision Making*** **(Leader, Senior Members, & Council)** | | | | |
|---|---|---|---|---|---|
| Step | 1) Supply ➔ | 2) Crack ( =➔ | 3) Test ←=) | 4) Package ➔ | 5) Distribute ➔ |
| **Aim** | *Obtain commercial content:*<br>• *Acquisition through Skill*<br>• *Acquisition through position*<br>• *Legal Purchase* | *Strip the copyright protection features.* | *Test the content to ensure it is fully functional with copyright protections removed.* | *Packages content to scene standards.* | *Distribute content to appropriate sites.* |
| **(Role)**<br><br>**Capable of fulfilling** | (Supplier)<br><br>One with access to new content | (Cracker)<br><br>One with highly specialized skills | (Tester)<br><br>One familiar with content | (Packager)<br><br>One familiar with scene standards | (Site Operator / Administrator and Couriers)<br><br>Possibly one with specialized hardware and/or high bandwidth capacity |
| **Visibility (X)** | Yes | No | No | No | Yes |

### 3.1.1 Administrative Functions

Individuals who completed this function filled the role(s) of Leader(s), Senior Member(s), and/or Council Member(s). The aim was to act as the decision making body for the group. Although not a formal "step" in the release process, administrators were heavily involved with the group's activities, sometimes performing many different roles themselves. For example, a leader in the group MaGe was cited as also supplying content and testing content after it had been cracked (US DOJ, Oct. 27, 2007). Another individual who acted as a senior member in Fairlight, performed all the steps of a release (supply, crack, test, package, and distribute) entirely by himself, by taking advantage of his position as an editor of a video game review magazine (USA v. Klienberg, Case Number 3:05CR49. D. CT, 2007).

This entrenchment in the scene is exemplified by a former leader of MaGe in a letter to the judge describing his early involvement in the scene, stating:

> *My involvement in the warez scene had become such a routine in my life that it completely went out of control [...] I enrolled in classes, but seldom did attend them, I stayed up until 5 or 6 in the morning day after day, constantly chatting online and seeing if there were new pirated works to spread around ... It was the illusion of power and fame that got to me I believe.*

The statement above illustrates a kind of quasi-addictive behaviour, as well as motivations to achieve a form of prestige. This addictiveness is reiterated by Hew Raymond Griffiths (the former leader of DoD) in an interview with Lateline where he describes himself as a "computer junkie". Interestingly, however, although many individuals performed multiple tasks within the group, this was not a

prerequisite to achieving these statuses. In the same interview, Griffiths describes how he had no skills to crack content; also stated in an interview preceding his apprehension (see BanDiDo Interview).

As the individuals filling these roles act as a decision making body, governing the actions of the group, they are partially invisible to law enforcement. Though the individuals may perform actions which are visible, such as aiding in the maintenance of a site, the specific act of decision making does not elicit law enforcement attention.

### 3.1.2 Supply

Without fresh content to release, warez groups lose their prestige in the scene; as such, it is in their interests to look for new supply lines, and to ensure that current supply lines continually produce content. Of the court cases examined, 16 individuals had the primary role of supplying content to the group (See Table 1). Successful suppliers are rewarded with accounts on lavish FTP sites and peer approval, while failures or lack of contribution can be punished by removal of FTP accounts or banishment from the group. For example, Jeffery Lerman, a supplier for the group Kalisto, a subsidiary of Fairlight, was granted access to at least eight FTP servers controlled by the group as a reward for his contributions (USA v. Lerman, Case Number 3:05CR50. D. CT, 2007); in contrast, Christopher Eaves, a supplier for the group aPC, was threatened with banishment from his group because of his lack of contribution (USA v. Eaves, Case Number 1:07CR00140, E.D. VA, 2007). Opportunities for acquisition of

content can be categorized as *acquisition through technical skill*, *acquisition through social position*, and *legal purchase*.

*Acquisition through skill* can be conducted using different techniques. Craig et al. (2005, pp. 42–54) list these as: snooping of company FTP servers; purchasing content through credit card fraud; hacking into company computer systems; and social engineering (e.g. creating fake companies or aliases to deceive victims into supplying content). Many of these methods allow the group to receive the content prior to its commercial release date. Given these methods are learned, individuals with these skills may be more difficult to replace than other suppliers. These methods may rely on illegal means, thereby increasing the visibility of their actions to law enforcement.

*Acquisition through position* does not specifically require skill, but depends instead on the individual's employment or social contacts. For example, the FBI has claimed that groups such as Rabid Neurosis (RNS), an audio release group, acquire their content from music industry employees, CD manufacturing plants, and/or DJs or stores that receive copies in advance of commercial release dates (US DOJ, Nov. 24, 2009). This is the case for a number of individuals arrested during the DOJ policing operations examined here: Colin Roy Jacobson and Paul Sherman, for example, were both movie critics who received (and later sold online to warez groups) advance copies of review DVDs (USA v. Jacobson, Case Number 5:06CR00477. N.D. CA, 2008; USA v. Sherman, Case Number 5:06CR00331. N.D. CA, 2007). Sherman sold an estimated 117 films to warez groups in advance of the commercial DVD release date. Acquiring content

through position is less visible to law enforcement than employing the skilful means noted above.

*Legal purchase* results in the slowest release of the three methods of obtaining content, as groups employing this method must wait for the product to be commercially released. This method was employed by a number of individuals in the court data, as many lacked either the social capital or skill to acquire content otherwise. The benefit of this method is that it can be performed by anyone and is invisible to law enforcement.

Generally, the *supply* step in the crime script is a point of visible criminal behaviour, and a point in the chain where disruption is possible by industry. Once content has been transmitted by the supplier to the cracker, it is invisible to outsiders until the final step in the crime script.

### 3.1.3 Crack

After content is acquired it must be stripped of its copyright protections. In an nfo file released shortly after the raids conducted by the FBI in Operation Fastlink, an anonymous representative of the release group Fairlight writes:

> *Protections of today are ones that *very* few can penetrate and those who do, should be worthy the respect. Downloading them fast is just a matter of a fast line in combination to access to a site. Skills stay, whereas the access can be revokes instantly!*[19]

Individuals who are capable of cracking current copyright protections of games and software are few in number, are instrumental to the release, and are very

[19] Fairlight nfo File, Retrieved on 7 November 2010 from http://www.defacto2.net/groups.cfm?mode=detail&org=flt

skilled. Only five out of the 94 people in our sample were crackers. Oddly, as Table 1 illustrates, these five received the lowest sentences of any of the roles listed in the court case data, as none were sentenced to a term of imprisonment. As crackers may qualify for a charge of "Circumvention of Copyright Protections" (17 USC 1201)[20] in addition to other charges for copyright infringement (17 USC 506) and conspiracy (18 USC 371), and are highly instrumental to the distribution of content (without these copyright protections removed, the content cannot be copied), it is surprising that these individuals received such low sentences.

The methods used by crackers to remove the copyright protections were not discussed in the majority of the court case documents. Only in one document (and only anecdotally) were the specifics explained. In the case of David Fish, the court records report conversations between the defendant and a confidential informant describing the process of copying console games (USA v. Fish et al., Case Number 5:05CR00445. N.D. CA, 2008). The absence of court data on the specifics of circumvention techniques may reflect that the documents available through PACER are public domain, and the courts do not wish to disseminate such information, or perhaps because the specifics of circumventing copyright protections were not substantial to the case.

As noted in the literature, a primary motivation for crackers is the personal challenge of cracking copyright protections (Goode and Cruise, 2006; Craig et al., 2005). One of the individuals in our dataset, Bryan T. Black, a cracker for the

[20] The law enacted by the US Digital Millennium Copyright Act (DMCA). The act criminalizes production and dissemination of technology, devices, or services intended to circumvent DRM; it also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself.

group Kalisto (a subsidiary of Fairlight), claimed that “his participation in the warez scene was driven by the intellectual challenge presented by the codes and a sense of membership in a collection of like-minded computer-heads on the internet” (USA v. Black, Case Number 3:09CR0056. D. CT, 2009). In another case of a Fairlight cracker, the defendant claimed that his attraction to the group was acceptance and the whole activity was just a sort of game (USA v. Klienberg, Case Number 3:05CR49. D. CT, 2007). Both seem to coincide with motivations described by the available literature.

### 3.1.4 Test

When a group releases content which is defective, improperly cracked, or which does not conform to scene specifications, it will be deleted from the scene in a process referred to as being ‘nuked’ (TGSC Editor, 2010). This entails removal from one or all sites in the scene: site operators will have their time and space wasted, couriers who uploaded the content will lose site credits and valuable time, and end users who downloaded the content will have wasted their download credits and time on useless content. Groups that release content that is continually nuked may be banned from uploading content to particular sites. To avoid this, groups test their releases rigorously to ensure quality (McCandless, 1997). Once crackers believe they have successful cracked content, it is passed to the testers to ensure that it is fully functional with the DRM technology removed. The testing stage in the script is a necessary step, and is an iterative process between tester and cracker to ensure that the content is properly cracked and fully functional. The role’s prerequisite is knowledge of the software

that is being tested: for most mainstream products (such as movies or games), this could be anyone. In other examples, especially with niche software where it takes a degree of knowledge to test and ensure the software is working properly, more knowledgeable individuals are necessary.

In the court data, only two individuals had the primary role of tester. David L. Pruett had no particular computer skills beyond his capacity to use CAD/CAM software for his work.[21] He had stumbled across the warez scene in an attempt to find CAD/CAM he could download for his home to use for practice. He was approached by the group Legends Never Die (LND), who asked him to test cracked versions for them: Pruett received the free software he needed for his job and the group had their content tested. He also received an account at an FTP server with access to copious warez (USA v. Pruett, Case Number 3:05CR286. W.D. NC, 2006). His motivations in performing as a tester seem mostly utilitarian. Other individuals listed as software testers, such as Seth Kleinberg (USA v. Klienberg, Case Number 3:05CR49. D. CT, 2007) or I-Che Lai (USA v. Lai, Case Number, 3:06CR00004. D. CT, 2007), both list motivations beyond pure access to content, such as friendship. Given that these individuals may be easily replaceable (as anyone can perform this task) and are in a position of little responsibility, with little control over the group's actions beyond testing, it seems bizarre that they were given such large sentences; although no pattern can be established from a sample of two cases.

[21] CAD/CAM (computer-aided design and computer-aided manufacturing) describes software tools covering a number of engineering functions, for example aiding in the design, analysis, and manufacture of products.

### 3.1.5 Package

Less information was available in the court data on the packaging step. After the content is cracked and tested, it is passed to a packager to compile and label the content to scene standards. *The Game Scene Charts* (TGSC), a monthly online magazine distributed within the scene, lists the rules by which a nuke may be issued. Regarding packaging:

> ***Bad Pack –*** *Means that the release is packed badly, like no compression of the release, wrong file size for the type of release. Can also mean that bin/cue wasn't used for a CDROM release. CDROM shall only use the bin/cue building, while DVDROM type releases uses the iso format. DVD9 releases are packing in 100mb files and DVDs in 50mb files. CDROM in 15mb files. All only accept Winrar extension type of files. (TGSC, 2010)*[22]

These, along with rules of naming and organizing files, are rules that dictate how a file must be packaged—all groups are expected to know and to follow these standards. The packaging stage in the script ensures that the content is adequately packed to scene standards: files must be properly named, files must be in the correct format, files must be the correct size, files and folders must be properly organized and labeled, and an nfo file containing required information must be included with the content.

[22] Files are broken up into bite-size portions to allow simultaneous upload by multiple couriers. This is model of distribution is more efficient for two reasons. First, the file transmits quicker because many different couriers are working on it all at once. Second, it disperses the *rewards* to many different couriers. See: http://www.reddit.com/r/IAmA/comments/cklx3 (retrieved 7 November 2010).

The packaging stage does not ostensibly require any particular skill or privileged social position—one must merely know scene standards and know how to adequately convert files into their required formats and file sizes.

### 3.1.6 Distribute

With the content packaged into an appropriate format, the distribution step begins with a process called “pre’ing”, in which content is uploaded by couriers to a hidden section of the group’s / affiliates’ sites. Once this is done, site administrators are instructed through an IRC bot command to make the content accessible to individuals with access to these sites (Craig et al., 2005). After a group has successfully released content, it can be distributed globally within minutes to a series of very secure FTP sites, called top sites. From here, couriers trade the content between other sites (Howe, 2005), and within hours it can trickle down to more accessible sites and eventually for p2p users to access (CCIPS, *Operation Buccaneer*).

It has been suggested that couriers outnumber all other roles in the scene combined (Craig et al., 2005, p. 137). However, in our dataset we found few of them (only five). Couriers may operate as part of the release group, as part of a courier group, or as independent traders (Lee, 2002). Generally, couriers are rewarded with a credit system from each site, called *ratio access* (See Operation Copycat Indictment/Information such as USA v. Fish et al., Case Number 5:05CR00445. N.D. CA, 2008), that typically allots three download credits per one upload credit. Thus, if a Courier uploads 100mbs of data, he/she will be rewarded with 300mbs of download credits. Couriers are motivated through this

reward scheme, as well as through ranking systems/magazines that rate couriers on their upload amounts (Lee, 2002). There were five individuals in our dataset with the primary role of courier. Of these, limited data on the defendants' activities is only available for two cases, which describe them as moving content from one site/computer to another (USA v. Gomez, Case Number 1:07CR00125. E.D.VA, 2007; USA v. Dickman, Case Number 5:06CR00054, N.D. CA, 2006).

The distribution step is one of partial visibility to law enforcement, and the three operations in our dataset (Buccaneer, Fastlink, and Site Down) focused on this step to gain entry. For example, Operation Copycat, a sub-investigation of Site Down, was conducted by setting up dummy distribution sites and then employing a confidential informant to convince warez groups to use them (See USA v. Fish et al, Case Number 5:05CR00445. N.D. CA, 2008), demonstrating the ability for law enforcement to surveil and apprehend individuals in these networks. Distribution is the final step in the script. Fittingly, the following chapter will review the results of the network analysis of Operation Copy Cat.

The data gathered from the crime-script indicates a number of important issues for identifying opportunities for disruption. First, there are steps in the script that are visible to law enforcement – the supply step and the distribution step. This indicates that though these groups operate in clandestine networks, there are points in their criminal activity that law enforcement can use to surveil or infiltrate these groups. Second, there are individuals in the script who are more material than others, as indicated by their role requirements. For example, the only requirement to fulfil the role of tester is familiarity with the content one's

testing; as such, most commercial content could be tested by anyone. However, roles such as cracker or supplier (by skill) require an amount of technical skill. As the crux of this script hinges on making the content ready for distribution, and as crackers require a high degree of skill, the results would suggest that the cracking step offers an opportunity for disruption. Third, the data re-enforces previous literature on motivations that encourage release groups: such as prestige, personal challenge, and friendship. Thus, as these motivations act *counter-productively* with some methods employed by law enforcement and industry to curtail this crime, new disruption methods will have to be mindful of these motivations.

# 4: RESULTS: OPERATION COPY CAT & SOCIAL NETWORK ANALYSIS

Operation Copy Cat, a sub-operation of Operation Site Down, was an investigation targeting a cluster of servers located in northern California between 2004 and 2005. Investigators employed 'dummy sites', that individuals used to download and upload copyrighted content, along with an undercover informant, to gather evidence, and ultimately, shut down this clandestine network. In sum, it elicited 40 criminal convictions (US DOJ, May 14, 2008), of which 32 were discovered for analysis and included in the Copy Cat database. Out of these 32 convictions, only three individuals were sentenced to a term of imprisonment (David Fish, William Venya, and Chirayu Patel).

