Strategies for Securing the Cyber Safety Net for Terrorists: A Multi-Disciplinary Approach (Chapter 16) in TERRORISM AND GLOBAL INSECURITY: A MULTIDISCIPLINARY PERSPECTIVE (ed. Klint Alexander)(Linton Atlantic Books, Ltd.)(2009)

*Doris Estelle Long

Abstract

Cyberspace provides a potent safety net for terrorists as its under-regulated spaces allow for a variety of illegal acts in support of terrorist activities. As traditional sources for terrorist funding have come under increased scrutiny and control, terrorists and other paramilitary organizations have increasingly turned to other illegal avenues for their fund raising activities. While high level crimes, such as drug running and human trafficking, have received increased attention, the threat to global security of such "low level" crimes as digital piracy, phishing and identify theft remain largely ignored.

This Article explores the growing evidence that "personal" crimes such as digital piracy, counterfeiting, phishing and digital fraud are being used to fund terrorists' activities. It examines the digital safety net in which these crimes exist, created by a mix of cultural and economic factors that have undervalued the global security threat of these crimes. After comparing current international enforcement efforts, in the United States, the European Union and India, with a focus on cyberfraud and digital piracy laws, this Article suggests a multidisciplinary, transborder approach for reducing this safety net and enhancing global security within the context of broader counter-terrorist efforts. Such approach, however, must be a nuanced one to avoid having prosecution of so-called "victimless" or "personal" crimes become new methods for locking up information or violating hard fought individual rights.

introduction

Terrorism,[1] like globalization, is not a new phenomenon of the 21st Century. Both,

1. This Article does not attempt to answer the question of which organizations qualify as "terrorist" groups. The question is problematic. For example, do para military organizations such as the IRA qualify as terrorists or criminal syndicates? *See, e.g.*, Testimony of Timothy Trainer, Hearing on International/ Global Intellectual Property Theft: Links to Terrorism and Terrorist Organizations, House Committee

*Doris Estelle Long is a Professor of Law and Chair of the Intellectual Property, Information Technology and Privacy Group at The John Marshall Law School in Chicago.

however, have been fundamentally changed with the advent of globalized digital communications, in particular, the development of the internet[2] and its companion communication technologies, including wi-fi and RFID. The new world of Digital Terrorism is composed of a wide array of new threats, some of which may well be old terrorism in new guises. Among the most prominent of the new forms of digital terrorism are "cyberterrorism—involving threats to infrastructure using the internet as a means of achieving such goals[3]—cybernetworking—where terrorist groups use the anonymity and encryption benefits of the internet to communicate public and private messages and plans[4]— and cyberfunding—where the internet serves as a means for raising and distributing funds for terrorist purposes.[5] In the 1999 Rand Study on "Countering The New Terrorism,"[6] the authors recognized (I think correctly) that the internet served

---

on International Relations, Before the United States House Committee on International Relations(July 16th 2003)[hereinafter "Trainer Testimony"]. For purposes of examining the cyber safety net for terrorist funding, the issue is largely one of statistical import (which category of illegal actors qualify as terrorists for purposes of determining funding activities?). These statistical issues do not significantly impact the analysis of the problem in this Article of the cyber net safety since both "terrorist organizations" and "paramilitary syndicates" are using the cyber safety net to protect their illegal funding activities. See generally 22 USC § 2656f(d)(defining "terrorism" as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience" and defining "terrorist group" as "any group practicing, or that has significant subgroups that practice, international terrorism" which the act further defines as "terrorism involving citizens or the territory of more than one country").

2. Although common usage continues to use an initial capital latter to describe "the Internet," such usage no longer seems appropriate given the internet's wide spread and long-standing use. Just as "the Telephone" has become "the telephone," so too, it is time to recognize that "the Internet" has become an accepted and longstanding communication form that no longer needs to be treated with the exclamatory reverence of an initial capital letter. Such special treatment, I believe, has been used in part to relieve international law of its responsibility to resolve the legal issues surrounding intellectual property and privacy on the internet. Capital letters subconsciously tell us all that the "Internet" is something new; so new that we cannot yet be expected to deal with the problems it poses. The time for such complacency, along with the initial capital letter, is long past.

