Piracy in cyber space: consumer complicity, pirates and enterprise enforcement

Peggy E. Chaudhry a*, Sohail S. Chaudhry a, Stephen A. Stumpf a and Hasshi Sudler b

aDepartment of Management and Operations/International Business, Villanova University, Villanova School of Business, 800 Lancaster Avenue, Villanova 19085, USA; bInternet Think Tank Inc, San Francisco, USA

(Received 4 May 2010; final version received 15 September 2010)

This article presents an overview of the growth of internet piracy in the global marketplace. The ethical perceptions (or lack of) of the younger generation is addressed, in terms of their willingness to consume counterfeit goods on the web. Firms face the task of educating the consumer that downloading music, software, movies and the like, without compensation, is unethical. This awareness is critical for decreasing the demand for counterfeit goods in the virtual marketplace, where a consumer can exhibit a rogue behaviour with a limited fear of prosecution. We address the pyramid of internet piracy, which encompasses sophisticated suppliers/facilitators, such as the Warez group. Recent sting operations, such as Operation Buccaneer, are also depicted to highlight successful tactical manoeuvres of enforcement agencies. An overview of the Digital Millennium Copyright Act and the No Electronic Theft Act is included to debate the controversy surrounding this legislation. A discussion of enterprise enforcement mechanisms and novel anti-piracy technology for cyberspace is provided to reveal some of the tools used to fight the pirates, such as innovations in digital watermarking and NEC's recently announced video content identification technology. Enterprise information systems and its interdependence on the internet are also demanding new technologies that enable internet investigators to rapidly search, verify and potentially remove pirated content using web services. The quality of service of web services designed to efficiently detect pirated content is a growing consideration for new anti-piracy technology.

Keywords: anti-piracy technology; internet piracy; cybercrime; consumer complicity; Warez; Digital Millennium Copyright Act; net act; watermarking

1. Introduction

Business managers need to monitor several trends relating to the protection of a firm’s intellectual property on the internet. On the one hand, the internet has presented many companies with the opportunity to explore markets, gather information and sell through the web. On the other hand, this virtual marketplace has been a way for unscrupulous players in an intricate game of cyber crime to infringe a company’s intellectual property rights and channel illicit goods by way of...
the pyramid of internet piracy. The overall positive growth in global technology, such as internet penetration rates, has also paradoxically created a lucrative distribution channel for the counterfeit trade. Moreover, the augmentation of legislation designed to curb internet piracy, such as the Digital Millennium Copyright Act (DMCA), has ignited controversy surrounding its enforcement, especially the ‘safe harbour’ provisions. The recent divergent outcomes of the litigation filed against EBay for selling counterfeit goods at its internet auction site by both Tiffany’s and Louis Vuitton are testimony to the dilemma-facing firms that goods are sold by way of the internet. In July 2008, after 4 years in the US court system, a US judge declined the liability of EBay regarding counterfeit jewellery sold at its site. However, in June 2008, a French court awarded Louis Vuitton €38 million as compensation from EBay for failure to prevent the sale of its luxury goods on this internet auction site (Waters 2008; Waters and Tait 2008).

Litigation and other law enforcement methods constitute one approach to dealing with internet piracy. Recently, however, enterprises and internet investigators are placing a greater emphasis on anti-piracy technology. Advancements in information hiding techniques, such as digital watermarking and digital video fingerprinting, are making it easier to track digital content back to the content owner. Other technologies are being introduced to prevent piracy of web applications and brand goods over the internet.

2. Turbulent virtual waters: anticipated growth in a sea of piracy

Passariello, in her article in the Wall Street Journal, reports that the internet is now the third largest market for the sale and distribution of counterfeits, behind China and Italy, and that companies such as Rolex and Tiffany & Co. have sued EBay to promote more responsible selling at its internet site (Passariello 2004). The counterfeiters have attracted the attention of policymakers, as the sale of fake pharmaceuticals, baby formula, airplane parts, and the like stimulates health and safety concerns. Carol Matlock of Business Week, in her personal interview with Jean-René Fortou, former head of the International Chamber of Commerce, asked what attributed to the dramatic increase in government policy makers’ attention to curbing counterfeit trade (Matlock 2005). In response, Mr. Fortou claims that recent government policy changes are resulting from the rampant growth and scale of the piracy problem, especially since the illicit trade is related to organised crime. Mr. Fortou cites the alarming increase in counterfeit goods that potentially threaten public health and safety, resulting in a broader perception of the scope of a problem which was initially associated primarily with the luxury goods sector.

Buzzeo, in his work on counterfeit pharmaceuticals, reports the success of the US Drug Enforcement Administration sting operation, Operation Cyber Chase, in shutting down 200 illegal e-pharmacies that were associated with a sophisticated black market industry. Overall, the increase of fake drugs as a dimension of the counterfeit market is a result of large profit potential, anonymous distribution channels by way of the internet, and price sensitive consumer demand. According to the Food and Drug Administration (FDA) official William Hubbard, ‘some experts are telling us it is more lucrative to sell a counterfeit drug than it is to sell a narcotic such as heroin’ (Buzzeo 2005, p. A20).