Ostensibly, each of these three individuals was an important target for the FBI as each individual was at one point in direct communication with the FBI's undercover informant and as each individual was directly responsible for the maintenance and development of the dummy sites. David Fish (See USA v. Fish et al, Case Number 5:05CR00445. N.D. CA, 2008), for example, was a 26 year–old Connecticut resident who was the Site Operator for "CHUD" – the dummy site and main server for the network. He was responsible for scripting the site (i.e. writing programs that aid in the maintenance of the site); supplying it with both hardware and content; cracking and encoding content; and brokering deals with release groups so that these groups would affiliate with the site. Between March

2004 and July 2005, he enabled the release of at least 68 movies and 131 software titles, and for these acts he was convicted on 5 counts of copyright related offenses and sentenced to 30 months imprisonment, 24 months probation, and a fine/restitution of $146,981.

William Veyna, another individual sentenced to a term of imprisonment, was a 34-year California resident who was a Site Operator for two servers: “VS” (or “Victoria Secret”) and its archive site called “VS2”. Veyna acted as a hardware supplier and broker for the sites, and in January 2005, began to associate with Fish and the CHUD server. Veyna’s friend and partner was Chirayu Patel, a 23 year-old California resident,  who aided him by scripting the server, supplying and installing hardware, and brokering deals between release groups. Patel, for example, wrote a script that allowed any content that was uploaded on VS to be automatically uploaded to CHUD. Venya and Patel both pled guilty to two counts of copyright related offenses: Venya was sentenced to 15 months in prison, Patel was sentenced to 18 months imprisonment, and each were given 24 months probation, and a fine/restitution of $172,872 (See USA v. Fish et al, Case Number 5:05CR00445. N.D. CA, 2008 for Fish, Veyna, and Patel’s cases).

After the convictions, the DOJ published Press Releases stating the facts of the case and the sentences doled out as both a success story and a warning (US DOJ, Apr. 29, 2008; US DOJ, May14, 2008). Interestingly, out of the 32 cases found, these were the only cases where terms of imprisonment were assigned. Though these sentences are likely linked to the role and/or level of

culpability in the conspiracy, one question that may be posed is: what is the relation between network centrality and sentence? It seems intuitive that individuals with greater culpability in an organized criminal venture would hold a more central position in the network,[23] and as copyright infringement of this nature is inherently a crime of organized and purposive groups acting in concert, a network analysis is particularly apt. Yet, despite this aptitude, no research has been conducted on the network structure of these illicit networks, and it is unknown if the courts considered such issues when assigning sentence. Thus, the following will examine the relation between sentence and network position. First, it will ask if these three cases (Fish, Veyna, and Patel) match SNA data with respect to centrality. In other words, are the most culpable individuals also the most well connected? Then, this thesis will also aim to answer whether there are other individuals who are material to the connectivity of the network besides these three? If so, who are they, and what did they do in these networks to be so well connected? Finally, the network position of these individuals will be compared and correlated to their fine, as a measure of culpability, to determine if a relationship exists between the centrality of actors from a SNA perspective and the sentence that those actors received.

## 4.1 Network Overview

To start, an overview of the Copy Cat network and how it functions is presented. Below, Figure 2 is a visual representation of the Copy Cat network. The squares denote servers, the circles denote actors, and the lines between

[23] See Baker & Faulkner (1993).

denote links. The graph was produced using Netdraw's "Spring Embedding" which positions "... points in such a way as to put those with smallest path lengths to one another closest in the graph" (Hannenman & Riddle, 2005); however, the nodes were slightly spread out so that the reader may see the labels. In sum, there are 32 actors and 7 servers[24] – five of these actors are isolates.[25] The thicknesses of the lines are indexical to the actor's relation to the server with respect to culpability and access. The thinnest lines denote actors with 'Leech' access to a server – download access but they are not required to upload content (See Soares' link to VS on the upper-left).[26] [27] The next thickest lines denote 'ratio' access to a server – access to download content in proportion to the amount they upload (See Zeman's link to CHUD on the mid-left). In the previous chapter, it is noted that this system of reward is one way that couriers are encouraged to contribute content to the server. The thickest lines denote actors who have Site Operator or Administrator access – partial or complete control over the server (See Russell to HOT on the lower-right).

In the dataset, there were 5 individuals with Site Op/Admin access to (a) server(s) in the network (Fish, Veyna, Patel, Templeton, and Russell). These

[24] HOT and LAD are the same server represented at two different points in time.

[25] These individuals were included because court case documents suggest that these individuals connected to server(s) in the network, but they not specify which server(s). These actors are located in the upper-left of Figure 2.

[26] In the event of a link between actor and server being suggested by the court and the type of access was not specified, leech access was assumed.

[27] At first glance it would seem that many individuals are connected through leech access, and thus, only a few out of the sample were responsible for contributions to the sites. However, US Sentencing Memos describe that hundreds of individuals connected to the these servers, but individuals that were considered "minor or minimal participants" (See Siloac US Sentencing Memorandum, p. 4 in USA v. Templeton et al., Case Number 5:06CR00054, N.D. CA, 2006) were not prosecuted. Individuals in these court cases contributed to further the ends of copyright piracy in some way, and were material actors in the conspiracy.

individuals were responsible for maintenance and day-to-day operations of the server. Noticeably, all three actors who received a term of imprisonment are Site Operators. For example, Patel (top-middle of Figure 2) connects to three servers (CHUD, VS, VS2); two of these, he has Site Operator status. The other two actors with Site Operators access who did not receive a term of imprisonment, Templeton and Russell (lower-right of Figure 2), were both Site Operators of LAD/HOT at different points in time.

Ostensibly, the most connected server in Figure 2 is CHUD, with almost two thirds of individuals in the network connecting to it (23 individuals). Material to this, however, this network was constructed based on court case information and, thus, constructed much like an 'ego network' – observing connections to CHUD & LAD, the dummy sites, and then travelling a few steps out. Thereby, it makes sense that CHUD would appear to be the 'center' of this network. A point re-enforced by Table 3, which lists the SNA centrality scores for servers in the network from highest to lowest Degree. CHUD has the highest of all centrality scores, followed by LAD, then VS. Snowcave ranks in the middle, and the remaining three servers (HOT, VS2, and Wasted Time) tie for last, with only two actors connecting to each of them. In general, the network has a density of .237, which simply indicates that 23.7% of all possible connections between the 32 individuals and the 7 servers are actually made.[28] Thus, though the network is

[28] For comparison, Borgatti & Everett (1997), in their re-examination of Davis et al. (1941) data, constructed a 2-mode network consisting of society women's attendance of social events. The networks Density was reported as .37, or 37% of total connectivity (Id., p. 253). This is approximately .13 higher than Copy Cat's density score. Another example, in a 2-mode drug trafficking network between differing positions in the drug trade, a study by Bouchard et al. (2010) found that the affiliation network had a Density of .32.

not necessarily tightly-knit, actors can connect to each other with relative ease as any actor is one to three steps away from reaching all others.

**Table 3 Copy Cat Network Server Centrality**

| | Degree | Betweenness | Eigenvector |
|---|---|---|---|
| CHUD | 0.719 | 0.543 | 0.831 |
| LAD [aka HOT] | 0.313 | 0.133 | 0.375 |
| VS | 0.281 | 0.078 | 0.349 |
| SNOWCAVE | 0.156 | 0.054 | 0.172 |
| HOT | 0.063 | 0.003 | 0.054 |
| VS2 | 0.063 | 0.001 | 0.099 |
| Wasted Time | 0.063 | 0.001 | 0.070 |

Noticeably, though Fish, Veyna, and Patel were allocated severe sentences, Figure 2 illustrates many other actors in the network who were well-connected but do not receive terms of imprisonment. Evans, for example (located between LAD and Snowcave) holds three links, of moderate culpability/access (Ratio). Fong (located to the left of Evans), is structurally equivalent to Evans with three links of equal weight. Ghani (located in the lower-middle), as well, holds three links, one of which is of moderate culpability/access (Ratio). In addition to this, each of these actors played a significant role in the conspiracy: Evans was a broker and a supplier (much like Veyna); Fong was an encoder; and Ghani was the leader of a release group that affiliated with the CHUD server. A more detailed analysis of individual centrality and sentence follows below.

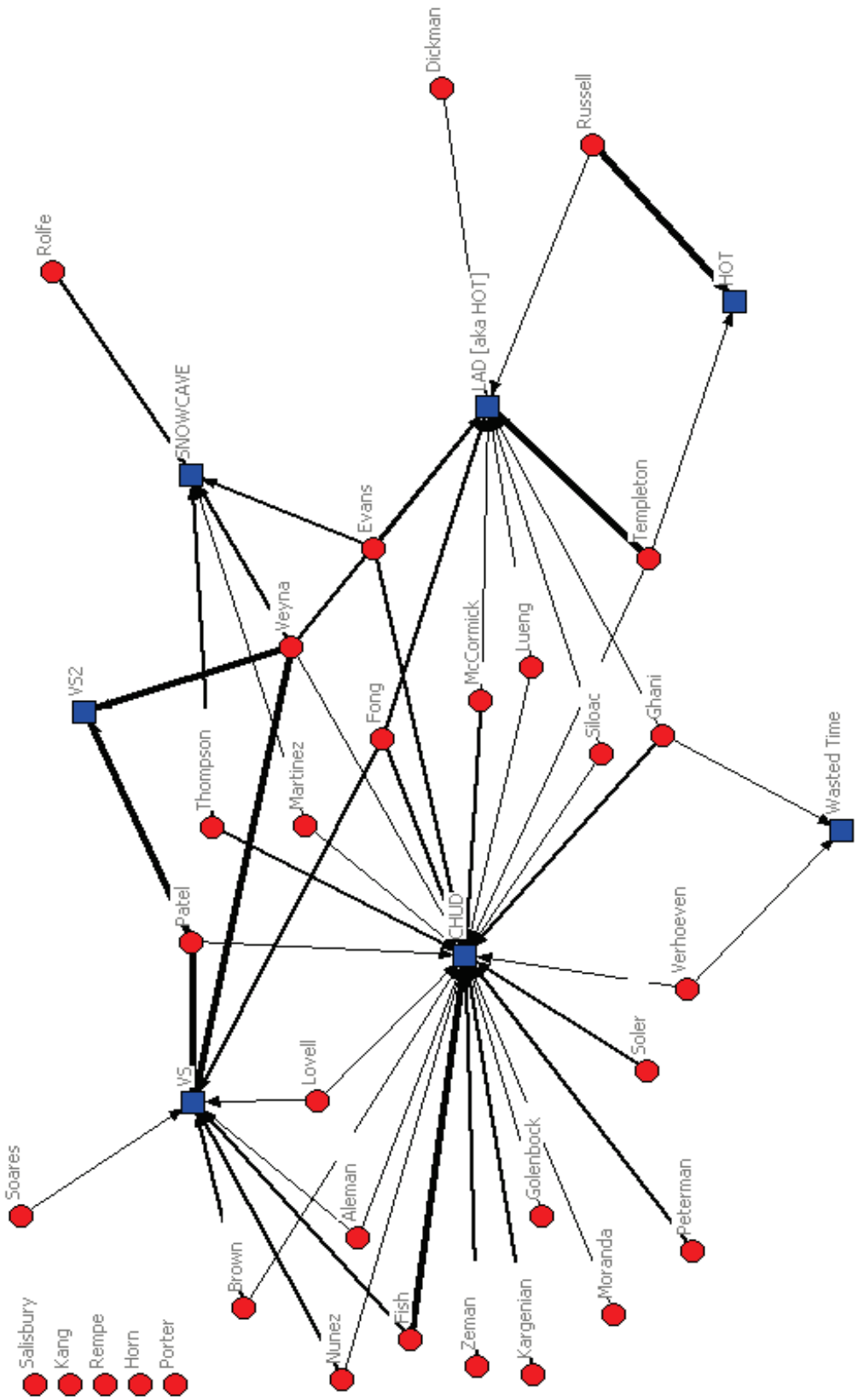



**Figure 2 Copy Cat Network Visual Graph**

## 4.2 Does Punishment Fit the Centrality?

To determine if the three cases that resulted in imprisonment (Fish, Veyna, and Patel) correspond to network centrality, first, each actor's centrality score (Degree, Betweenness, and Eigenvector) were listed from greatest Degree to lowest, below in Table 4. Initially, one may see in Table 4 that the highest ranked individual in each category of centrality is Veyna, as well he has the highest number links (5). Corresponding to these figures, Veyna was sentenced to a term of imprisonment and a high fine/restitution of $172,872. Patel, on the other hand, though sharing a similar sentence to Veyna, ties for second highest, as four other individuals (Ghani, Fong, Templeton, and Evans) score an equal Degree. As well, with respect to other measures of centrality. Despite these similarities, Patel served a term of imprisonment and paid a high fine/restitution; while the other four actors, received moderate to high fines and equal terms of probation.

The third member of the trio, Fish, appears to be much less material to the network. In Table 4, 15 individuals (other than Veyna and Patel) outrank or tie Fish for his Degree and Betweenness. As indicated by this low Betweenness score, his network position does not bridge into any unique servers. In other words, he does not fill any *structural holes* (Burt, 1992) between resource pools. Nevertheless, despite these weak scores, Fish receives the largest term of imprisonment (30 months). From a purely SNA perspective, this is an intriguing result: that an actor who is ostensibly peripheral or, at the very least, immaterial

to the connectivity of the network is doled such a large sentence. Additionally, that 15 other actors who have similar centrality scores are assigned comparatively lenient sentences – with no imprisonment and a mean fine/restitution of $33,350: 5 times less than Patel or Veyna.