3. This would include denial of service attacks, cyber extortion and other net-based attacks. See generally Dan Verton, Black Ice: The Invisible Threat of Cyber-Terrorism (McGraw Hill 2003); Peter Grabosky, Russell G. Smith, Gillian Dempsey, Electronic Theft: Unlawful Acquisition in Cyberspace (Cambridge University Press 2001); Lawrence V. Brown, Cyberterrorismand Computer Attacks (Novinka Books 2006); James F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism (Citadel 2003); Lech J. Janczweski & Andrew M. Colarik (eds), Cyberwar And Cyber Terriorism (IGI Global 2007). .

4. See Eben Kaplan, *Terrorists and the Internet* (May 12, 2006)(available at www.cfr.org/publciations/10005/terrorist_and_the_internet.htm0)(last visited Jnauary 4, 2009); Gabriel Weimann, Terror Onthe Internet (USIP Press Books 2006); Gabriel Weimann, Special Report No. 116: How Modern Terrorism Uses the Internet (March 2004)(available at www.usip.org/pubs/specialreports/sr116.html) (last visited January 4, 2009); Maura Conway, Terrorist Uses of the Internet and Fighting Back (September 2005)(available at http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=20642)(last visited January 4, 2009).

5. *Id. See also* T.G. Winston, *The Use of the Internet for Terrorist Purposes: A Discussion of the Intelligence Challenges in Tracking, Tracing, and Investigating Terrorist Fund-Raising and Fund Transfer Activities via the Internet* (available at www.allacademic.com/meta)(last visited May 31, 2007).

6. Ian O. Lesser, Bruce Hoffman, et al, *Countering The New Terrorism* (Rand 1999)[hereinafter "Rand Study"].

such a valuable organizational and communicative function for their activities that its potential destruction by terrorists was exaggerated if not mistaken.[7] But simply because the internet qua internet may not itself be a target of cyberterrorism does not mean that it cannot be used to advance terrorist aims.

Just as globalization has made every Mom and Pop store a potential global marketer, the internet has made every local terror group a potential member of a vast global network.[8] The relationships and goals between such members may be vastly different from prior incarnations. The "members" may no longer have the identical goals or even perceive themselves to be members of a network or particular terrorist group per se.[9] But as participants in the newly emerging digital terrorist network, they are all beneficiaries of the enhanced ability to communicate plans, and information much more quickly and with potentially greater anonymity than ever before. The internet has made even the most localized terrorist a potentially deadlier threat as he taps into information and funding sources that were unknown at the end of the last century.[10]

Aside from potential new methods of terrorism that the internet provides, including viruses designed to take down even the net itself, the internet also poses new funding opportunities that are even more difficult to track and eliminate. Fund tracing has always been a risky effort at best. In the 1990s when Al Qaeda first emerged into global consciousness, many wrongly believed that its funding was derived primarily from the individual wealth of Osama Bin Laden.[11] It was only over time that these agencies

7. This does not mean that terrorist organizations will not target certain websites for denial of service and other disruptive attacks. However, such attacks will be directed toward individual sites and not bringing down the entire internet infrastructure. This does not mean that such directed attacks do not present a serious challenge to cyber safety; merely that despite these attacks the cyber safety net will remain secure unless steps are taken to reduce or eliminate it.

8. I do not mean to suggest that all terrorist groups are organized into some vast formal network. To the contrary, current evidence seems to indicate that such wide-ranging hierarchical organizations, such as were believed to have existed at the end of the Twentieth Century between disparate groups such as Al Qaeda and Hezbollah, may have been greatly exaggerated. Instead, the current network is more like a loosely connected group of chat room users who share interests, ideas and information. *See generally* Eli Karnon, Coalitions Between Terrorist Organizations: Revolutionaries, Nationalists and Islamists (Brill 2005). See also Marc Spenser, Understanding Terror Networks (U. Penn. Press 2004); Richard Rothberg, From Whole Cloth: Making Up the Terrorist Network, Connections (Vol 24, Issue 3)(available at http://www.insna.org/pubs/connections/v24.html)(last visited January 4, 2009); Center for Defense Information, *The Business of Terror: Conceptualizing Terrorist Organizations As Cellular Businesses* (May 23, 2005)(available at www.cdi.org/pdfs/terror-business-model.pdf)(last visited January 4, 2009); E. Rothstein, Lacking a Center, terrorist networks are hard to find let alone fight, New York Times (October 20, 2001).