The problem of counterfeit trade is growing and the seizure statistics of physical goods provided by the US Customs and Border Protection show a change in total
number of seizures in 2005 at 8022 (estimated US domestic value of $93,234,510) to 2009 at 14,841 (estimated US domestic value of $260,697,937) in this 5-year time frame (Intellectual Property Rights, US Customs and Border Protection 2009, p. 6). However, even with this significant growth in seizure data, Chaudhry and Zimmerman (2009) argue that these figures represent just a fraction of the increased volume of counterfeit trade in physical goods since it is estimated that the US Customs and Border Protection authorities search less than 5% of all goods entering the USA. However, these data collected by the US Customs and Border Protection represent physical goods seized at some port of entry into the USA and the problem of counterfeit trade in a virtual marketplace, such as via internet auctions on e-Bay or peer-to-peer downloading, is an activity that many industry associations claim is growing, especially with internet penetration expanding in many global markets, yet the illicit trade in cyber space is difficult to measure. The Internet World Stats (IWS 2008) estimates there are 1,319,872,102 internet consumers in the world (www.internetworldstats.com). The IWS estimates that 676.6 million consumers are located in markets (43 countries) with greater than 50% internet penetration.

The Business Software Alliance (BSA) claims that the demand for counterfeit computer software will go up or down as a function of consumer education, law enforcement, the number of new users coming into the market, the ease of access to pirated software and certain external factors, such as political conditions. The BSA also notes elements such as culture, institutional effectiveness and even geography as having an impact on the abilities of countries to reduce piracy. Overall, the BSA forecasts that the increased use of the internet, the proliferation of peer-to-peer networks, and the growth of broadband access will increase software piracy rates, especially in emerging markets such as China, India and Russia (Fourth Annual BSA, 2007).

As shown in Figure 1, the Motion Picture Association of America (MPAA) portrays the pyramid of internet piracy to provide better insight on how suppliers at the top of the pyramid (e.g. release groups, such as Warez) use top sites to start the chain of supply/demand for fake movies on the internet. In a recent press release of the MPAA, ‘The Impact of Piracy on Avatar,’ the trade association illustrates the pyramid of internet piracy to highlight that once the movie, Avatar, had been released on 18 December 2009 in movie theatres it took less than 24 h for the suppliers in this pyramid (refer to Figure 1) to place the movie on the internet for illegal sites, such as Avatar.2009.TELESYNC.XviD-Camelot. Within 3 months, at just this one illegal torrent site, the MPAA estimated that it had lost $5000 in ticket sales due to illegal downloads in this short-time frame (‘The Impact of Piracy on Avatar,’ 2009).

3. Creating the supply and demand for virtual fake goods: the internet piracy pyramid

The virtual marketplace via internet activity poses an even more lucrative distribution channel for fake goods, a concern which is coupled with the aforementioned awareness that the internet penetration in markets across the world is rapidly growing. Kupferschmid (2003) described the main types of internet piracy as auction piracy (e.g. EBay), FTP piracy (e.g. hijacking a corporations FTP site to place illegal files in its directories), peer-to-peer piracy (e.g. the infamous Napster case), instant messaging (e.g. sharing illegal software via buddy lists) and internet
relay chat (IRC) (which allows access by many users to large files in a main location with security of anonymous postings).

3.1. The Warez scene

Warez is a generic term used to describe software that has been stripped of its copyright protection and placed on the internet for downloading without a financial compensation. Members of this illicit group can be the first-providers – that is, the original source for the illegal trading and online distribution of pirated works. Once a release group prepares a stolen work for distribution, the material is distributed in minutes to secure, top-level servers and made available to a select clientele. From there, within a matter of hours, the pirated works are illegally distributed throughout the world, ending up on public channels on IRC and peer-to-peer file sharing networks accessible to anyone with internet capability. Since releases are duplicated, renamed and then re-uploaded to different sites, it can become impossible to trace the original file. Release groups are hierarchical, highly-structured organisations with leadership positions that control day-to-day operations, recruit new members and manage the group’s various computer archive sites. These groups exist solely to engage in piracy and compete with each other to be the first to place a newly pirated work onto the internet, often before the work is legitimately available to the public. The groups employ highly sophisticated technological measures to shield their illegal activity from victims and law enforcement. Some Warez groups targeted by recent government-led sting operations, such as Site Down, include RiSCISO, Myth,
Goodfellaz and the like (Justice Department Announces International Internet Piracy Sweep 2005).

3.2. **Internet sites**

The internet provides access to a readily available virtual counterfeit shopping environment. The Replica Center blatantly informs consumers where they can purchase a fake Swiss Rolex watch, and provides ‘customer satisfaction reviews’ and ‘testimonials’ for the illicit dealers (www.replicacenter.com). Industry watchdogs, such as the Software Information Industry Association, are constantly ‘trolling’ internet auction sites, such as EBay and Yahoo! to detect pirates and, for example, can use the ‘notice-and-takedown’ process in the Digital Millennium Copyright Act (DMCA) or the Verified Rights Owner (VeRO) programme in EBay to slow the growth of software piracy at this type of internet auction site (SIIA Anti-Piracy 2005 Year in Review 2006). The BSA claims to have shut down an estimated 13,800 auction sites in 2007 for selling illegally pirated software. The sites were selling more than 50,500 software products with an estimated value of $13.3 million. The majority of these auction sites (over 67%) were located at US auction websites (BSA Raises the Stakes in the Fight 2008).