**Table 4 Copy Cat Network Actor's Centrality Scores and Sentences**

| Actor | Degree | Betweenness | Eigenvector | Roles | Prison (Months) | Fine |
|---|---|---|---|---|---|---|
| Veyna | 0.714 | 0.094 | 0.327 | Supplier; Broker | Yes (15) | $172,872.68 |
| Patel | 0.429 | 0.025 | 0.229 | Supplier; Scripter; Broker | Yes (18) | $172,872.68 |
| Ghani | 0.429 | 0.039 | 0.228 | Leader | No | $107,663.85 |
| Fong | 0.429 | 0.025 | 0.278 | Encoder | No | $27,645.69 |
| Templeton | 0.429 | 0.054 | 0.225 | Scripter | No | $21,135.32 |
| Evans | 0.429 | 0.033 | 0.246 | Broker; Supplier | No | $10,982.00 |
| Fish | 0.286 | 0.006 | 0.211 | Supplier; Encoder; Scripter; Broker | Yes (30) | $146,981.46 |
| Verhoeven | 0.286 | 0.020 | 0.161 | | No | $69,756.17 |
| Lovell | 0.286 | 0.006 | 0.211 | Supplier | No | $57,863.02 |
| Aleman | 0.286 | 0.006 | 0.211 | Supplier | No | $48,478.01 |
| Nunez | 0.286 | 0.006 | 0.211 | Cracker | No | $34,615.31 |
| Thompson | 0.286 | 0.014 | 0.179 | | No | $22,380.93 |
| Lueng | 0.286 | 0.008 | 0.216 | | No | $18,385.76 |
| Brown | 0.286 | 0.006 | 0.211 | | No | $16,532.00 |
| McCormick | 0.286 | 0.008 | 0.216 | Courier | No | $15,881.30 |
| Russell | 0.286 | 0.008 | 0.077 | | No | $11,508.93 |
| Siloac | 0.286 | 0.008 | 0.216 | Courier | No | $4,074.00 |
| Martinez | 0.286 | 0.014 | 0.179 | Courier | No | N/A |
| Zeman | 0.143 | 0.000 | 0.149 | Courier | No | $120,000.00 |
| Kargenian | 0.143 | 0.000 | 0.149 | | No | $89,614.36 |
| Soler | 0.143 | 0.000 | 0.149 | | No | $69,818.00 |
| Golenbock | 0.143 | 0.000 | 0.149 | Supplier | No | $63,699.98 |
| Dickman | 0.143 | 0.000 | 0.067 | | No | $31,515.50 |
| Rolfe | 0.143 | 0.000 | 0.031 | Supplier | No | $31,203.60 |
| Moranda | 0.143 | 0.000 | 0.149 | | No | $21,483.86 |
| Soares | 0.143 | 0.000 | 0.062 | Supplier | No | $17,222.95 |
| Peterman | 0.143 | 0.000 | 0.149 | | No | $3,577.98 |
| Horn | 0.000 | 0.000 | 0.000 | | No | $69,756.17 |
| Kang | 0.000 | 0.000 | 0.000 | | No | $23,809.89 |
| Salisbury | 0.000 | 0.000 | 0.000 | Supplier | No | $4,000.00 |
| Porter | 0.000 | 0.000 | 0.000 | Courier | No | $3,611.60 |
| Rempe | 0.000 | 0.000 | 0.000 | Supplier | No | $3,471.91 |

For example, the third highest individual listed in Table 4, Ali Ghani, is connected to three servers – one of which is the headquarter server for a video release group called “WastedTime”. Ghani was the leader of the group and would work with Brian Verhoeven to release films that were screened at a hotel.

Though Ghani was given a moderately large fine ($107, 663), he received no term of imprisonment, and an equal term of probation to almost every other actor in the network. As well, Verhoeven, who has about equal centrality scores to Fish, is the only actor in the network to sell copyrighted material and make a profit from his participation in the conspiracy, yet he receives a fine of $69,756 (2.5 times less than the fine imposed on to Venya or Patel) and no term of imprisonment. Another individual, Phillip Templeton, who scored higher on all centrality scores than Fish, and tied Patel for Degree, was allotted a moderately low fine ($21,135). However, Templeton was similar to Fish and Patel in that he was a Scripter and Site Operator for LAD, a server under surveillance by the FBI.

Thus, the results of this first cursory analysis indicates: 1) although Veyna's, and to some extent Patel's, sentences correspond to their SNA centrality scores, that Fish's scores are very low considering his high sentence. 2) As well, there are many actors (15) of equal or greater centrality than Fish and Patel, who received significantly more lenient sentences. 3) Some of these individuals, such as Templeton, even had similar roles in the conspiracy, with a similar amount of surveillance by law enforcement. As such, there are actors in the network who are highly central, and significant to the connectivity of the network, but were over-looked by the courts in terms of sentencing.

### 4.2.1 Categorical Core/Periphery Analysis

Two-mode SNA provides a more systematic method of identifying *core* participants in a network. The method, called "core/periphery analysis" (C/Pa), is analogous to well-known cluster analysis methods, as it attempts to create

groups of similar characteristics – in this case – groups of actors and servers with similar connections between each other. This method uses a genetic algorithm to cluster actors and servers together, aiming to achieve an optimal fitness,[29] in which there are two groups for each axis in the matrix: the core and the periphery (Hannenman & Riddle, 2005). Using this method, researchers can locate core actors in a network that account for most of the network's connectivity. As such, this method is used to analyse the Copy Cat network, and the results offer a privileged perspective on network centrality.

Table 5 lists the results of this analysis. The network used in this analysis is weighted, in other words, links between individuals and servers have values that are dependent on level of site access (1=Leech; 2=Ratio; 3=Site Op/Admin). The results show that the "core" consists of the three most central servers (LAD, CHUD, and VS) and places the other four in the periphery. With respect to actors in the network, all three of the individuals sentenced to a term of imprisonment are located in the core. In addition, the C/Pa also included four other actors as members of the core (Fong, Evans, Russell, and Templeton). These four actors each have moderate to strong link weights, and are each connected to at least two servers. Fong and Evans, as discussed in the previous section, have structural equivalency to each other, as each possesses three links of equal weight. Additionally, out of the 7 actors, 5 are Site Operators, whom we would expect to be important targets for the FBI.

[29] Fitness is measured by cluster density, in a C/Pa of ideal fitness the "core " will have a density of 1, while the "periphery" will have a density of 0.

**Table 5 Copy Cat Network Actor's Centrality Scores and Sentences**

Starting fitness: 0.585
Final fitness: 0.688

**Weighted Network**

Blocked Adjacency Matrix

| | | 2 L | 3 C | 5 V | 1 H | 4 S | 6 V | 7 W |
|---|---|---|---|---|---|---|---|---|
| 1 | Templeton | 3 | 1 | | 1 | | | |
| 22 | Veyna | 2 | 1 | 3 | | 2 | 3 | |
| 5 | Fong | 2 | 2 | 2 | | | | |
| 20 | Fish | | 3 | 2 | | | | |
| 17 | Evans | 2 | 2 | | | 2 | | |
| 8 | Russell | 1 | | | 3 | | | |
| 21 | Patel | | 1 | 3 | | | 3 | |
| 2 | Siloac | 1 | 1 | | | | | |
| 3 | Thompson | | 2 | | | 2 | | |
| 10 | Dickman | 1 | | | | | | |
| 7 | Ghani | 1 | 2 | | | | | 1 |
| 12 | Peterman | | 2 | | | | | |
| 11 | Soares | | | 1 | | | | |
| 14 | Moranda | | 1 | | | | | |
| 15 | Nunez | | 1 | 2 | | | | |
| 16 | Brown | | 1 | 2 | | | | |
| 9 | Rolfe | | | | | 2 | | |
| 18 | Martinez | | 1 | | | 1 | | |
| 19 | Aleman | | 1 | 1 | | | | |
| 4 | Kargenian | | 2 | | | | | |
| 13 | Lueng | 1 | 1 | | | | | |
| 6 | Soler | | 2 | | | | | |
| 23 | Lovell | | 1 | 1 | | | | |
| 24 | Zeman | | 2 | | | | | |
| 25 | Salisbury | | | | | | | |
| 26 | Golenbock | | 1 | | | | | |
| 27 | Kang | | | | | | | |
| 28 | Rempe | | | | | | | |
| 29 | Horn | | | | | | | |
| 30 | Verhoeven | | 1 | | | | | 1 |
| 31 | McCormick | 1 | 2 | | | | | |
| 32 | Porter | | | | | | | |

Density matrix

| | 1 | 2 |
|---|---|---|
| 1 | 1.400 | 0.481 |
| 2 | 0.452 | 0.062 |

Starting fitness: 0.667
Final fitness: 0.714

**Dichotomized Network**

Blocked Adjacency Matrix

| | | 2 L | 3 C | 5 V | 1 H | 4 S | 6 V | 7 W |
|---|---|---|---|---|---|---|---|---|
| 1 | Templeton | 1 | 1 | | 1 | | | |
| 22 | Veyna | 1 | 1 | 1 | | 1 | 1 | |
| 7 | Ghani | 1 | 1 | | | | | 1 |
| 5 | Fong | 1 | 1 | 1 | | | | |
| 17 | Evans | 1 | 1 | | | 1 | | |
| 21 | Patel | | 1 | 1 | | | 1 | |
| 4 | Kargenian | | 1 | | | | | |
| 2 | Siloac | 1 | 1 | | | | | |
| 8 | Russell | 1 | | | 1 | | | |
| 10 | Dickman | 1 | | | | | | |
| 3 | Thompson | | 1 | | | 1 | | |
| 12 | Peterman | | 1 | | | | | |
| 11 | Soares | | | 1 | | | | |
| 14 | Moranda | | 1 | | | | | |
| 15 | Nunez | | 1 | 1 | | | | |
| 16 | Brown | | 1 | 1 | | | | |
| 9 | Rolfe | | | | | 1 | | |
| 18 | Martinez | | 1 | | | 1 | | |
| 19 | Aleman | | 1 | 1 | | | | |
| 20 | Fish | | 1 | 1 | | | | |
| 13 | Lueng | 1 | 1 | | | | | |
| 6 | Soler | | 1 | | | | | |
| 23 | Lovell | | 1 | 1 | | | | |
| 24 | Zeman | | 1 | | | | | |
| 25 | Salisbury | | | | | | | |
| 26 | Golenbock | | 1 | | | | | |
| 27 | Kang | | | | | | | |
| 28 | Rempe | | | | | | | |
| 29 | Horn | | | | | | | |
| 30 | Verhoeven | | 1 | | | | | 1 |
| 31 | McCormick | 1 | 1 | | | | | |
| 32 | Porter | | | | | | | |

Density matrix

| | 1 | 2 |
|---|---|---|
| 1 | 0.765 | 0.182 |
| 2 | 0.342 | 0.049 |

As the C/Pa constructs the “Core” cluster to be the most central actors in the network, the actors in the Copy Cat Core group can be considered *Key-Players* (Borgatti, 2006) in the network, and nearly half of all connection in the network (21 out of 53) are held by these Core actors. In other words, ~22% of the network’s actors accounts for ~50% of the connectivity. Table 6 lists the “Core”

group's, and "Periphery" group's, mean: age, fine, amount infringed, and number of links.

**Table 6 Copy Cat Network Weighted Core/Periphery Actors Means**[30]

| | Core | Periphery | Significance 2-Tail t-test | Total Network |
|---|---|---|---|---|
| N | 7 (Fish; Veyna; Patel; Russell; Templeton; Evans; Fong) | 24 | - | 32 |
| Mean Age (STD) | 24.0 (6.4) | 25.7 (8.0) | .636 | 25.3 (7.6) |
| Mean Fine (STD) | $80,571.25 ($78,946.64) | $39,517.34 ($24,154.93) | .291 | $48,787.58 ($49,450.38) |
| Median Fine | $27,645.69 | $27,506.75 | - | $27,645.69 |
| Mean Amount Infringed (STD) | $445,714.29 ($518,486.81) | $64,500.00 ($48,037.81) | .061 | $163,333.33 ($304,476.22) |
| Median Amount Infringed | $30,000.00 | $70,000.00 | - | $70,000.00 |
| Mean # of Links (STD) | 3.0 (1.0) | 1.28 (.8) | - | 1.7 (1.1) |

The results indicate that the "Core" group's mean fine is more than double the "Periphery". This value, though, does not indicate a significant difference in means. The mean amount infringed by the "core" is approximately 7 times higher than of the periphery, and is close to significant (.061). These results create a hazy view of the sample, as the difference of means is very high and suggest

[30] Significance tests for Fine and Amount Infringed were logged prior to conducting t-test to control for the large values in the dataset. However, non-logged values are presented in the table. Additionally, the C/Pa constructs its groups by attempting to create an optimum fitness with respect to density; thus, number of links are a dependent variable, and its significance is not reported.

greater culpability for the “Core”, but the median reports the opposite. Thus, in the “Core” there are a few very powerful players (Fish, Veyna, and Patel), that skew the sample. When fine was tested against amount infringed to discover if a pattern exists between sentence and culpability measured by the court, a very high correlation ($p<.001$) was discovered.[31] These results, in concert with the fact that the core was constructed to maximize density while pairing actors of similar patterns of connectivity, suggests that network centrality is not significantly related to sentence or culpability, as measured by fine.

Note that the C/Pa above took role into account. Site Operators, for example, were coded as such, which influenced the C/Pa as it tried to identify the core from the periphery.[32] This serves the aim of the court well in that the courts also take role into account to determine culpability. At the same time, it is useful to examine exactly how much that coding influenced our results, if at all. To find out, the network was dichotomized: the presence of a connection was simply coded as 1, and absence as 0. This dichotomized network was also tested with a C/Pa, and the results are located in Table 7.

[31] This high correlation exists with or without the three imprisoned included. This results is expected as the MPAA, BSA, and ESA helped calculate the values that the court relied on for sentencing; which, in turn, were mimicked for restitutions paid back to these organizations.

[32] The link weight provides an additional piece of information for the algorithm to take into account, in addition to connection patterns. This is analogous to a cluster analysis drawing from two, instead of one characteristic.

**Table 7 Copy Cat Network Dichotomized Core/Periphery Actors Means**[33]

| | Core | Periphery | Significance 2-Tail t-test | Total Network |
|---|---|---|---|---|
| N | 6 (Veyna, Patel, Evans, Fong, **Ghani**, Templeton) | 26 | - | 32 |
| Mean Age (STD) | 23.5 (7.3) | 25.7 (7.8) | .613 | 25.3 (7.6) |
| Mean Fine (STD) | $85,528.70 ($75,897.39) | $39,969.70 ($37,922.51) | .183 | $48,787.58 ($49,450.38) |
| Median Fine | $67,654.77 | $23,809.89 | - | $27,645.69 |
| Mean Amount Infringed (STD) | $368,333.33 ($490,526.93) | $104,761.90 ($210,127.80) | .266 | $163,333.33 ($304,476.22) |
| Median Amount Infringed | $75,000.00 | $70,000.00 | - | $70,000.00 |
| Mean # of Links (STD) | 3.3 (.8) | 1.3 (.8) | - | 1.7 (1.1) |

The dichotomized C/Pa includes the same servers in its core (LAD, CHUD, and VS), but with two differences with respect to actors: two actors disappear from the core, including Fish (the other is Russell); and a new core player if found: Ghani. When this "Dichotomized Core" undergoes the same tests for differences in mean, with respect to sentence, the values are extremely similar. In fact, the dichotomized C/Pa resulted in an additional $5,000 difference

[33] Significance tests for Fine and Amount Infringed were logged prior to conducting t-test to control for the large values in the dataset. However, non-logged values are presented in the table. Additionally, the C/Pa constructs its groups by attempting to create an optimum fitness with respect to density; thus, number of links are a dependent variable, and its significance is not reported.

between the Core and Periphery. The median fine for the Core is now higher than the peripheral group. As well, the mean number of connections is .33 higher now in the Core group over the weighted sample. However, none of these values indicate significant differences in mean between the “Core” and “Periphery”. The dichotomized C/Pa cannot tell the difference between individual relations to servers, and as well, the “Dichotomized Core” contains two less Site Operators: yet, it still retains similar levels of connectivity and sentence. Thus, this re-enforces the notion that there is not a relation between centrality and sentence, with respect to fine, in this network. Interestingly, when fine is compared to number of connections, for the entire network, the results indicate a .40 Pearson Correlation (.037 significance), and an equal correlation when compared to amount infringed (.026 significance). However, if the three imprisoned actors are removed, and the Pearson correlations drop to .04 for fine and .214 for amount infringed with respect to number of connections: neither is significant.[34]

In the weighted network all three imprisoned actors (Fish, Veyna, and Patel) were included in the “Core” group by the weighted C/Pa; however, there are five other individuals who are central to the network according to this method who did not receive terms of imprisonment. These individuals were “Core” actors, or network *key-players*, but somehow evaded sentencing.