9. Id.

10. See, e.g., Rand Study supra note 2 (describing changes in new brand of terrorism at the end of the 20th Century); Matthew Carr, *The infernal Machine: A History of Terrorism* (New Press 2007); Walter Lacqueur, *A History of Terrorism* (Transaction Publishers 2001): Albert Parry, *Terrorism: From Robespierre to the Weather underground* (Dover Publications 2006); Donatella della Porta, *Social Movements, Political Violence and the State: A Comparative Analysis of Italy and Germany* (Cambridge 2004).

11. This belief was so prevalent that the National Commission on Terrorist Attacks upon the United States, in their report on the 9/11 attacks directly addressed the issue and announced that no such evidence had been found to support this belief. *See* National Commission on Terrorist Attacks

gradually began to focus on other sources, including the social and charitable umbrellas for Hezbollah and other recognized terrorist organizations.[12]

Just as the earlier focus on personal wealth of acknowledged leaders delayed the tracking of actual funding through "charitable foundations," the focus on these organizations today may well delay action against the new, growing source of terrorist funds—the internet, and the relatively low tech crimes it supports. Although the diaspora and private funding of terrorist organizations through front organizations posing as charitable or service organizations remain significant sources for terrorist funds,[13] law enforcement has become more adept at finding and tracking such funds.[14] Yet as traditional sources for terrorist funding have come under increased scrutiny and control, terrorists have increasingly turned to other illegal avenues for their fund raising activities, including piracy, phishing and identity theft.

This Article explores the burgeoning role that cyberspace plays in supporting funding activities that are increasingly being used to support diverse terrorist groups and activities. It explores the potential for cyberspace to serve as a potent safety net for terrorists due to its largely unregulated nature. This unregulated nature is only partially caused by the diaphanous, temporary nature of the net and is instead largely supported by public and law enforcement indifference which perceives many internet based crimes as victimless and largely either insignificant or unstoppable. Neither assumption is correct. To the contrary, given the transborder nature of many of these underground activities, without a well developed multidisciplinary, international approach, these "victimless" crimes will continue to develop as part of the underground economy that supports organized crime and terrorist activities.

In Part I, I provide a brief overview of "low level" digital crimes, including digital piracy, phishing and identify theft, and examine the growing evidence that such crimes are increasingly being used to fund terrorist activities. I also explore some of the reasons why the prosecution of such crimes has remained largely non-existent. In Part II, I examine some of the current international efforts to combat these low level, victimless

---

Upon the United States, *Monograph on 9/11 and Terrorist Travel* 20 – 21 (2004)(available at www.9-11-commission.gov/staff_statements/index.htm)(last viewed January 4, 2009).

12. *See, e.g*. National Commission on Terrorist Attacks Upon the United States, *Monogram on Terrorist Funding* (2004)(available at www.9-11commission.gov/staff_statements/index.htm)(last viewed January 4, 2009)["hereinafter National Commission on Funding"]; Victor Couras, *Al Qaeda Finances and Funding to Affiliated Groups, Strategic Integrity* (Vol. 4, Issue 1)(January 2005); Eben Kaplan, *Tracking Down Terrorist Financing* (April 4, 2006)(available at www.cfr.org/publication/10356) (last visited January 4, 2009); Jeremy Scott-Joynt, *US terror fund drive stalls* (September 3, 2002) (available at http://news.bbc.co.uk/1/hi/business/2225967.stm)(last visited January 4, 2009).

13. *See generally* Testimony of Ronald K. Noble, Secretary General of INTERPO, "The links between intellectual property crime and terrorist financing," Before the United States House Committee on International Relations (July 16th 2003)[hereinafter "Noble Testimony"]; Kaplan, *supra* note 13; Elaine Landau, *Osama Bin Laden: A War Against the West* (21st Century Books 2002); National Commission on Funding, *supra* note 13;

14. *See generally* Noble Testimony; Eben Kaplan, *Rethinking Terrorist Financing* (January 31, 2007) (available at www.cfr.org/publication/12523/rethinking_terrorist_funding.html)(last visited January 4, 2009).