In September 2006, 11 persons were indicted on the premise of their involvement in an Atlanta-based generic drug scam on the internet. This recent case is testimony to the fact that many consumers can ‘unknowingly’ purchase counterfeit via the web. Indeed, the customers in this case actually thought they were purchasing prescription drugs, such as Ambien, Xanax and Viagra over the internet from a Canadian firm. However, according to the indictment, the entire operation began in 2002 by Jared Wheat, principal owner of Hi-Tech Pharmaceuticals, who lured the internet customers through ‘spam’. The drugs were allegedly manufactured in unsafe conditions in a house in Belize (Hi-Tech Pharmaceuticals 2006).

4. **US government-led sting operations to curb internet piracy**

In June 2005, US Attorney General Alberto R. Gonzales cautioned that the Department of Justice would be directing their combating efforts towards the top of the internet piracy pyramid in an effort to dismantle the networks that feed the supply chain of illegal digital content on the web (Justice Department Announces International Piracy Sweep 2005). Some recent sting operations are briefly discussed below.

4.1. **Operation Buccaneer**

In October 2000, the US Customs Service, in cooperation with its allies in Australia, Finland, Norway, Sweden and the UK, worked together under the codename Operation Buccaneer to commence a string of undercover operations designed to infiltrate the operations of criminals that distribute software, games and movies over the internet through the Warez scene by targeting such release groups as DrinkorDie, Razor1911, RiSCISO, Myth and POPZ (www.cybercrime.gov). As a result of this 14-month undercover operation, approximately 70 search warrants were executed worldwide in the initial phase of Operation Buccaneer, and it is, to date, notably the most significant law enforcement penetration of international
organisations engaged in the criminal distribution of copyrighted material via the internet. The law enforcement officials seized several Warez archive sites terminology described as highly-secured computers used to store massive quantities of pirated software, games and movies. Access to these sites is used as a reward for active Warez group members and as an incentive for them to continue their illegal activity.

4.2. Operation Digital Gridlock

Operational Digital Gridlock was a joint investigation conducted by the FBI, the US Attorney’s Office for the District of Columbia, and the Department of Justice’s Computer Crime and Intellectual Property Section. This joint prosecution manoeuvres targeted illegal file-sharing of copyrighted materials over direct connect peer-to-peer networks that belonged to an online group of hubs known as the underground network. These networks required their users to share large quantities of computer files with other network users, all of whom could download each others’ shared files. These were the first federal felony convictions for copyright piracy using peer-to-peer networks, all occurring within about 9 months of the original searches and seizures. The search warrants executed today are the result of Operation Digital Gridlock.

4.3. Operation Higher Education/Operation Fastlink

Higher Education is the largest component of the global law enforcement action known as Operation Fastlink, announced by the Department of Justice on 22 April 2004. Twelve nations participated in Higher Education; it ensued as an 18-month, multinational software piracy investigation. Three men were found guilty of assisting in the cracking, storing and distributing of copyrighted material throughout the world. Operation Fastlink is presently the largest global enforcement action ever undertaken to combat online piracy. It was the culmination of four separate undercover investigations simultaneously being conducted by the FBI, coordinated by the FBI Cyber Division, the US Department of Justice and the Computer Crimes and Intellectual Property Section (CCIPS) of the Criminal Division. The investigation has so far yielded searches and seizures of over 70 high-level targets that were conducted in Belgium, Denmark, France, Germany, Hungary, Israel, the Netherlands, Singapore, Spain, Sweden and the USA, as well as Great Britain and Northern Ireland.

4.4. Operation site down 2005

This enforcement initiative integrated assistance from 10 countries to further apprehend and prosecute the virtual pirates. In a 24-h time frame, the agencies involved in this sting operation conducted over 70 searches in the US and 20 overseas to yield arrests of four individuals in the USA, and stimulated other actions in Australia, Belgium, Canada, Denmark, France, Germany, Israel, the Netherlands, Portugal and the UK. Once again, the main goal of this sting operation was to target the individuals and organisations of the Warez scene since their sites are part of the distribution channel for other suppliers to obtain the counterfeit goods via the internet and resell for a profit. For example, a spam email that advertises cheap software is often downloaded from one of these sites at the top of the internet piracy pyramid and can actually bear the ‘signature mark’ of the Warez group responsible
for its release. This illustrates a striking example of a case where the ‘middleman’ in the internet pyramid bears the profit incentive of the illicit trade.

5. Recent legislation for digital piracy: enforcement is a quandary in the virtual marketplace

It can be very difficult to convince consumers that internet piracy negatively affects such industry giants like the motion picture industry. Consumer willingness to purchase counterfeits can emerge from an anti-big business sentiment; many times the consumer describes a ‘Robin Hood’ (Warez groups stealing from the rich to give to the poor) and/or ‘David vs. Goliath’ (e.g. internet piracy is a means to attack the price-gouging music, software and movie industries) types of analogies to justify their actions of obtaining illegal goods. A quick search in Google using a search query of ‘internet piracy’ produces more individual blogs that support internet piracy than hits which serve to refute its legitimacy. Companies need to reposition the stereotype of a pirate and place a higher emphasis on the connection of the activity to organised crime. For example, Rob Clyde, Vice-President for Technology at Symantec, states that ‘Cyber crime today isn’t about computer geeks just having fun at other people’s expense . . . its real criminals, making real money off of real victims. And it gets more serious by the day’ (The Fight for Cyberspace 2008, p. 2). The message that internet piracy is hurting more than the ‘Goliath’, a term representing firms such as Microsoft or highly-paid screen stars such as Will Ferrell ($43 million in 2006), is a message that needs to be disseminated to the populous to change their sentiment (Rose 2006).