### 4.2.2 Over-looked *Key-Players*

The above analysis showed that the three imprisoned members were also identified as belonging to the “core” of the Copy Cat network, but that at least 5

[34] Fine and Amount Infringed were logged prior to this test to control for the large values.

other individuals could not be differentiated in the SNA data from this initial top three players. Table 8 lists the difference in means between the imprisoned trio and five other actors found in the C/Pa (Fong, Templeton, Russell, Evans, and Ghani). Notably, there is very little variation in the imprisoned with respect to fine and amount infringed as opposed to the over-looked key-players group, who have high standard deviation values. As well, the imprisoned group contains a higher mean number of connections, but the difference is slim. To understand these five over-looked *key-players*' circumstance better, to both elucidate why they were so well connected and why they evaded imprisonment, the following will delve into each of these five "Core" actors' court case documents for qualitative information.

**Table 8 Copy Cat Network Imprisoned Actors Compared to Over-Looked *Key-Players***

| | **Official key players: Fish, Veyna, and Patel** | **SNA derived other key players: Fong, Templeton, Russell, Evans, and Ghani** |
|---|---|---|
| Mean Fine (STD) | $164,242.27 ($14,948.30) | $35,787.16 ($40,779.73) |
| Median Fine | $172,872.68 | $21,135.32 |
| Mean Amount Infringed (STD) | $1,000,000 (0.0) | $48,000.00 ($40,249.22) |
| Median Amount Infringed | N/A ($1,000,000) | $30,000.00 |
| Mean # of Links (STD) | 3.3 (1.5) | 2.8 (.4) |

**Matthew Fong** (See USA v. Templeton et al, Case Number 5:06CR00054. N.D. CA, 2007), an 18 year-old Florida resident at the time of the

conspiracy operating under the alias “cyber”, was connected to three servers in the network (LAD, CHUD, and VS) with ratio access, and was responsible for a terabyte of site traffic during his participation, between August 2004 and June 2005. Fong was an encoder: he would convert films into playable and transmittable formats and strip their copyright protection features, such as identification markers. As well, Fong would encode films for other defendants as well as instruct other actors in the network on how to encode films and methods of *camming*. For example, he worked with Curtis Salisbury (USA v. Salisbury, Case Number 5:05CR00505. N.D. CA, 2006), a *cammer* and another defendant in the conspiracy, on one occasion in June 2005 to remove the copyright protection from the films “Bewitched” and “The Perfect Man”. The courts predicted his maximum infringement amount at $30,000. He was sentenced to 36 months probation and a fine/restitution of $27,645.

Much like in the larger dataset, as a Cracker of-sorts, Fong is relatively young and has no criminal history; as well, his sentence is slight even in relation to actors outside of the “Core” group. From the perspective of individual role, this lenient sentence corresponds with the results found in the previous chapter.

**Phillip Templeton** (USA v. Templeton et al, Case Number 5:06CR00054. N.D. CA, 2007), the Site Operator and Scripter for LAD, went by the alias “kryptor”. Between November 2003 and March 2005, Templeton was responsible for 490 gigabytes of traffic between the servers in the network. Templeton was highly active in the maintenance of LAD, as he would install hardware, control site access, and create security features to protect the site. He had three

connections in the network (CHUD, LAD, and Hot). The courts predicted his maximum infringement amount at $30,000. He was sentenced to 36 months probation and a fine/restitution of $21,153.

Templeton played a significant role in the construction, maintenance, and security of LAD, which would lead one to wonder why his sentence was so slight compared to Patel: who is structurally similar and similar in role. One answer to this may be the difference of size and severity between LAD/HOT and CHUD. LAD/HOT started out at 700 megabytes and grew to 3.5 terabytes over the course of the investigation. LAD/HOT became the archive site for CHUD, and old content that CHUD did have space for was moved to LAD/HOT. CHUD, in comparison was 11 terabytes (over 3 times bigger) and contained newly released content. Thus, it may be that the courts saw Templeton as a less significant actor in the conspiracy, as the site was smaller and less material to the release of content. As well, fewer individuals in the network had access to LAD/HOT than CHUD.

**Johnny Russell** (See USA v. Templeton et al, Case Number 5:06CR00054. N.D. CA, 2007), the Site Operator of HOT (the same server as LAD at a different point in time) went by the alias “wishbone”, and like Templeton, was responsible for the maintenance of the site. However, in Russell’s case, his Defence Sentencing Memorandum provides a story that suggests that his involvement in the conspiracy was restricted to “... [managing] the TV section of one of the sites that was already in existence. ... [His] sole function and responsibility was to delete the old television shows and replace them with

current episodes" (Russell Defence Sentencing Memorandum, Id.). As well, the courts predicted his maximum infringement amount at $30,000. He was sentenced to 36 months probation and a fine/restitution of $11,508. Russell's evasion of a prison sentence makes sense in light of these circumstances: LAD/HOT was much smaller than CHUD, and Russell's involvement, as purported in his defence, was extremely limited.

**Deston Evans** (See USA v Nunez et al., Case Number 5:05CR00734. N.D. CA. 2007), an equipment supplier and broker, went by the alias "hammer". He had three Ratio links in the network (LAD, CHUD, and Snowcave); as well, it is noted in sentencing memos that he contributed funds to help support the operating costs of CHUD. Between May 2004 and July 2005, Evans was responsible for only 41.5 gigabytes of traffic between the servers. The courts predicted his maximum infringement amount at $30,000. He was sentenced to 36 months probation and a fine/restitution of $10,982. Fewer documents were available that explained Evan's role in the network, and thereby information pertaining to Evan's involvement was slim. However, his Indictment reports that he had contributed $2,962 to Fish, to help maintain the site. It seems that Evan's contribution to the network was logistical, as he was helping to support the site financially and was brokering deals to have groups affiliate with the site. His small sentence, in comparison to other actors of similar structural equivalency, may be because his financial contributions suggest him to be an actor of minor participation; in other words, Evans may have not had content or skill to contribute.

**Ali Ghani** (See USA v. Templeton et al, Case Number 5:06CR00054. N.D. CA, 2007), a leader of the release groups “Wasted Time” and “Wasted Kung Fu”, was connected to three servers in the network (CHUD, LAD, and Wasted Time). He had ratio access to LAD, and Leech to the other two. Ghani went by the alias “waters” and was responsible for uploading at least 16 movies and 4 games/software to the network, and it was estimated that he was responsible for 300 gigabytes of traffic between servers in the network. The courts predicted his maximum infringement amount at $120,000. He was sentenced to 36 months probation and a fine/restitution of $107,663.

Ghani’s case is an odd one: he is a core actor by both role and network position; yet, he receives the same term of probation as every other actor, but with a high fine. One explanation for this is the difference between Ghani’s defence and the court: in his defence he claimed to be a minor participant; while the court, in their Indictment and Sentencing Memorandum, suggested that he was significant to the release of content. In Ghani’s defence Sentencing Memorandum, his attorney argued that a) the content that was purportedly “uploaded” by Ghani was merely transferred between servers at the behest of the FBI, and he had not uploaded new content, and b) that the account Ghani used for the server(s) was a shared account between other users. The courts, on the other hand, suggest that he is the leader of two release groups that were supplying pre-released films. In concert with the court’s holding that Ghani had access to such content, a co-conspirator in a separate case (Brian Verhoeven (USA v. Verhoeven, Case Number 5:06CR00247. N.D. CA, 2007)), who was also

a member of Wasted Time, had sold copies of films that he had downloaded from the various servers in the network, of which he had accessed approximately 700 of these films from the Wasted Time's headquarter server.

Ghani's case, being as odd as it is, demonstrates the difficulty of prosecuting warez cases. Though the courts have evidence that an account had transmitted a certain amount of content between servers, identifying the actor responsible and whether or not he/she was the provider of the content or simply the messenger may be difficult. Although Ghani may be a central SNA actor, whether or not he is a highly culpable actor is still unknown, and presumably, this uncertainty played a role in his sentencing.

### 4.2.3 Is there a relation between Sentence and Centrality?

The results are hazy, as some evidence suggests this connection while others suggest no-relation at all. Two of the three actors who received a term of imprisonment (Veyna and Patel) both had central SNA scores and both had high fines along with their terms of imprisonment. However, Fish, the third actor to receive a term of imprisonment, had very moderate SNA scores but received a high fine along with his term of imprisonment. As well, when the C/Pa was conducted, the results indicated five other actors that were central to the network,[35] but their sentences (fines) were not significantly different from periphery actors. When sentence (fine), for the entire network, was tested against number of links held by each actor, a correlation exists – however, when

[35] This includes all Core actors between both the weighted and dichotomized C/Pa.

the three imprisoned actors are removed from the sample, this correlation disappears.[36]

Additionally, when over-look network *key-players* are qualitatively examined for explanations that may mitigate or aggravate culpability, a number of issues emerge. One, for example, is role in the conspiracy: Fong is an encoder, a form of cracker, and as indicated by the SCP chapter and previous literature, these individuals receive slighter sentences. Another is size/weight of the server to which one connects. Though Templeton is structurally equivalent to Patel and is largely equivalent by roles and site access, the size/weight of the LAD/HOT server that he operates is much smaller than that of CHUD. Last, the amount of evidence that is aggregated by the court has an impact on the strictness of the sentence. Ghani, for example, though being relatively highly culpable to the release of content, both by role and network position, receives the same term of probation, but with a higher fine. This could have been because of gaps in evidence, pointed out by the difference in Court and Defence Sentencing Memorandums – such as Ghani's role as a leader of a release group, the amount of content for which he was responsible, and whether the evidence gathered by the court even implicated Ghani, as he suggests others used his account.

In contrast to each of these, the three imprisoned individuals in the sample all: 1) had roles that, by comparison to the previous chapter, are one's for which

[36] A significant issue related to Fish's sentence is his guilty plea to distribution of technology used to circumvent encryption technology. US sentencing guidelines mandate that if an offense breaches 17 USC 1201 and/or 1204, then one's sentence will be adjusted to a minimum of level 12. Thus, Fish's Adjusted Offense Level was a minimum of a Zone C penalty – increasing his probability of a prison term.

the courts impose higher sentences (See Table 1; Site Ops/Admins); 2) had control/high-access to a site of significant size/weight; and 3) had much tighter cases with respect to evidence, as only in four cases (Fish, Veyna, Patel, and Lovell) is the information provided by the undercover informant included. As well, three of these individuals alone account for approximately 1/5$^{th}$ of the networks connectivity (10 links out of 52 total links). Thus, it appears that the relation between network centrality in this sample is led by these three individuals, as in their absence, sentence is not related centrality.

# 5: DISCUSSION

This study aimed to examine and discover methods to disrupt the activities of release groups. Employing a crime-script of the release process and a Social Network Analysis of these groups' distribution design. The study has yielded several interesting results. With respect to the crime-script and attempts to disrupt the release process, prevention schemes must disrupt activities, through increased risk and effort or decreased reward (Clarke, 1980), without further encouraging behaviour through counterproductive prevention (Wortley, 2003; Wortley, 2001; Grabosky, 1996). The data suggests that law enforcement may be able to increase the effort groups employ and industry may be able to decrease the rewards gained by groups, without increasing the risk of counterproductive prevention.

With respect to the Social Network Analysis, the data paints an interesting picture regarding the relation between sentence and centrality. For example, the Copy Cat network exhibits some evidence that demonstrates a "security vs. efficiency trade-off" (Morselli, 2009, pp. 63-71), as central actors such as Veyna and Patel received terms of imprisonment; however, other actors who were also central received lighter sentences. Additionally, as the objective of site operators in this group was to acquire new content for their sites, through affiliation with release groups, *social capital* (Burt, 1992; Burt, 2005) helps shape their opportunities, as greater access to resource may equate to more network or

individual success (Hulst, 2009, pp. 105 -110). Finally, when *key-players* (Borgatti, 2006) in the network were located with UCInet's "Core/Periphery Analysis", the results showed large difference in fines received between the core and periphery; however, when tested, this difference was not significant. As well, when sentence (fine) was tested against network centrality (number of links) no relation was found. This section will discuss the results of both the crime-script and the social network analysis, followed by the limitations of this study and avenues for future research.

## 5.1 Crime-Script: Release Groups and Situational Crime Prevention

The question at issue regarding release group piracy and disruption efforts is how to disrupt release groups when the methods used to prevent their behaviour may serve only to further encourage it. Examining cases of individuals involved in release groups, motivations suggested by the existing literature are indeed present in this dataset, for example some individuals' perceived rewards being gained through circumventing DRM and others from the prestige gained from releasing content.

Digital content may be protected by two means; by industry, through DRM, and by law enforcement, through policing (Holsapple et al., 2008). Each of these may disrupt release group activities by increasing effort, increasing risk, reducing rewards, reducing provocations, or removing the excuses that offenders may use to justify their behaviours (Bullock et al., 2010; Clarke, 1995; Cornish and Clarke, 2003). Situational crime prevention is often concerned with modifying the

environment, in order to control contextual factors that facilitate the commission of a criminal event. However, cybercrime is committed in a digital environment where authorities have little or no control. Thus, the traditional crime control methods suggested by SCP, such as screening exits, denying benefits, and/or discouraging imitation (Cornish and Clarke, 2003) are difficult, if not impossible, to implement in the warez scene. Put simply, industry and law enforcement have no home field advantage and such environmental modifications are impractical.

As such, when applying these SCP concepts, some are more useful than others. First, the difficulty in employing a prevention strategy targeting justifications used by individuals in warez groups is that, with respect to certain copyright issues, these justifications may be right: for example, the rising price paid by consumers for audio CDs in the late 1990s despite decreased cost of production by record companies may have contributed to the rise of Napster (Kot, 2009). Second, with respect to reducing provocations, though it may be the case that announcements by DRM industries may result in release groups taking notice of particular content, it is unknown if this is an issue which needs to be resolved,[37] as it has been suggested that encouraging compliance with copyright may prevent illicit copying (Wortley, 2001, p. 20). Third, with respect to reducing rewards, unlike many criminal behaviours, the cracking and distribution of copyrighted content is perceived by many in the warez scene to be not just a means, but an end in itself. For those seeking prestige, however, one suggestion

[37] However, McCandless (1997) describes a scenario in which a DRM technology had been created and advertised as particularly difficult to crack—calling it a "clarion to crackers if there ever was". The technology was cracked two weeks after its release by the release group DoD.

might be to disrupt bragging channels or to disseminate disinformation. However, it is unlikely that industry or law enforcement could gain access to the private communication channels that these groups employ—and if so, more suitable disruptive measure could be employed, such as gathering information on individuals within the group, than interfering with their bragging opportunities.

Thus, the two options that are left, from a SCP perspective, are to (a) increase the effort, or to (b) increase the risk involved with releasing content. With respect to increasing effort, this is typically an issue for industry and is difficult to prescribe—and as the challenge of cracking difficult DRM technologies may be a motivating factor for these groups, adjustments in DRM to increase the effort necessary to crack them may lead to counterproductive prevention. Additionally, some consumers may dislike DRMs; industry would need to decide whether amendments in these technologies outweighed the possible negative factors ascribed to them—for example, the cost of manufacturing and employing DRM, or the risk of DRM technology disrupting the use of the content to legitimate consumers. With respect to increasing risk, this is typically an issue for law enforcement, and there is the question of what to make more risky: increasing the risk associated with every process may again result in counterproductive prevention, by encouraging thrill seekers or re-enforcing an ideology held by some in these groups.