5.1. Digital Millennium Copyright Act (DMCA)

In October 1998, the Digital Millennium Copyright Act (DMCA) was unanimously supported by the US Senate and signed into law by former President Bill Clinton. Basically, the DMCA makes it a crime to disable anti-piracy measures with respect to goods, such as software; outlaws code-cracking devices; requires service providers to remove items from their websites if one suspects copyright infringement; limits liabilities of non-profit institutions of higher education. Digital Rights Management (DRM) allows the copyright holder to thwart access, copying or conversion alteration to other formats by the consumer. The passage of the DMCA has been replete with controversy in terms of both consumer rights and scepticism surrounding enforcement, such as the role of internet service providers’ (ISPs) play by policing their sites for intellectual property rights violations. First, consumer advocates, such as the Electronic Frontier Foundation (ETF), have expressed that ‘technological locks’ inappropriately limit how the purchaser can play and view his or her CDs and DVDs. Second, there is a key provision of the DMCA called the ‘safe harbour’ clause that protects ISPs from being liable for the activities of its users. In general, if a service provider qualifies for the safe harbour exemption, only the individual infringing customers are liable for monetary damages; the service provider’s network, through which they engaged in the alleged activities, remains free of liability.

5.2. Safe harbour of DMCA

The ‘safe harbour’ aspect of the DMCA has proved a source of debate, especially in the legal community. Trevor Cloak in his 2007 article in the Vanderbilt Law Review,
‘The Digital Titanic: The Sinking of Youtube.com in the DMCAs Safe Harbor,’
provides an outstanding example of how the emergence of video-sharing internet
sites (VSIs), such as YouTube.com and the exposure to millions of savvy bloggers,
has created a significant challenge for any provider that allows this type of digital
content. Cloak reaffirms the controversy of the ‘safe harbour’ provision by stating,
‘Given the current operational framework of VSIs, are owners of these sites liable for
copyright infringement when copyright material is illegally posted by their users?’
(Cloak 2007, p. 1561). This presents the premise for an ongoing deliberation of the
liability of the ISPs. Cloak notes that many VSIs will be facing multimillion – if not
billion – dollar law suits in the future due to copyright infringement. The previous
question presents two related issues for discussion: (1) whether the VSIs receive
financial benefits from the copyright materials illegally posted by their users and (2)
whether the VSIs have the ‘right’ and means to effectively control what their users
post on the site.

Another dispute involving the DMCA centres on its ability to have copyright
holders shut down websites if they suspect intellectual property rights violations. For
example, in a case brought by InternetMovies.com to the district court for the
District of Hawaii, the firm asked the court to require that copyright holders provide
some type of investigation and/or evidence of copyright infringement before websites
could be shut down. This request for proof of infringement was rejected by the court,
and the article reported that ‘This decision rules that the Digital Millennium
Copyright Act (DMCA) does not require a copyright holder to conduct an
investigation to establish actual infringement prior to sending notice to an ISP
requiring them to shut-down an allegedly infringing web site, or stopping service all
together to an alleged violator’ (Court Confirms DMCA 2003, paragraph 3).

5.3. No Electronic Theft Act (1997)
The No Electronic Theft Act (NET) embodied a critical form of anti-counterfeit
enforcement, since it was mentioned that Warez scene infringements are often not
motivated by profit-oriented incentives. The NET posits that it is a federal crime to
reproduce, distribute or share copies of electronic copyrighted works, such as songs,
movies, games or software programs, even if the person copying or distributing the
material acts without commercial purpose and/or receives no private financial gain.
Prior to the passage of this legislation, people who intentionally distributed copied
software over the internet did not face criminal penalties if they did not profit from
their actions. As such, Warez scene involvement, driven by the mere incentive of
‘cracking the code’, had flourished due to transgressors’ perception of this liability
free mentality.

6. Ethical perceptions of the internet piracy dilemma: Generation Me is a
willing player
Jeane Twenge in her 2006 book publication, Generation Me, provides a descriptive
label of the cohort of people in the USA born in the 1970s, 1980s or 1990s, or a
person currently aged between 9 and 37 (Twenge 2006). Twenge selected to brand
this population segment, Generation Me, since he or she has focused on ‘self’. The
title does not allude to selfishness, but is rather ‘branding’ which stems from the
significance this generation places on the individual. For example, people within this
age bracket have been consistently told to ‘Be yourself,’ and/or ‘Believe in yourself.’ A few firms and trade associations have conducted studies on buyers likely to purchase counterfeits which suggested that this generation constitutes key players contributing to counterfeit sales. In 2005, the Motion Picture Association (MPA), in their study on the cost of movie piracy, found that the typical consumer of fake goods was aged 16–24, male, and lived in an urban environment (The Cost of Movie Piracy 2005). Although this demographic profile does not yield detailed segmentation, it does show the bias of the younger generation as a ‘willing player’ in the internet piracy game. A recent study conducted for the BSA by Harris Interactive, involving 1644 youth, found that young people clearly viewed downloading music (60%), software (56%) and games (54%) without payment less harmful than stealing from a store (92%) (www.bsa.org). In another web-based survey of 254 (77% response rate) college students from three different universities – one each in New York, Oklahoma and Pennsylvania – Chaudhry and Stumpf (2008) found the following rank order of relative importance of reasons why these students were willing to buy counterfeit movies, where ‘1’ is highest rank, was:

1. Is easy to obtain (mean 2.22, SD 1.17)
2. Desirable quality (mean 2.34, SD 1.37)
3. Not an immoral or unlawful act (mean 2.82, SD 1.17)
4. Have low income or low education (mean 3.55, SD 1.46)
5. It is acceptable due to anti-big business sentiment (mean 3.80, SD 1.13)

Younger students were more inclined to be willing users of counterfeit movies ($r = -0.23, p < 0.001$) and acquire them ($r = -0.19, p < 0.002$). Male students were more inclined to find the internet shopping experience hedonic ($r = 0.22, p < 0.001$), be willing users of counterfeit movies ($r = 0.20, p < 0.001$) and to have acquired them ($r = 0.17, p < 0.01$). More active users of the internet reported less ethical concern ($r = -0.13, p < 0.05$), perceived anti-counterfeiting tactics to be less effective ($r = -0.18, p < 0.005$), social marketing to be less effective ($r = -0.15, p < 0.05$) and find the internet shopping experience hedonic ($r = 0.19, p < 0.002$). They also reported to be more willing users of counterfeit movies ($r = 0.21, p < 0.001$) and to have acquired them ($r = 0.14, p < 0.01$).

As shown in Table 1, Chaudhry and Stumpf (2008) found a number of predictors of student complicity with counterfeit products: the extent to which they had ethical concerns with acquiring counterfeits, the perceived quality of the counterfeit, and the extent to which the shopping experience was hedonic. Their sample also assessed the perceived effectiveness of three actions intended to reduce consumer complicity: product-specific actions (e.g. special packaging), reducing price and social marketing advertisements. For those that were complicit with counterfeit products, these anti-counterfeiting actions were perceived to be ineffective or to have little effect.

As shown in Table 1, Chaudhry and Stumpf (2008) studied three attitudinal predictors of student complicity with counterfeit products: ethical concerns with being complicit, the perceived quality of the product and the desire for hedonic shopping experiences. Each of these attitudes was able to predict the willingness to use a counterfeit product, and to a lesser extent, the actual reported acquisition of counterfeit products. Those who expressed ethical concerns with counterfeits were much less willing to use a counterfeit ($r = -0.43$) or acquire one ($r = -0.32$). Those who perceived quality of the counterfeit to be acceptable, were more willing to use it.
Table 1. Correlations among attitudes, shopping experience and actions intended to reduce complicity with consumer complicity with counterfeit movies.

<table>
<thead>
<tr>
<th></th>
<th>Ethical concerns</th>
<th>Product quality</th>
<th>Hedonic shopping experience</th>
<th>Anti-counterfeiting product-specific strategies</th>
<th>Anti-counterfeiting reduced price</th>
<th>Anti-counterfeiting social marketing tactics</th>
<th>Willing use</th>
<th>Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethical concerns</td>
<td>0.77 (4)</td>
<td></td>
<td>0.77 (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product quality</td>
<td>-0.015*</td>
<td>0.77 (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hedonic shopping experience</td>
<td>-0.022**</td>
<td>0.26**</td>
<td>0.86 (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Perceived effectiveness of actions intended to reduce product counterfeiting

<table>
<thead>
<tr>
<th></th>
<th>Product-specific strategies</th>
<th>Reduced price</th>
<th>Social marketing tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product-specific strategies</td>
<td>0.34**</td>
<td>-0.008</td>
<td>-0.016*</td>
</tr>
<tr>
<td>Reduced price</td>
<td>0.14*</td>
<td>-0.005</td>
<td>-0.013*</td>
</tr>
<tr>
<td>Social marketing tactics</td>
<td>0.34**</td>
<td>-0.007</td>
<td>-0.012</td>
</tr>
</tbody>
</table>

Complicity with counterfeit products

<table>
<thead>
<tr>
<th></th>
<th>Willing use</th>
<th>Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willing use</td>
<td>-0.043**</td>
<td>-0.032**</td>
</tr>
<tr>
<td>Acquisition</td>
<td>0.36**</td>
<td>0.15*</td>
</tr>
</tbody>
</table>

Descriptive statistics

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.3</td>
<td>1.29</td>
</tr>
<tr>
<td></td>
<td>3.3</td>
<td>1.60</td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td>1.36</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>1.31</td>
</tr>
<tr>
<td></td>
<td>5.3</td>
<td>1.67</td>
</tr>
<tr>
<td></td>
<td>4.2</td>
<td>1.27</td>
</tr>
<tr>
<td></td>
<td>3.1</td>
<td>1.71</td>
</tr>
<tr>
<td></td>
<td>0.53</td>
<td>0.50</td>
</tr>
</tbody>
</table>

N = 262.