However, with the use of the data gathered by this study and the construction of the crime script, we find that these traditional prevention schemes may actually increase their impact by trading hands: that is, industry increasing

the risk (rather than effort), and law enforcement increasing the effort (rather than risk). Industry may have the ability to increase the perceived risk associated with the commission of copyright piracy by amendments in DRM technology, and law enforcement may increase the effort by targeting and apprehending the most crucial members of top release groups. Neither prevention scheme modifies the digital environment in which the crime is committed, but rather counts on the digital environment's aim for content quality and competition in their design. These options are discussed below.

### 5.1.1 Possible Disruption Schemes

Any successful policy that aims to curb release group piracy is one that accounts for the paradox that occurs between increasing effort/risk and offender motives. This study suggests the following policy recommendations. For industry, DRM technologies may be modified to be more latent, with slow activating features which may slip by unnoticed by testers, thereby increasing the risk associated with releasing content by putting groups' prestige at risk. For law enforcement, investigations should focus their efforts on apprehending crackers from top groups, thereby increasing the effort needed by top groups to commit an offense.

#### Industry

Regarding specific methods of adjusting DRM techniques and technologies, little information is available through court documents to explain the specific methods used to defeat these protections. Specific amendments to these

protections may be better discovered through other methods of study, such as computing science or industry research and development. What court case data does illuminate through the crime script analysis, however, is the relation between release group structure (e.g. the iteration step between crackers and testers) and the groups' goal to release functional content. Releasing ill-cracked content can result in a loss of prestige for groups, and elite groups will go to great lengths to ensure that released content is up to 'scene standard'. Disrupting the cracker–tester process would place groups' ability to gain prestige at risk when they attempt to release content.

A good example of a warez copyright protection that targeted warez groups' prestige is described by McCandless (1997):

> *Nobody wants the ignominy of anything like the bad crack for Autodesk's 3D Studio that made the rounds in 1992. For all the intents and purposes it ran correctly, all features seemed 100 percent functional. Except that the dedongled program slowly and subtly corrupted many 3-D model built with it. … A rectified "100 percent cracked" version appeared soon after, but the damage was done. The Myth of the Bad Crack was born, and the pirates groups' reputations tarnished* (McCandless, 1997).

Notably, this example is close to twenty years old, and obviously much has changed since in the methods used to crack and protect software. However, this example illustrates a method to use the groups' motivations against them. As every group is attempting to crack and release content as quickly as possible, there is a limited amount of time a group may be willing to allot for testing in order to beat other groups to the finish line. Employing a slow and unnoticeable (i.e. latent) copyright protection that allows ill-cracked software to slip through the

cracker–tester iterations would target the process by which groups obtain prestige, and simultaneously leak useless content into the scene. Groups will lose respect and prestige for their bad cracks. Couriers who transmit the ill-cracked content will lose credits from distribution sites. Sites will lose prestige and may be ranked lower if they distribute ill-cracked content. End users will be frustrated and discouraged by wasting their time and download credits on bad or unusable content. The internal quality control methods typically employed by the scene would act against the release group's interests by making the process of obtaining prestige far more risky. Thus, copyright protection features with a latent disruptive characteristic may make it possible to make the risk of releasing a type of content too high in the eyes of the warez scene. In other words, the potential loss of prestige and peer-approval within the scene may be so high that groups will avoid releasing software with this particular copyright protection.

To give an example of this how this type of protection may operate, consider the following. Under The Game Scene Charts' rules, the method of scoring releases is listed, detailing how games that require greater skill to crack are given more points. For example, a game with complex copy protections is worth 8 points; whereas a game with no copy protection but with an installation key is worth 5.5 points (TGSC, 2010). A game protected by a simpler form of DRM would be less desirable as a release, as it would yield fewer points for the group. Additionally, if this DRM were to enact under a latent condition, after the content has already been in use, then the content might already be distributed, resulting in damage to the group's reputation. As the content is valued less on

the point scale, but carries a greater risk of failure, it may be a less desirable target and future content by that game developer may follow suit.

Significantly, these features need not be more difficult or more obtrusive than current DRM technologies. In fact, they may even be more innocuous; they only need to be latent and activate, possibly randomly, at a period of time much later in the course of using the content. Of course, as with any copyright protection, the possibility for counterproductive prevention is present; however, by accounting for, and specifically targeting, motivations that drive warez scene piracy, the objective is *not* to increase effort, but to increase risk. As an added bonus, copyright protection features of this sort may foster an environment of uncertainty by allowing ill-cracked content to be shared amongst end-users.

**Law Enforcement**

Regarding efforts which may aid law enforcement in policing release group piracy, law enforcement may be able to increase the effort required for groups to release content. The crime script highlights two issues that aid in this endeavour: steps in the script which are more vulnerable to disruption, and steps which are visible to law enforcement. As a few groups are responsible for most of the illicit content available online (Goode, 2010; Urbas, 2006; CCIPS, *Operation Buccaneer*), targeting the most prolific groups would likely have the greatest utility. Operations Buccaneer, Fastlink, and Site Down seem to have done this by targeting the likes of DoD, MaGe, Fairlight, RISCiso, and so on. The next step to this strategy would be to target particular individuals who are more instrumental to the release process than others. According to the crime script, the most

necessary step within the script is the cracking step; crackers being difficult to replace and all other steps being dependent on it, as content cannot be copied without being cracked. If policing operations focused their efforts on targeting crackers of prominent groups within the warez scene, law enforcement efforts might result in greater disruption of these groups' piracy attempts, increasing the effort required by groups to release content.

The difficulty, however, in prescribing a policing strategy of targeting particular individuals within the group is locating them within these clandestine networks. I am aware of no published studies on release group network structures and predicting the optimal means of targeting these individuals is difficult. However, one issue that may aid law enforcement is the level of visibility: both the supply and distribution steps within the script are visible, to some degree, to law enforcement investigations. By targeting individuals engaging in these steps, and then surveilling them, one may be able to locate individuals instrumental to the release process, such as the cracker. Although law enforcement may have employed this apprehension strategy in the three above cited operations, the court data demonstrate that few of the individuals arrested had the primary role of cracker.[38]

In these three operations, almost one-third of the arrests reported in the court data were of individuals who performed an administrative function or

[38] "Judging from previous raids, it is clear that legal authorities will continue to use sites as a method of infiltrating a group. FBI agents do not know how to crack or supply, so they will go for the easy option and simply log everyone who enters their site" (Craig et al., 2005, p. 208). Operation Copy Cat (mentioned before) followed this format: agents created a fake site, and enticed groups to use it through a confidential informant.

operated a site. This may be because of a perception of higher culpability (or higher visibility, in the case of site operators) to law enforcement. It may also be that these individuals are more motivated than others: a case which could easily be argued for Hew Raymond Griffiths and the former leader of MaGe. However, despite these arrests the scene persists, and even in the absence of these administrative positions, content can still be cracked and released. Since group administrators remain motivated, and require a cracker, the apprehension of their group's cracker will force the group to seek new members, leaving an opportunity for law enforcement infiltration.

Thus, as it behooves law enforcement to target the most instrumental individuals within the release process, targeting the crackers within the most prominent groups may aid policing strategies through increasing the effort required by groups to release content. The cracking step is the most significant step, and as such, individuals who fulfil this role should be a higher priority for law enforcement than others within the group. Since these individuals operate clandestinely, law enforcement may surveil visible targets, such as those operating in the supply or distribution steps, to locate and apprehend crackers. This strategy may not require an increase in policing efforts—the same investigation strategy may be employed, just focusing on different targets – nor would it require an increase in the severity of punishment, as it has been suggested that many apprehended warez traders have a low probability of recidivism (DuBose, 2006). Thereby, this strategy is less likely to further strengthen the ideology held by some members in these groups.

## 5.2 Social Network Analysis: Concepts, *Key-Players*, and Sentence

The core question at the beginning of this thesis with respect to network data was whether or not there was a relation to sentence and centrality. Criminal enterprises may be similar to their licit counterparts in many ways (See Levitt & Dubner, 2005); however, they must remain clandestine in order to remain successful (Morselli, 2009; see also Bouchard, Beauregard, and Kalaczska, in press). Thereby, actors must maintain a balance between their efforts to maximize their criminal goals and their efforts to maximize their invisibility to threat: called the "security vs. efficiency trade-off" (Morselli, 2009, pp. 63-71). Baker and Faulkner (1993), for example, suggest that an actor's centrality is inversely related to the amount of security they are afforded. However, as a central position affords more access to information and control, the leaders of a criminal network must balance between concealment and coordination. In their study, they found that the probability of a guilty verdict along with the severity of sentence was related to an actor's centrality in the network (Id., p. 822).

Thus, it should be expected that the actors who receive the strictest sentences would be central, and actors who receive lighter sentences to be peripheral to the network. The results, partly, indicate this: as Veyna and Patel both occupied central positions in the network and received terms of imprisonment and high fines. However, Fish, another actor in the conspiracy, receives a severe sentence but only occupies a position of average centrality. As well, other actors in the network with similar centrality do not receive

imprisonment. This result may be related to 1) the method of aggregating and graphing the data, as well as 2) the nature of the criminal offence.

To the first, this network was constructed much like an ego network: CHUD and LAD were points of law enforcement surveillance and operated as 'dummy' sites that, along with an undercover informant by the name of "griffen", logged information about individuals who connected to them (See Indictment for USA v. Fish et al, Case Number 5:05CR00445. N.D. CA, 2008). In court documents, only in the cases of Fish, Veyna, Patel, and Lovell are specific communications between the undercover informant and the defendants mentioned. As three out of these four were sentenced to a term of imprisonment, this increased surveillance is most likely related to an increase in evidence that aggravates the sentence one would receive. Additionally, Fish was under surveillance for a longer period of time, beginning in Operation Fastlink (resulting in an additional, but separate court case from Copy Cat - See USA v. Fish, Case Number 5:05CR 06-00109. S.D. IA, 2008). However, it would seem that increased surveillance would also yield greater information about these individual's connections. In conjunction with this issue, Copy Cat was analyzed as a 2-mode network, and only connections between actors and servers were graphed. This is accurate, as the network represents relations between nodes of differing type, in this case individuals and servers. However, and to the second issue, in the course of the actual conspiracy, individuals can (and must) communicate and share resources with each other without using a server as a medium. This is significant, as actors who operate to increase the

effectiveness/rank of their respective sites and individual position must communicate with other **actors** for site affiliation and/or access. Thus, this disconnect between sentence and centrality may be related to the network's inability to include actor to actor communications. This is an issue that may be amended in future studies by analyzing these connections through 1-mode network, or possibly with a hybrid 2-mode that allows all connections, but interprets connections on the second mode to indicate a media of shared resource between all connected actors.

Another issue of merit concerning the Copy Cat network is the significance of *social capital* (Burt, 2005; Burt, 1992) on group success and network success. As sites are competing to receive exclusive new content (Craig et al., 2005; Lee, 2002), their opportunity to succeed is governed by their relations to groups that release new content. In other words, sites that affiliate with many different groups, that release different media or have access to different resources, will have more opportunity to receive new or exclusive content; thereby, they will be more likely to succeed relative to competitors who do not have these connections (See also Hulst, 2009; Lin, 2001; Portes, 1998).

Social Capital, then, can be interpreted as the measurable effect the inclusion of an actor filling a *structural hole* (Burt, 2005; Burt, 1992) has on the greater network and/or on the individual (Hulst, 2009; Lin, 2001; Portes, 1998). In the distribution architecture of the warez scene, the opportunity to acquire new content is related to one's connection to release groups, as they are the providers of new content. In the Copy Cat network, two individuals, Verhoeven

and Ghani. were identified as belonging to a release group called Wasted Time. As well, both actors were connected to a server of the same name that operated as the headquarter server for the group. The affiliation between the release group Wasted Time and CHUD is an example of *social capital* in action, as this relation supplied CHUD (and subsequently, all who connected to CHUD) with the resources that the release group acquired. Fascinatingly, the connections between the “Wasted Time” server and the CHUD server are weak-ties (Granovetter, 1973); in other words, other actors in the network who connect to peripheral servers are connected to either the peripheral server or to the CHUD server via a strong-link weight (i.e. Site Op/Admin access). However, in the case of “Wasted Time” no strong connection exists between actors who bridge this gap. With respect to individual success, Verhoeven is the only member suggested by court documents to have employed his position in the conspiracy for financial gain by selling pirated films obtained from the CHUD and Wasted Time servers (See USA v. Verhoeven, Case Number 5:06CR00247. N.D. CA, 2007). Verhoeven was suggested to have sold as many as 7,350 illicit DVDs during the course of the investigation, a retail value of $146,632. Under different circumstances, this would appear to be a significant result (i.e. an individual occupying a structural hole being the only one to gain financially, and substantially at that); however, because of the stigma of selling pirated material held in the warez scene (See Rehn, 2004; McCandless, 1997), this should be interpreted cautiously. Lastly, with respect to social capital, it should be noted that all four individuals who were deemed “brokers” by the FBI were located in

the “core” (See Table 4 for roles). The ascription of this role is independent of network characteristics, and is meant to reflect individuals who were responsible for negotiating deals between release groups and sites for affiliation and site access.

This is an interesting result, which future research should investigate. This process of brokerage seems to be the mechanism through which new and exclusive content is acquired for servers and through which groups gain access to top-sites and/or highly ranked servers. Thus brokerage in these networks offers a fascinating chance for examining criminal occupational prestige (See Matsueda et al., 1992), criminal achievement (See Bouchard & Nguyen 2010; See also Morselli & Royer, 2008), and adaptation in network architecture to achieve their goals. As groups and sites are competing for prestige (Craig et al., 2005; Goldman, 2005; Lee, 2002; McCandless, 1997), their opportunity to advance in this world is governed by their access to content; or if they are a provider, their access to high-ranking sites to receive content. Brokers facilitate this transaction, by seeking out groups that wish to supply content and connecting them to servers. Thus, it should be expected that brokers connecting suppliers of original content to the servers that require it must bridge structural holes (Burt, 2005; Burt, 1992). As well, in the absence of new content, these individuals must actively seek out new supply lines; thus amending their network architecture.

Finally, the actors in the “core” group, though, accounting for 50% of the network’s connectivity, did not have a significant difference in average fines

received. This result is noteworthy for two reasons. First, these actors were considered *key-players* (Borgatti, 2006) in the network, and in-line with Borgatti (2006), the identification of a key-player is related to one's objectives: fragmenting the network or being well connected to as many unique nodes as possible. To the first, the research would seek nodes with high betweenness, as removing these nodes would result in fragmenting the network. For the latter, one would seek nodes with a high degree, as surveilling these nodes would result in greater resource acquisition (Id.). Employing this concept to the Copy Cat network, there is little aid to fragment the network by removing actors. However, the results indicate that there are individuals with high degree centrality who may be useful to law enforcement to surveil, such as Veyna.

Second, one's network centrality is directly related to one's vulnerability (Baker & Faulkner, 1993), and thus, centrality scores can hint to network structure with respect to the location of leaders. For example, networks with a hierarchical organization often position leaders in the periphery to protect them; whereas networks without leaders, such as partnership models, centrality is more evenly distributed (Morselli, 2009, p. 60; Bouchard, 2010). This is significant because the Copy Cat network has as many as 8 actors in the "core", and 5 of these are Site Operators/Administrators. As these actors have similar centrality scores, and since, each actor is in control of each of his/her respective sites, this would hint at a more egalitarian network architecture. This corresponds with data from the crime-script and from previous literature (See McCandless, 1997) that suggests that there are mechanisms that promote contribution.