*rs above 0.12 are significant at p < 0.05, two-tailed.

**rs above 0.17 are significant at p < 0.005, two-tailed.

Main diagonal contains coefficient alpha estimates of internal consistency (reliability) and number of scale items (in parentheses).

All items except movie acquisition were responded to on a seven point scale anchored as follows: 1 = strongly disagree, 4 = neither agree nor disagree, 7 = strongly agree.

Movie acquisition requested a yes/no response.
Those who reported the shopping experience to be more hedonic, also reported a greater willingness to use a counterfeit \( (r = 0.36) \) and acquire it \( (r = 0.15) \). Their study also assessed the perceived effectiveness of three actions intended to reduce consumer complicity: product-specific actions (e.g. special packaging), reducing price and social marketing advertisements. Although product-specific actions and social marketing ads did have a modest significant effect for the entire sample \( (r's \ from -0.19 \ to \ -0.27) \), for those that were most complicit with counterfeit products, the anti-counterfeiting actions were perceived to be ineffective or to have little effect (ns \( r's \), not shown in Table 1).

Companies are devoting attention and effort to devising effective ways to decrease internet piracy, as they acknowledge that the consumer demonstrates a more rogue behaviour and erroneously misjudges his or her ability to be punished for this type of intellectual property theft. For example, the Recording Industry Association of America has an established record of litigation against consumers who are at the bottom of the internet piracy pyramid. In the absence of the fear of being caught and punished, company or industry sponsored anti-counterfeiting actions may do little to deter consumer complicity.

7. Enterprise enforcement mechanisms

Chaudhry and Zimmerman (2009) address an array of plausible enforcement mechanisms that enterprises can use to combat piracy in their book, *The Economics of Counterfeit Trade: Governments, Consumers, Pirates and Intellectual Property Rights*. There is a plethora of anti-counterfeiting actions targeted at consumers (e.g. labelling techniques), distribution channels (e.g. RFID tags, DNA markers), pirates (e.g. monitoring purchases of key components), governments (e.g. lobbying for more IP legislation), international organisations (e.g. using the TRIPS of WTO) and company-based (e.g. developing IP data gathering and monitoring system) (Chaudhry and Zimmerman 2009, p. 158). These researchers’ recommend that an enterprise use an action programme that includes (1) developing an IP protection strategy; (2) forming a brand integrity team; (3) registering trademarks, patents and copyrights; (4) creating information monitoring programme; (5) developing a multi-pronged action plan; (6) fighting pirates; and (7) establishing measurement feedback programme. Clearly, the need to quickly funnel any information about how counterfeits are affecting the enterprise across country markets should be channelled into some type of central repository for the firm (Kakousis et al. 2010).

The BSA, the voice of the world’s commercial software industry, reports on an annual basis its piracy study and claims that worldwide software piracy went up from 28% in 2007 to 41% in 2008 (BSA Piracy Study 2009). However, this study claims that in some countries, piracy rates were reduced by education of consumers, enforcement of governments and technological shifts, such as the increased use of DRM by enterprises. Chaudhry and Stumpf (2009a) emphasised in their *Wall Street Journal* article, ‘Getting Real About Fakes,’ that enterprises must centre their anti-counterfeiting tactics on the fact that fakes are poor substitutes and sometime dangerous (e.g. fake pharmaceuticals); that pirates are not robin hoods (e.g. dispel the cult-like following of Pirate Bay); that enterprises are not faceless corporations (e.g. piracy affects the bottom line and resources available for innovation); and that
ethical concerns are key to consumer education of piracy (e.g. counterfeits can harm consumers).

The Business Action to Stop Counterfeiting and Piracy (BASCAP) in conjunction with the International Chamber of Commerce presented several findings related IP protection from a business perspective (Global Survey on Counterfeiting and Piracy 2007). Despite all of the legislation listed above in the USA, the enterprises reported that the key issues were enforcement, not the need for more legislation to protect their IP. One of the main outcomes of the BASCAP study was to discern how these business managers would allocate anti-counterfeiting resources between efforts to promote more legislation, enforcement and/or public education on their illicit behaviour. The enterprises overwhelmingly chose placing more of their resources into enforcement mechanisms. However, when the firms in this survey were probed on how they would specifically distribute anti-piracy funds to guard their products/services, the managers responded that (a) investing in anti-counterfeiting technologies and securing productions against infringement through product differentiation (56% of expenditure) was more important than (b) supporting local enforcement authorities (28%) or (c) spending on educating consumers (16%). A new way for managers to dedicate their resources to both investing in new technologies and educating consumers is to empower consumers by leveraging technology. Software firm Provalidate, for instance, is developing an electronic warranty card for many enterprises to use that allows the consumer to authenticate purchases at the brand owner’s website by using a sophisticated system of verification codes that also provides managers with the opportunity to collect consumer data. Using an electronic warranty card for both physical and virtual purchases to ensure authenticity can – and will – empower consumers to buy legitimate products (Chaudhry and Stumpf 2009b).