## 5.3 Limitations

This research suffers from several notable limitations regarding data, data acquisition, and the methods employed. First, all of the court case data used for this study are constructed by either the prosecution or defence. The prosecution, thus, is portraying a perspective of increased culpability on the part of the defence; while the defence is portraying a perspective of reduced culpability. In other words, Indictment Reports, Sentencing Memorandums, Plea Agreements, and Letters to the Court are all purposively biased towards adjusting guilt in one way or another. To minimize this limitation in this thesis, secondary sources were employed to ensure that the framing of the criminal behaviour on the part of the courts and the defendants was accurate. However, this limitation may have had an effect on the data by aggravating or reducing the culpability and severity of defendants in their participation in the overall conspiracy.

Second, in gathering data for this study, many cases had varying amounts of data, differing file names and formats, and differing definitions of role in the conspiracy. When cases were located via a DOJ Press Release or through a snow-ball effect, they were accessed with PACER. However, all cases had sealed documents, to which the researcher was not privy to view. The types and frequency of sealed documents varied from case to case, and jurisdiction to jurisdiction. For example, some cases allowed for defendants' Plea Agreement to be viewed; however, in almost every case tried in California, the plea agreements were sealed. Thus, some cases yielded large quantities of both qualitative and quantitative data; while others simply had a docket report and

judgement that yielded very little information on the facts of the case. In addition to this case format differed from jurisdiction to jurisdiction. For example, whereas one district would have Indictment Reports others would have Bills of Information. Last, there appeared to be a learning curve with respect to the court's construction and presentation of the conspiracy in court documents.[39] Thus, the operationalization of role and the presentation of individual behaviour changed over-time and from district to district in court documents. These differences in court data made analysing for qualitative information pertaining to individual participation in the conspiracy difficult.[40] Some of these limitations are unmitigated, as it is not possible to gather data on sealed cases; however, data between jurisdictions was managed as best possible to ensure consistency and secondary sources were used to help ensure proper and uniform operationalization of role. These limitations explain why the SNA was limited to a single set of defendants for which more (and more uniform) data was available.

Third, the construction of the Operation Copy Cat network suffers from two minor limitations; a small sample size and the inclusion of a server at two different points in time. The data used for the construction of the Copy Cat network was 32 cases out of 40 total convictions (US DOJ, May 14, 2008) (See Section 2.1.2 "Operation Copy Cat – SNA Data"), and out of hundreds of actors who accessed the sites but were not convicted. Second, the network was constructed with LAD and HOT as different servers; however, in reality, they are

[39] Examining patterns in this learning curve would be an excellent avenue for future research.

[40] Operation Copy Cat is the exception to this limitation, as almost all cases were tried in California. Thus, their access to files, formatting and naming of files, and definitions of actors in the conspiracy was almost all uniform.

the same server at two different points in time. This was done because court documents, specifically in Russell's case, suggested that Russell had two different connection types between LAD and HOT; a fact mirrored in Templeton's case (See USA v. Templeton et al, Case Number 5:06CR00054. N.D. CA, 2007 for both cases). To include this difference in connections, LAD and HOT were treated as different servers, and the network was constructed to include all links that had occurred during the time of surveillance. Thus, the graph is akin to a slow-shutter photograph, in that links that seem to occur simultaneously; however, in reality they may not be occurring at the same time.

# 6: CONCLUSION

> *"We will never stop piracy, never. We just have to make it as difficult and as tedious as possible, and we have to let people know there are consequences if they're caught"* (Dan Glickman, Chairman of the MPAA in King, 2007).

Copyright piracy is not a new phenomenon (See Alexander, 2007; Lessig, 2004; Lunney, 2001; Patterson, 1968), and as the world traverses further into the information age, the importance of protecting intellectual property (IP) will become greater. Mark Getty's statement that "[i]ntellectual property is the oil of the 21st century" (*The Economist*, March 2, 2000) is an understatement – IP is more like the vassalage of the 21st century. Companies like Nike and Tommy Hilfiger are no longer in the business of producing physical *things* – they are brand companies: industries that hold IP and outsource the production of physical media to the lowest bidder (Klein, 2000). Thus, these and other IP industries are in the business of controlling IP and depend on laws, such as copyright laws, to protect their system of ownership (*Intellectual property rights in an age of electronics and information*, 1986, p. 158-159) – and business is good. Though studies have been cited that show the harm digital piracy has had on the global market (Siwek, 2007; Tera Consulting, 2010), others have argued that the seemingly out-of-control expansion of piracy has been a constructed effort to put greater pressure on legislators to create stricter IP laws; thereby giving greater control to these industries (Yar, 2005).

It is an argument that makes some sense, given that copyright industries continued to be profitable even in the post-napster world; in fact, the employment of pay-per download music tools such as "iTunes" has allowed the industry to generate revenue from a previously illicit distribution media (Buskirk, Mar 12, 2008). Further to the point, it is difficult to argue for an increase in the policing or penalties associated with a *mala prohibita* offense like copyright, especially when their construction is shrouded in censorship and greed (See Alexander, 2007; Lessig, 2004; Lunney, 2001; Patterson, 1968). So why should individuals in release groups be subject to the left-hand of the law? Especially when so many people download at least some content illicitly, and release groups are, in some way, doing a public service – providing content without asking for compensation (Rehn, 2004; McCandless, 1997).

This is the question that I have struggled with while writing about these groups, and, to be sure, there is no simple answer. Lobbyists and lawmakers are not right in their increasing control of content. After the enactment of the *Sonny Bono  Copyright Term Extension Act*, copyrights are renewable for up to120 years;[41] which is odd considering the marketability and viability of content has decreased in lifespan in recent years. Who uses DOS applications or how many people line up to purchase 1920's vaudeville or ragtime phonographs? Yet, these may still be copyrighted and individuals who infringe the copyrights may be subject to penalties. On the other hand, copyrights have increased the quality of content and allowed authors to make a living off their efforts. The quote by Bill

[41] See the following, retrieved April 17 2011,  http://www.copyright.gov/legislation/s505.pdf

Gates at the beginning of this thesis demonstrates a number of issues pertaining to copyright, but Gates' point in the interview was that if software writers are compensated for their work the quality of software will go up – and it has.[42] Since the 1980s, computers have gone from a hobbyist's past time to an absolute necessity for life in the information age.

Although copyrights are not a completely just imposition by the State, they are a necessary evil to improve the quality of content and allow for authors to be compensated. As well, the law may not be in a condition that reflects the needs of the digital age but this issue may be resolved with time and with the influence of the disenfranchised in mass. With that, the activities of release groups do not reflect a desired shift in the distribution of content. Though they advocate for users to purchase content (See Appendix A), and perhaps even purchase it themselves, their activities entail, as well as promote, illicit distribution. These groups offer an interesting challenge to criminologists. They operate in organized groups (Urbas, 2006; Craig et al., 2005), in an odd ecology of motivations (Goode & Cruise, 2006; Goldman, 2005), possess diversity in roles between/within scenes (Cooper & Harrison, 2001), with an alternative scale of value for commercial content (Rehn, 2004; McCandless, 1997). These groups often involve individuals of varying ages, well outside the scope of traditional criminal involvement and are typically well educated and successful (DuBose, 2006).

[42] See http://features.slashdot.org/article.pl?sid=00/01/20/1316236&mode=thread, Retrieved on February 7, 2011.

This thesis aimed to examine release groups' *modus operandi* and motivations in the release process to discover opportunities to disrupt their efforts as well as to examine their network architecture and to determine whether a relation existed between sentence and centrality. To the first, a *crime-script* (Cornish, 1992) was constructed to map out each necessary step in the release process, including each step's objectives, role, role requirements, and visibility to law enforcement. This data yielded several results for future research in SCP of digital piracy as well as policy suggestions for law enforcement and industry to disrupt the activities of these groups. First, digital piracy is a difficult challenge for SCP as guardians and policy makers have little, or no, control over the environment in which the crime is committed , and as such, former SCP methods of controlling a criminal behaviour (Cornish and Clarke, 2003) may not be particularly apt. Second, *counterproductive prevention* (Wortley, 2003; Grabosky, 1996) operates in this aggregate; thus, methods to disrupt the activities of these groups must be mindful of these groups' motivations. Finally, with respect to policy suggestions for law enforcement and industry, the results indicate that industry may be able to increase the risk of releasing content relative to the release group motivations, while law enforcement may be able to increase the difficultly. By modifying DRM technologies to be more latent, while not increasing the difficultly of the protections employed, the value of cracking content will not increase while the risk associated with releasing ill-cracked content, damaging the groups prestige, will increase – making the crime riskier relative to the groups' goals. For law enforcement, the results indicate that the most optimal

step for disruption in the release process is the *cracking* step, as all other steps are futile without the content being cracked. Crackers are very skilled, and it has been suggested by secondary data, and anecdotally by court data, that crackers are fairly rare - making them difficult to replace. Thus, if law enforcement targets crackers in prominent release groups, those groups will be unable to release content, and since the top groups are responsible for cracking most illicit content (Goode, 2010; Urbas, 2006; CCIPS, *Operation Buccaneer*), the incapacitation of their crackers can be expected to have a significant preventive effect. As well, since these groups remain motivated, they will be forced to seek out new group members leaving them vulnerable for identification or infiltration.

Copyright infringement in the scene is inherently an organized crime wherein purposive groups act in concert. The “dark networks” (Raab & Milward, 2003) that these groups operate in can distribute content globally within minutes (Urbas, 2006; CCIPS, *Operation Buccaneer*), and all the while remain invisible to law enforcement, suggesting an incredible balance between security and efficiency (Morselli, 2009; See also Bouchard, Beauregard, and Kalaczska, in press). Thus, these networks seem particularly apt for Social Network Analysis, as concepts such as *social capital* (Burt, 2005; Lin, 2001; Portes, 1998; Burt, 1992) and *Key-players* (Borgatti, 2006) may offer explanations for criminal success, and expose methods to successfully infiltrate or disrupt these networks. It seems intuitive that individuals with greater culpability in an organized criminal venture would hold a more central position in the network. The data, retrieved from court case documents of convictions from Operation Copy Cat (US DOJ,

May 14, 2008), yielded mixed and somewhat hazy results in this regard. The analysis revealed that the network contained as many as eight key-players (out of 32) in the network, of whom, four received high fines relative to others and three received terms of imprisonment (the only three in the dataset). Ostensibly, the results would suggest a relation between sentence and centrality; but when compared to the non-key-players, no significant difference was found with respect to fine. As well, when the three imprisoned individuals were excluded from the dataset, no correlation was found between sentence (fine) and centrality (number of links). Thus, it seems that the three individuals who were imprisoned are driving the relation.

The Copy Cat network demonstrates the affiliation process through which servers receive and distribute new content. As well, out of the seven key-players listed in the “Core” group, four are ascribed the role of “brokers”. Brokers operate, as the name denotes, to negotiate deals between groups to affiliate them with sites; it is interesting to find them in highly central positions by degree but not by betweenness. Future research should examine this relationship, as it may yield valuable information into how these groups distribute content so efficiently, while maintaining a relatively low-density.

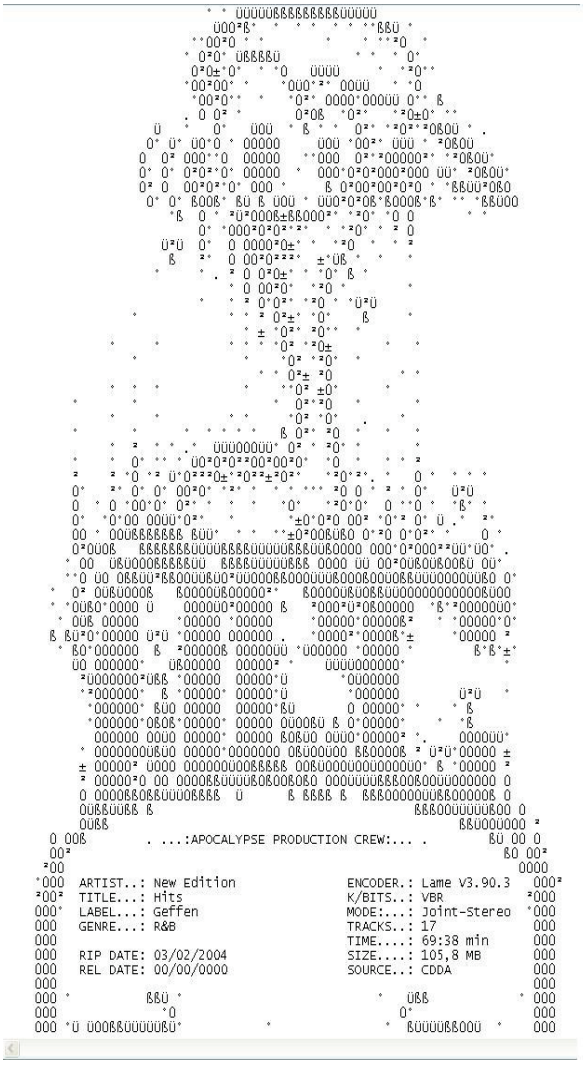
This study aimed to shed light on the issue of release groups, digital copyright infringement, and the illicit networks through which this content is supplied. Intellectual property as an intangible good driving the future’s economy and governing its social structure is a phenomenon worthy of future inquiry, as is the deviance associated with this construct. This study has lent suggestions to

the furtherance of control on the part of content owners, and whether this is a just imposition is still questionable. Nevertheless, despite studies, policing, or lobbying, the scene will go on: a modern Teumessian fox from the deep recesses of Internet.

# APPENDICES

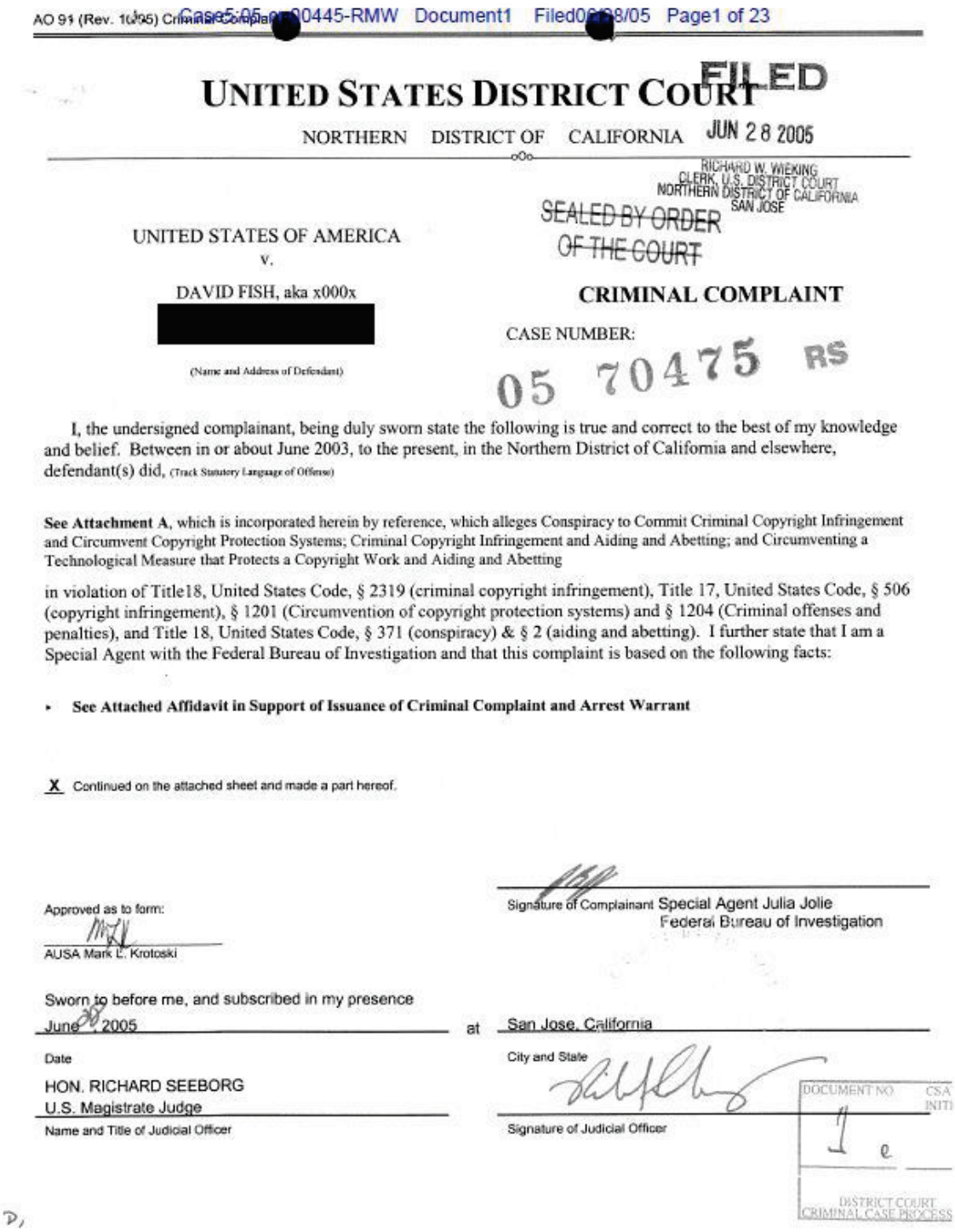
## Appendix A – aPC ‘nfo File

The following is a screenshot from the first and last portions of an Apocalypse Production Crew ‘nfo File.



## Appendix B – David Fish Indictment Report

The following is a screen-shot of a David Fish's Indictment Report. It includes pages 1, 4, and 5.



AO 91 (Rev. 10/95) Criminal Complaint Case5:05-mj-70445-RMW Document1 Filed06/28/05 Page1 of 23

# UNITED STATES DISTRICT COURT

FILED

NORTHERN DISTRICT OF CALIFORNIA

JUN 28 2005

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

SEALED BY ORDER OF THE COURT

UNITED STATES OF AMERICA
v.
DAVID FISH, aka x000x
[redacted]
(Name and Address of Defendant)

**CRIMINAL COMPLAINT**

CASE NUMBER:
05 70475 RS

I, the undersigned complainant, being duly sworn state the following is true and correct to the best of my knowledge and belief. Between in or about June 2003, to the present, in the Northern District of California and elsewhere, defendant(s) did, (Track Statutory Language of Offense)

**See Attachment A**, which is incorporated herein by reference, which alleges Conspiracy to Commit Criminal Copyright Infringement and Circumvent Copyright Protection Systems; Criminal Copyright Infringement and Aiding and Abetting; and Circumventing a Technological Measure that Protects a Copyright Work and Aiding and Abetting

in violation of Title18, United States Code, § 2319 (criminal copyright infringement), Title 17, United States Code, § 506 (copyright infringement), § 1201 (Circumvention of copyright protection systems) and § 1204 (Criminal offenses and penalties), and Title 18, United States Code, § 371 (conspiracy) & § 2 (aiding and abetting). I further state that I am a Special Agent with the Federal Bureau of Investigation and that this complaint is based on the following facts:

- **See Attached Affidavit in Support of Issuance of Criminal Complaint and Arrest Warrant**

X Continued on the attached sheet and made a part hereof.

Approved as to form:
AUSA Mark L. Krotoski

Signature of Complainant Special Agent Julia Jolie
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence
June 28, 2005 at San Jose, California
Date City and State

HON. RICHARD SEEBORG
U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

DOCUMENT NO. CSA INITI
1 e
DISTRICT COURT CRIMINAL CASE PROCESS

D,

*Aiding and Abetting*

9. Title 18, Unites States Code, Section 2(a) states, in pertinent part:

(a) whoever commits an offense against the United States or aids, abets, counsels, commands, induces of procures it commission, is punishable as a principal.

SOURCES OF INFORMATION USED IN THIS AFFIDAVIT

10. The facts set forth below are based upon my own personal observations, my own training and experience, reports, e-mails, on-line communications, other information provided to me by the undercover employee (UCE) conducting the undercover investigation, and from my conversations with other law enforcement agents knowledgeable in computer disciplines, and records I have obtained, and my conversations with other private companies who investigate copyright violations and have assisted in this investigation. This affidavit is intended to show that there is probable cause for the issuance of criminal complaints and arrest warrants, and does not purpose to set forth all of my knowledge of or investigation into this matter.

BACKGROUND CONCERNING WAREZ INVESTIGATION

11. In summary, this case involves an undercover investigation of organized groups of individuals and coconspirators – also known as "warez groups" or "warez coconspirators" – engaged in the illegal reproduction and distribution of copyright protected software over the Internet, including the illegal copying of movies, games, and software, in violation of federal copyright laws. The investigation stemmed from a Group II Undercover Operation (UCO) initiated in June 2003 by the Federal Bureau of Investigation (FBI), San Francisco Division and U.S. Attorney's Office, Northern District of California, San Jose Division. During the course of the investigation, investigators identified a number of large-scale software piracy groups, also known as "warez groups" or "warez coconspirators," engaged in the uploading, copying, duplication, reproduction, and distribution of copyright-protected computer software, games, and movies by way of the Internet, in violation of federal copyright and conspiracy laws.

Two Warez Sites: LAD and CHUD

12. During the undercover investigation, two warez sites were established in the Northern District of California, known as LAD and CHUD. The first was originally known as HOT and later named LAD. LAD was a smaller site (approximately 700 megabytes early on) and eventually became an archive site, holding older movies, games, and software (which is currently approximately 3.5 terabytes).[1] The second undercover warez site, CHUD, became an eleven terabyte site. In total, the two warez sites, combined with two servers (called VS and

[1] One terabyte equals approximately one trillion bytes, or approximately 700,000 3.5-inch floppy diskettes.

SNOWCAVE) which were provided by warez members, includes approximately 27 terabytes of pirated movies, games, and software, making this one of the largest undercover warez investigations. David Fish (aka x000x) and dact, among others, were instrumental in establishing CHUD. Acting as a Site Op, David Fish, aka x000x agreed to script the site and dact would broker introductions with top warez groups.

13. Numerous warez groups and coconspirators came to the undercover sites to store a large number of movies, games, and software that could be uploaded and downloaded by hundreds of individuals. Warez leaders operated and controlled the sites and established terms of membership and conditions governing and restricting access. Some warez members were compensated under a credit ratio (also known as "ratio access") of one upload amount equal to three downloads (i.e. one gigabyte/three gigabytes) as a means of private financial gain. In other words, an individual who uploaded one movie could download three movies. In addition, other members paid money to other individuals suppliers to obtain early releases of movies, games, or software. Under this large conspiracy, involving multiple individuals and warez groups, hundreds of individuals obtained free, unauthorized access to pirated movies, games, and software. Investigators discovered numerous pre-released movies, which were placed onto the undercover warez site before the scheduled DVD release to the general public.

Distinct Conspiracy Roles

14. The success of any warez conspiracy depends on the roles and contributions of many coconspirators. Based on information obtained in the investigation, and based on my training and experience, I have formed the opinion that the Warez scheme and conspiracy were committed by individuals having distinct roles. While some members may handle multiple roles, other members may only be responsible for one role. Investigators learned that all members hold some responsibility in keeping their warez group and site up and running. In this investigation, the distinct roles have included but were not limited to: **Founders or Leaders** (originally formed the warez group and look for additional members who could provide something of value to the warez group); **Scriptors** (responsible for creating, programing, building the warez site); **Site Operators** (SiteOps) (site manager holding root access to the warez site); **Suppliers** (providing an unauthorized copyrighted movie, game or software); **Cammer** (uses an audiovisual recording device (such as a camcorder) to make an unauthorized copy of a motion picture or other audiovisual work that is protected by the copyright laws); **Equipment Suppliers** (provides hardware (such as hard drives, computer parts, and computer servers) to the warez site); **Brokers** (found groups to participate on the warez site); **Couriers** (charged with gathering computer software programs, games, and movies and uploading them to the warez site); **Encoder** (sometimes referred to as "ripper" and "cracker", is responsible for circumventing the technological measures and protections of copyrighted works on the DVDs to prevent unauthorized access and copying); **Leech** (a member based on friendship, not group affiliation with leech access to the movies, games, and software on the warez site); **Ratio** (a member who was required to fulfill a contribution requirement in order to download copyright works; e.g., the most common ratio is one upload to three downloads, permitting the warez member to download

# REFERENCE LIST

A&M RECORDS, INC. v. Napster, Inc., 284 F. 3d 1091 – (Court of Appeals, 9th Circuit 2002, Retrieved via Google Scholar)

Alexander, I. (2007). Criminalising Copyright: A Story of Publishers, Pirates, and Pieces of Eight. *Cambridge Law Journal*, *66*(3), 625-656. doi: 10.1017/S0008197307000694

Baker, W. E., & Faulkner, R. R. (1993). The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment. *American Sociological Review*, *58*, 837-860. Retrieved December 14, 2010, from http://www.jstor.org/stable/2095954

BanDiDo [Hew Raymond Griffiths]. (n.d.). Interview with BandDiDo/DoD & RiSC [Interview by BiXen]. Retrieved November 1, 2010, from http://www.defacto2.net/legacy/apollo-x/bandido.htm

Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, J. (2007). Script Analysis of the Hunting Process of Serial Sex Offenders. *Criminal Justice and Behavior*, *34*(8), 1069-1084. doi: 10.1177/0093854807300851

Blood and oil. (2000, March 2). *The Economist*. Retrieved June 3, 2010, from http://www.economist.com/businessfinance/displaystory.cfm?story_id=E1_NRRVTV&source=login_payBarrier

Borgatti, S. (1997). Network analysis of 2-mode data. *Social Networks*, *19*(3), 243-269. doi: 10.1016/S0378-8733(96)00301-2

Borgatti, S. P. (2006). Identifying sets of key players in a social network. *Computational and Mathematical Organization Theory*, *12*(1), 21-34. doi: 10.1007/s10588-006-7084-x

Borgatti, S. P., & Everett, M. G. (1997). Network Analysis of two-mode data. *Social Networks*, *19*, 243-269. Retrieved April 9, 2010, from http://www.steveborgatti.com/papers/borgatti%20-%20network%20analysis%20of%202-mode%20data.pdf

Bouchard, M. (2010). Chain reaction: Identifying the key players in drug distribution networks. Paper presented at the annual conference of the *American Society of Criminology*, San Francisco, November 2010

Bouchard, M., Beauregard, E., Kalacska, M. (in press). Journey to grow-op: Linking process to outcome in criminal site selection. *Journal of Research in Crime and Delinquency.*

Bouchard, M., & Nguyen, H. (2010). Is It Who You Know, or How Many That Counts? Criminal Networks and Cost Avoidance in a Sample of Young Offenders. *Justice Quarterly*, *27*(1), 130-158. doi: 10.1080/07418820802593386

Borgatti, S.P. [forthcoming]. 2-Mode Concepts in Social Network Analysis. *Encyclopedia of Complexity and System Science*. Retrieved December 1, 2010, from http://www.steveborgatti.com/publications.htm

Brantingham, P. J., & Brantingham, P. L. (1981). *Environmental criminology*. Beverly Hills, CA: Sage Publications.

Bullock, K., Clarke, R. V., & Tilley, N. (2010). Introduction (K. Bullock, Ed.). In R. V. Clarke & N. Tilley (Eds.), *Situational Prevention of Organised Crimes* (pp. 1-16). Portland, O: Willan Publishing.

Buskirk, E. V. (2008, March 12). Apple Apparently Turned $570 Million Profit from ITunes Last Year. *Wired*. Retrieved April 17, 2011, from http://www.wired.com/listening_post/2008/03/apple-apparentl/

Burt, R. S. (1995). *Structural holes: the social structure of competition.* Cambridge, MA: Harvard University Press. Retrieved August 2, 2010, from Google Books.

Burt, R. S. (1997). A note on social capital and network content. *Social Networks*, *19*(4), 355-373. doi: 10.1016/S0378-8733(97)00003-8

Burt, R. S. (2005). *Brokerage and closure an introduction to social capital* [Ebrary Reader]. Oxford: Oxford University Press.

CCIPS. (n.d.). Illegal “warez” organizations and Internet piracy. *Operation Buccaneer*. Retrieved November 08, 2010, from http://www.justice.gov/criminal/cybercrime/ob/OBorg&pr.htm

Cesarini, L. M., & Cesarini, P. (2008). From Jefferson to Metallica to your Campus: Copyright Issues in Student Peer-to-Peer File Sharing. *Journal of Technology Studies*, *36*(1), 45-54. Retrieved August 2, 2010, from http://scholar.lib.vt.edu/ejournals/JOTS/v34/v34n1/cesarini.html

Clarke, R. V. (1980). "Situational" Crime Prevention: Theory and Practice. *British Journal of Criminology*, *20*(2), 136-147. Retrieved September 18, 2010, from http://bjc.oxfordjournals.org.proxy.lib.sfu.ca/content/20/2.toc

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, *19*, 91-150. Retrieved September 15, 2010, from JSTOR.

Cohen, L. (1981). Modeling crime trends: A criminal opportunity perspective. *Journal of Research in Crime and Delinquency*, *18*(1), 138-164. doi: 10.1177/002242788101800109

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588-608. Retrieved September 18, 2010, from JSTOR.

Cooper, J., & Harrison, D. M. (2001). The social organization of audio piracy on the Internet. *Media, Culture & Society*, *23*(1), 71-89. doi: 10.1177/016344301023001004

Cornish, D. B., Clarke, R. V., & Cornish, D. B. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational. In M. J. Smith (Ed.), *Theory for Practice in Situational Crime Prevention* (Vol. 16, Crime Prevention Studies, pp. 41-96). Monsey, NY: Criminal Justice Press.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime prevention studies* (Vol. 3, pp. 151-196). Monsey, NY: Criminal Justice Press.

Craig, P., & Honick, R. (2005). *Software piracy exposed* (M. Burnett, Ed.). Rockland, Mass.: Syngress Pub.

David, M., & Kirkhope, J. (2004). New Digital Technologies: Privacy/Property, Globalization, and Law. *Perspectives on Global Development and Technology*, *3*(4), 437-449. doi: 10.1163/1569150042728884

Davis, A., Gardner, B. B., Gardner, M. R., & Silver, J. W. (1941). *Deep South a social anthropological study of caste and class*. Chicago, IL: University of Chicago Press.

Dombrowski, K., Curtis, R., & Friedman, S. R. (2007, June 16). *Injecting Drug User Network Topologies and Infectious Disease Transmission: Suggestive Finding*. Retrieved December 20, 2010, from http://www.syrondesign.com/snrg/index_files/Page682.htm

DuBose, M. M. (2006). Criminal Enforcement of Intellectual Property Laws in the Twenty-First Century. *The Columbia Journal of Law & the Arts*, *29*, 481-496. Retrieved September 1, 2010, from LexisNexis Academic.