8. Advances in internet anti-piracy technology

Recent trends suggest anti-copying technology may prove more effective in preventing piracy than enforcement. Current enterprise information systems (EISs) are connected with the internet, making the boundaries of EISs more uncertain and vulnerable to brand and data theft (Wang et al. 2010). Given the ease of peer-to-peer file sharing and brand auctioning, anti-piracy technology may offer the most feasible way to prevent or detect, analyse and remove the high volume of pirated content circulated on the web. In this section, we review four anti-piracy technologies shaping the direction of DRM and brand protection: digital watermarking, digital video fingerprinting, software-splitting/virtual leashing and brand protection architecture.

8.1. Digital watermarking

Digital watermarking is a widely used method for securing audio, video and image content over the internet. Watermarking is a class of information hiding techniques that embeds a host signal, such as a video, with a perceptible (visible watermarking) or imperceptible (invisible watermarking) distortion. A watermark reader is used to detect this distortion. The watermark identifies original content, making copies traceable back to the content owner. In DRM systems, watermarks should be robust, limiting pirates from detecting or removing the watermark without
significantly distorting the content. DRM systems use watermarking for a number of purposes: owner identification, copy protection, access control and content tracking. One of the primary uses of watermarking is in copyright protection systems, whereby a copy device reads the watermark image and decides whether or not to make a copy of content depending on the authenticity of the watermark.

Recently proposed techniques have introduced real-time watermarking for DVD and streaming video content protection. Real-time watermarking has the potential to limit pirating of streaming videos on the internet. In 2007, Mohanty et al. proposed the secure digital camera (SDC), which embeds a lossless watermarking image with a cryptographic hash into the host signal immediately upon recording. Mohanty et al. also introduced CryptMark, a novel method that uses cryptography and invisible watermarking simultaneously to provide a double layer protection to digital media. To provide additional protection and better image quality to video and image content, CryptMark may use two watermarks, a user-specific binary watermark and a synthetic watermark generated by the system, fusing them together into the host signal (Mohanty et al. 2007). These advances in robust watermarking techniques may help limit piracy of streaming video content and images on the internet.

8.2. Digital video fingerprinting

Fingerprinting is a relatively new class of information hiding techniques allowing recognition of video excerpts of long or short durations, altered videos for subtitle overlays, video mashups, and videos having different resolution compared to the original. Digital video fingerprinting extracts several unique features of a video, which can be stored as a highly compressed database file for future comparisons. The creation of a digital fingerprint involves specialised software that decodes the video data and applies several feature extraction algorithms. One of the key advantages fingerprinting has over watermarking is that digital watermarks can potentially be removed from a host signal with acceptable distortion to the content, however, digital fingerprinting cannot be removed from content since nothing was added to the original host signal. This makes pirating fingerprinted content more difficult.

On 7 May 2010, Japanese multinational IT firm, NEC Corporation, announced a new video content identification technology based on digital video fingerprinting capable of rapidly detecting illegal copies of video uploaded onto the internet in a matter of seconds (Shimizu 2010). The video identification technology allows service providers and content owners to register original videos and compare the fingerprint signature of the copy to the signature of the original. This technology significantly reduces the time and cost of video inspection by automatically detecting illegal copies and preventing their uploading to the internet. According to NEC, key features of its new technology are: (1) ‘accurate detection of copied or altered video content’, (2) ‘a high detection rate and low false-positive rate for all video contents’, (3) ‘detection of short video scenes’ and (4) ‘compatibility with home PCs’ (Shimizu 2010). Altered video content produced during pirating for placing caption overlays or producing camera captured copies and analogue copies, can be quickly and accurately detected within seconds, even for very short video segments (2 s). Currently, the technology can only be applied to P2P sharing for the detection of illegal copies; however, NEC is currently planning development of additional enforcement mechanisms to aid in the removal of pirated content from the internet. The new technology was

NEC’s technology will help usher in new web services for internet investigators and EIS managers to detect and remove pirated material from the web. Selecting the appropriate web service will involve matching its Quality of Service (QoS) with the requesters’ detection needs. Researchers are investigating QoS brokers that identify an optimum web service for a requester that satisfies his QoS preferences and constraints (i.e. detection rate, accuracy and removal privileges) (D’Mello and Ananthanarayana 2010).

8.3. **Software-splitting and virtual leashing**

Software-splitting is a software protection technique that limits piracy by removing code fragments from an application and running them from a remote server. By having the remote server provide the missing software functionality, but not the code, the application will not run unless it validates itself to the remote server. Provided the missing functionality is difficult to reverse-engineer, software-splitting serves as an effective deterrent to software piracy.

Virtual leashing is a recently introduced class of software-splitting that splits an application into two programs: a client program, which executes the applications’ active tasks, and the server program, which executes the applications’ ‘lazy tasks’ (Dvir *et al.* 2005). Current software-splitting methods scale poorly to the internet due to the synchronous communication between client and server, causing communication latency, where the client blocks waiting for a response from the server. Latency, therefore, has become the most formidable challenge for implementing software-splitting. Virtual leashing, however, is the first non-blocking software-splitting technique. To accomplish this, virtual leashing maintains asynchronous communication between client and server, such that the performance of the application is not impacted by network latencies. One of the key features of virtual leashing is the difficulty it introduces to software pirates in figuring out when memory can be freed. In addition, virtual leashing can use ‘decoy’ messages, which are ignored by the server, but are indistinguishable from valid messages between the client and server (Dvir *et al.* 2005). Virtual leashing is making software-splitting a viable option for software developers to protect their applications over the internet.