Fox Film Corp. v. Doyal, 286 U.S. 123 (May 16, 1932) (Google Scholar, Dist. file).

Frank, R., Westlake, B., Bouchard, M. (2010). The Structure and Content of Online Child Exploitation Networks, *Proc. 16th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD '2010)*, Washington D.C., USA.

Gallupe, O., Bouchard, M. (2010). Mapping the middle: A Social Network Analysis of middle market distributors. *American Society of Criminology*, San Francisco, November 2010.

Gardner, H. (1985). *The mind's new science: a history of the cognitive revolution*. New York, NY: Basic Books.

Gardner, E. (2010, May 11). 'Hurt Locker' lawsuit target pirates. *The Hollywood Reporter*. Retrieved July 13, 2010, from http://www.hollywoodreporter.com/hr/content_display/film/news/e3ia3e81d4dc935f423aef090323c40270a

Goldman, E. (2003). A Road to No Warez: The No Electronic Theft Act and Criminal Copyright Infringement. *Oregon Law Review*, *82*, 369-432. Retrieved July 18, 2010, from LexisNexis.

Goldman, E. (2004) Warez Trading and Criminal Copyright Infringement. Available at SSRN: http://ssrn.com/abstract=487163 or doi:10.2139/ssrn.487163

Goldman, E. (2005). The Challenges of Regulating Warez Trading. *Social Science Computer Review*, *23*, 24-28. doi: 10.1177/0894439304271531

Goode, S. (2010). Exploring the supply of pirate software for mobile devices: An analysis of software types and piracy groups. *Information Management & Computer Security*, *18*(4), 204-225. doi: 10.1108/09685221011079171

Goode, S., & Cruise, S. (2006). What Motivates Software Crackers? *Journal of Business Ethics*, *65*(2), 173-201. doi: 10.1007/s10551-005-4709-9

Grabosky, P. N. (1996). Unintended Consequences of Crime Prevention. *Crime Prevention Studies*, *5*, 25. Retrieved November 24, 2010, from http://www.popcenter.org/library/crimeprevention/volume_05/

Granovetter, M. S. (1973). The Strength of Weak Ties. *American Journal of Sociology*, *78*(6), 1360-1380. doi: 10.1086/225469

Gunter, W. D. (2008). Piracy on the High Speeds: A Test of Social Learning Theory on Digital Piracy among College Students. *International Journal of Criminal Justice Sciences*, *3*(1), 54-68. Retrieved July 20, 2010, from http://www.sascv.org/ijcjs/gunterijcjsjan2008.pdf

Hanneman, R. A., & Riddle, M. (2005). *Introduction to social network methods*. Retrieved April 9, 2010, from http://www.faculty.ucr.edu/~hanneman/nettext/

Healy, C., & Liddell, C. (2007, July 20). Microsoft F4Q07 (Qtr End 6/30/07) Earnings Call Transcript. *Seeking Alpha*. Retrieved July 10, 2010, from http://seekingalpha.com/article/41697-microsoft-f4q07-qtr-end-6-30-07-earnings-call-transcript

Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An Application of Deterrence Theory to Software Piracy. *JCJPC*, *12*(3), 166-184. Retrieved November 8, 2010, from http://www.albany.edu/scj/jcjpc/vol12.html#vol12is3

Hinds, J. (2010, March 3). Army bomb expert claims 'Hurt Locker' based on him. *USATODAY.com*. Retrieved July 14, 2010, from http://www.usatoday.com/life/movies/news/2010-03-03-hurt-locker-lawsuit_N.htm

Hinduja, S. (2006). *Music piracy and crime theory*. New York, NY: LFB Scholarly Pub. LLC.

Holsapple, C. W., Iyengar, D., Jin, H., & Rao, S. (2008). Parameters for Software Piracy Research. *The Information Society*, *24*(4), 199-218. doi: 10.1080/01972240802189468

*Home Recording of Copyrighted Works: Hearings Before the Subcommittee on Courts, Civil Liberties ,and the Administration of Justice of the Committee on the Judiciary House of Representatives*. 97th Cong., 2nd Sess. (1982) (Testimony of Jack Valenti): Retrieved on August 2, 2010 from http://cryptome.org/hrcw-hear.htm

Howe, J. (2005, January). The Shadow Internet. *Wired*, *13.01*. Retrieved November 8, 2010, from http://www.wired.com/wired/archive/13.01/topsite.html

Hulst, R. C. (2009). Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends in Organized Crime*, *12*, 101-121. doi: 10.1007/s12117-008-9057

Hunter, P. (2004). Combating video piracy. *Network Security*, *2004*(2), 18-19. doi: 10.1016/S1353-4858(04)00039-X

*IMPLEMENTATION OF THE "NET" ACT AND ENFORCEMENT AGAINST INTERNET PIRACY*:*HEARING BEFORE THE SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY OF THE COMMITTEE ON THE JUDICIARY, HOUSE OF REPRESENTATIVES*. 106 Cong., 1st Sess. (2000)

Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: an empirical examination. *Deviant Behavior*, *29*, 344-366. doi: 10.1080/01639620701588131

*Intellectual property rights in an age of electronics and information.* (1986). Washington, D.C.: Congress of the U.S., Office of Technology Assessment.

Internet World Statistics. (2010). United States Internet Usage. *Internet Usage World Stats - Internet and Population Statistics*. Retrieved September 17, 2010, from http://www.internetworldstats.com/am/us.htm

Jeffery, C. R. (1977). *Crime prevention through environmental design*. Beverly Hills, CA: Sage Publications.

King, J. J. (Director). (2007). *Steal this Film II* [Motion picture]. League of Noble Peers. Retrieved April 1, 2010, from http://www.stealthisfilm.com/Part2/index.php

Klein, N. (2001). *No logo*. London, UK: Flamingo.

Konstantakis, N. I., Palaigeorgiou, G. E., Siozos, P. D., & Tsoukalas, I. A. (2009). What do computer science students think about software piracy? *Behaviour & Information Technology*, *29*(3), 277-285. doi: 10.1080/01449290902765076

Kornblum, J. (1997, January 28). FBI hunts software pirates. *CNET News*. Retrieved December 12, 2010, from http://news.cnet.com/FBI-hunts-software-pirates/2100-1023_3-265813.html

Kooi, B. R. (2010). *Theft of Scrap Metal* (Guide No. 58). Retrieved January 25, 2011, from http://www.popcenter.org/problems/metal_theft/

Kot, G. (2009). *Ripped: how the wired generation revolutionized music*. New York, NY: Scribner.

Lacoste, J., & Tremblay, P. (2003). Crime and Innovation: A Script Analysis of Patterns in Check Forgery. *Crime Prevention Studies*, *16*, 169-196.

Lee, J. (2002, July 11). Pirates on the Web, Spoils on the Street. *New York Times*. Retrieved October 21, 2010, from http://www.nytimes.com/2002/07/11/technology/pirates-on-the-web-spoils-on-the-street.html

Lessig, L. (2004). *Free culture: how big media uses technology and the law to lock down culture and control creativity*. New York, NY: Penguin Press.

Levitt, S. D., & Dubner, S. J. (2005). *Freakonomics: a rogue economist explores the hidden side of everything*. New York, NY: William Morrow.

Leyshon, A., Webb, P., French, S., Thrift, N., & Crewe, L. (2005). On the reproduction of the musical economy after the Intern. *Media, Culture & Society*, *27*, 177-209. doi: 10.1177/0163443705050468

Lin, N. (2001). *Social capital: a theory of social structure and action*. Cambridge, UK: Cambridge University Press.

Lunney, G. S. (2001). The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act. *Virgina Law Review*, *87*(5), 813-920. Retrieved June 3, 2010, from JSTOR.

Matsueda, R. L., Gartner, R., Pillavin, I., & Polakowski, M. (1992). The Prestige of Criminal and Conventional Occupations: A Subcultural Model of Criminal

Activity. *American Sociological Review*, *57*(6), 752-770. Retrieved June 8, 2008, from JSTOR.

McCandless, D. (1997, April). Warez Wars. *Wired*, *5.04*. Retrieved June 3, 2010, from http://www.wired.com/wired/archive/5.04/ff_warez.html

Moreno, J. L. (1937). Sociometry in Relation to Other Social Sciences. *Sociometry*, *1*, 206-219. Retrieved December 20, 2010, from JSTOR.

Morselli, C. (2009). *Inside Criminal Networks*. New York: Springer.

Morselli, C., & Roy, J. (2008). Brokerage Qualifications in Ringing Operations. *Criminology*, *46*(1), 71-98. Retrieved July 29, 2010, from Wiley-Blackwell.

Morselli, C., & Royer, M. (2008). Criminal Mobility and Criminal Achievement. *Journal of Research in Crime and Delinquency*, *45*(1), 4-21. doi: 10.1177/0022427807309630

Patterson, L. R. (1968). *Copyright in historical perspective.* Nashville, TN: Vanderbilt University Press

Pickerill, A., Klein, J., & Oberdorf, T. (2008, February 4). Getty Images Q4 2007 Earnings Call Transcript. *Seeking Alpha*. Retrieved July 10, 2010, from http://seekingalpha.com/article/62973-getty-images-q4-2007-earnings-call-transcript

Portes, A. (1998). Social Capital: Its Origins and Applications in Modern Sociology. *Annual Review of Sociology*, *24*(1), 1-24. doi: 10.1146/annurev.soc.24.1.1

Pouwelse, J., Garbacki, P., Epema, D., & Sips, H. (2008). Pirates and Samaritans: A decade of measurements on peer production and their implications for net neutrality and copyright. *Telecommunications Policy*, *32*(11), 701-712. doi: 10.1016/j.telpol.2008.09.004

Raab, J., & Milward, B. (2003). Dark Networks as Problems. *J Public Adm Res Theory*, *13*(4), 413-43. doi: 10.1093/jpart/mug029

Rehn, A. (2004). The politics of contraband The honor economies of the warez scene. *Journal of Socio-Economics*, *33*(3), 359-374. doi: 10.1016/j.socec.2003.12.027

RIAA. (2005). *2005 Commercial Piracy Report* [Press release]. Retrieved July 12, 2010, from http://www.riaa.com/physicalpiracy.php?content_selector=piracy_annual_comm_reports

Sandoval, G. (2010, July 13). A copyright ruling no one can like. *Technology News - CNET News*. Retrieved July 14, 2010, from http://news.cnet.com/8301-31001_3-20010428-261.html

Schank, R. C., & Abelson, R. P. (1977). *Scripts, plans, goals, and understanding: an inquiry into human knowledge structures*. Hillsdale, NJ: L. Erlbaum Associates.

Scott, J. (1988). Social Network Analysis. *Sociology*, *22*(1), 109-127. doi: 10.1177/0038038588022001007

Scott, J. (2010). *You're Stealing it Wrong: 30 Years of Inter-Pirate Battles*. Speech presented at Defcon 18 in NV, Las Vegas. Retrieved February 13, 2011, from http://vimeo.com/15400820

Scott, J. (Director). (2005). *BBS: The Documentary* [Motion picture]. Retrieved September 17, 2010, from http://www.archive.org/details/BBS.The.Documentary

Siwek, S. E. (2007). *The True Cost of Copyright Industry Piracy to the U.S. Economy* (Rep. No. 189). Retrieved June 3, 2010, from http://www.ipi.org/

Siwek, S. E. (2009). *Copyright industries in the U.S. Economy: The 2003 - 2007 report* (International intellectual property alliance). Retrieved August 3, 2010, from http://www.iipa.com/

Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (January 17, 1984) (Google, Dist. file).

Stephenson, P. (2005). Managing Intellectual Property. *Computer Fraud & Security*, *2005*(4), 14-16. doi: 10.1016/S1361-3723(05)70200-1

TERA Consultants. (2010). *Building a digital Economy : The Importance of Saving Jobs In The EU'S creative Industries* (Study). Retrieved August 3, 2010, from http://www.teraconsultants.fr/fr/Accueil.html

TGSC Editor. (2010, June 19). Issue 43. *The Game Scene Charts*. Retrieved September 18, 2010, from http://www.defacto2.net/

Tichy, N. M., Tushman, M. L., & Fombrun, C. (1979). Social Network Analysis for Organizations. *The Academy of Management Review*, *4*(4), 507-519. Retrieved December 14, 2010, from http://www.jstor.org/stable/257851

United States v. LaMacchia, 871 F. Supp. 535 (United States District Court, D. Massachusetts December 28, 1994) (Google Scholar, Dist. file).

United States v. Paramount Pictures, Inc., 334 U.S. 131 (May 3, 1948) (Google Scholar, Dist. file).

Urbas, G. (2006). Cross-national investigation and prosecution of intellectual property crimes: the example of "Operation Buccaneer" *Crime, Law, and Social Change*, *46*, 207-221. doi: 10.1007/s10611-007-9060-x

US DOJ. (2001, December 11). *Federal Law Enforcement Targets International Internet Piracy Syndicates* [Press release]. Retrieved April 12, 2010, from http://www.justice.gov/opa/pr/2001/December/01_crm_643.htm

US DOJ. (2004, April 22). *Justice Department Announces International Internet Piracy Sweep* [Press release]. Retrieved April 11, 2010, from http://www.justice.gov/criminal/cybercrime/fastlink.htm

US DOJ. (2005, June 30). *Justice Department Announces International Internet Piracy Sweep* [Press release]. Retrieved September 19, 2010, from http://www.justice.gov/opa/pr/2005/June/05_crm_353.htm

US DOJ. (2006, April 6). *Five Additional Defendants Charged with Violating Copyright Laws as Part of Operation Copycat* [Press release]. Retrieved December 17, 2010, from http://www.justice.gov/criminal/cybercrime/soaresCharge.htm

US DOJ. (2007, October 26). *Defendant Sentenced to 12 Months in Prison as part of Internet Piracy Crackdown* [Press release]. Retrieved November 24, 2010, from http://www.justice.gov/criminal/cybercrime/emchSent.pdf

US DOJ. (2008, May 14). *Two Site Operators Receive Prison Terms for Criminal Copyright Infringement* [Press release]. Retrieved April 17, 2011, from http://www.justice.gov/usao/can/press/2008/2008_05_14_patel.veyna.sentenced.press.html

US DOJ. (2009, September 9). *Four Member of Alleged Internet Music Piracy Group Charged with Copyright Infringement Conspiracy* [Press release]. Retrieved November 24, 2010, from http://www.justice.gov/criminal/cybercrime/cassimPlea.pdf

Wang, W. (2004). *Steal this file sharing book: what they won't tell you about file sharing*. San Francisco, CA: No Starch Press.

Wasserman, S., & Faust, K. (1994). *Social network analysis: methods and applications*. Cambridge, UK: Cambridge University Press. Retrieved December 15, 2010, from GoogleBooks.

Williams, F. P., & McShane, M. D. (2004). *Criminological Theory* (4th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, *16*(4), 304-324. doi: 10.1016/j.infoandorg.2006.08.001

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403-414. doi: 10.1057/palgrave.ejis.3000592

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133-137. doi: 10.1145/1562164.1562198

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal*, 14(4), 63-82

Wortley, R. (2003). Situational Crime Prevention and Prison Control: Lessons for Each Other. *Crime Prevention Studies*, *16*, 97.

Yar, M. (2005). The global 'epidemic' of movie 'piracy': Crime-wave or social construction? *Media, Culture & Society*, *27*(5), 677-696. doi: 10.1177/0163443705055723