8.4. **Brand protection software architecture**

Detecting brand piracy and unauthorised use of brand logos requires a systematic analysis of web content and how brand products are being searched on the internet. Pinsdorf and Ebinger outline three scenarios for detecting brand piracy over the internet:

*Scenario 1* – The manufacturer of a product looks for offers on online stores with a price so low that with a certain probability they are grey imports or even fakes.

*Scenario 2* – A commercial provider of digital images on the internet wants to find out which images appear on other web pages. For this reason, he has marked them with a digital watermark.
Scenario 3 – A certain company wants to find offers on an online auction that contain the brand logo of the company, although the vendor is not an authorised dealer.

Pinsdorf and Ebinger have introduced a brand protection software architecture, which enables an automated inquiry for brand piracy identification on the internet. This architecture supports internet detectives and service providers in tracing dubious web pages potentially violating the rights of brand owners. The brand protection software architecture uses multistage analyses, which allows flexible searching depending on the nature of brand investigation and varying criteria based on the investigated web pages. The distributed nature of the architecture’s filters and servers allows brand piracy investigators to analyse web sites by requests that originate from different servers at different times. Such inquiries are considered less noticeable than queries made using web crawlers (Pinsdorf and Ebinger 2005). QoS for effective brand detection architecture must also emphasise qualitative rather than just quantitative analysis. Most QoS assessments emphasise quantifiable metrics, such as time, speed and volume of data; however, QoS for a brand detection system will be primarily concerned with understanding what people are searching and how it relates to a particular brand (Issa et al. 2009). The introduction of systematic brand protection architecture constitutes significant progress for piracy control of non-digital products over the internet.

9. Conclusions
There have been both recent trends which have facilitated the growth of digital piracy in the past decade, as well as enforcement measures acting to curb the spread. The common denominators to assist the growth of piracy in the global marketplace are namely that, (1) internet penetration rates are growing, (2) the consumer is willing to download and/or purchase fake goods in cyber space and (3) the internet piracy pyramid remains intact to generate supply and/or demand. The main factors developed to impede this market are the various unilateral and multilateral enforcement tactics, such as Operation Buccaneer, and government legislation, such as the DMCA. It can be concluded that firms face a battle that is really just beginning; one which is to be fought in a virtual war zone and thus requires awareness of measurable implications and managerial talent that understands the key players.

One can question how much enforcement is required to seriously demotivate the main actors in the Warez scene to stop supplying the internet piracy pyramid. Overall, these groups are releasing the illicit products on the web as a matter of pride in an elaborate art of cracking the code and subsequently engaging in a ‘digital war’ with copyright holders. Government legislation, such as the safe harbour provision in the DMCA, will be tested in the court systems to define the liabilities of the ISPs, the pirates selling [or posting] at the site and the consumers. The entire topic of digital piracy is a paradoxical issue presented by current technology advances. On the one hand, the internet has literally provided us with boundless information capacity to feed our insatiable appetite for knowledge, such as the proliferation of information freely posted on the web. Could we have conceived or understood a concept like YouTube.com a decade ago? On the other hand, advances in technology and the expansion of internet market penetration have created a dark side to cyber
space. Namely, the challenges associated with managing the growing concern for internet piracy implications.

Ironically, the future demise of piracy may stem from creative technological solutions, such as software developed by Provalidate\textsuperscript{1} to provide enterprises the ability to use electronic warranty cards that are validated through the company’s website to thwart the pirates. NEC has also introduced groundbreaking technology for video content identification that significantly reduces the time to verify video segments or long or short durations. NEC plans to introduce additional tools that address the distribution of its video content identification technology, potentially making it widely available in home computers and web services. Research in the area of web services QoS and QoS brokers will further empower EIS managers and content owners to find an optimum piracy detection tool for particular detection needs.

A wide range of technologies are being developed that defend against different types of piracy: digital watermarking and fingerprinting protect image and video content, software splitting/virtual leashing protect software applications and brand piracy software architecture aims to protect non-digital brand goods. The combination of these technologies will offer enhanced content protection. For example, watermarking and fingerprinting have different goals, and, therefore, use different schemes (watermarking identifies the content owner and fingerprinting seeks to identify a traitor), but the combination of both schemes can greatly enhance the protection of digital content against piracy depending on the pirate’s intention (Li \textit{et al.} 2005). Mohanty \textit{et al.} has also illustrated the benefits of combining digital watermarking and cryptography for enhanced-content protection.

We are sure to see a proliferation of technologies used by both anti-piracy agents and pirates. As more tools are used to dismantle the piracy pyramid, pirates will seek new ways to circumvent such tools. The solution in breaking the piracy pyramid may be the coordinated effect of preventing illegal content uploads; removing illegal content from the web faster than pirates can repost them, and applying enforcement pressure through litigation and sting operations on major offenders. Ultimately, consumers may find it increasingly difficult to source pirated goods online and acquire products easier through authorised channels.

\textbf{Acknowledgement}

We acknowledge the support to conduct this research from the Fred J. Springer Chair in Business Leadership at the Villanova School of Business.

\textbf{References}