crimes and discuss why such efforts are currently unavailing. In Part III, I propose a multidisciplinary approach to taking back cyberspace and securing it from becoming a safety net for terrorists. This requires a nuanced approach, however, to avoid having prosecution of "victimless" crimes become new methods for locking up information or violating hard fought individual rights.

i. cybercrimes and the hidden funding bonanza

The use of criminal activities to fund radical or terrorist activities is not a new development. Anarchists of the 19th century robbed banks to obtain funding.[15] So too did the Bader Meinhoff gang of the 20th Century in West Germany.[16] Kidnapping has helped fund various guerrilla movements in Latin America and South East Asia.[17] But at least the crimes of bank robbery and kidnapping are considered significantly wrongful so that law enforcement will devote substantial resources to investigate and stop such activities. Current "victimless" crimes in the Digital Era, however, remain low on the enforcement radar screen and, consequently, are becoming increasingly profitable sources for terrorist funding.

Perceived as low level, individual impact crimes, with infrequent prosecutions, and largely non-existent criminal penalties, the "victimless" crimes of digital piracy,[18] identity theft[19] and phishing[20] are becoming cash cows for growing numbers of terrorist and paramilitary groups. Lax enforcement has created a safety net for terrorist funding activities, enabled in part by public apathy.

A. Digital Piracy[21]—The Secret Cash Cow

The illicit reproduction and sale of copyrighted books, films, albums, and software

---

15. *See generally* Carr, *supra* note 11; Lacqueur, *supra* note 11; Parry, *supra* note 11; Walter Reich and Walter Lacqueur, *Origins of Terrorism: Psychologies, Idealogies, Theologies, States of Mind* (Woodrow Wilson Press Center); Paul Avrich, *The Haymarket Tragedy* (Princeton U Press 1986); Paul Avrich, Sacco & Vanzetti (Princeton U Press 1996).

16. *Id. See also* Della Porta, *supra* note 11. Hijacking has also been used in connection with diverse terrorist activities through the years, with particular prominence in the 1970s.

17. *See texts* cited note 16 *supra*. *See also* Gerard Chaliand & Arnaud Blin (eds), *The History of Terrorism From Antiquity to Al Queda* (U. Cal. Press 2007).

18. For a definition and further discussion of the nature of digital piracy, see text *infra* at Part I.A.

19. For a definition and further discussion of the nature of identity theft, see text *infra* at Part I.D.

20. For a definition and further discussion of the nature of phishing, see text *infra* at Part I.C. While phishing is a form of identity theft using internet based sources, its unique use of digital technology makes it worthy of separate consideration because, like digital piracy, it is tainted by the assumption that illegal conduct on the internet is virtually incapable of control.

21. Basically, digital piracy is the unauthorized reproduction and distribution of virtual copies of copyright protected works. *See, e.g.,* Agreement on Trade Related Aspects of Intellectual Property Rights [hereinafter "Trips"], Art.52, Note 14 (defining "pirated copyright goods" as "any goods which are copies made without the consent of the right holder or person duly authorized by the right holder in the country of production and which are made directly or indirectly from an article where making of that copy would have constituted an infringement of a copyright or related right…"). By contrast, digital counterfeiting is the unauthorized production and distribution of goods bearing "spurious" or virtually identical versions of another's trademark or service mark. *See, e.g.,* 15 USC § 1127 (defining counterfeit

has been a problem since the invention of the printing press in the 14th Century and the enactment of the first licensing acts for printers.[22] With the development of digital technologies for reproduction (such as reproducing music into digital format for burning onto CDs), and more specifically for digital distribution (including illegal distribution of digital downloads of music and motion pictures through peer to peer software[23]), piracy rates have skyrocketed. The amount of money lost through such illicit activities is always difficult to measure. It is even more difficult in the instance of copyright piracy, where criminals are notoriously poor accountants, and the value of pirated works is subject to dispute.[24] Even in light of these limitations, the amount of lost sales to digital piracy on a global basis is staggering. According to a recent report on global software piracy, 35% of all installed software in 2004 was pirated, resulting in over $33 billion dollars in lost revenue for US industries alone.[25] By 2007 global software piracy rates had grown to 38% with over one half of the studied countries posting a piracy rate of 61% or higher.[26]Estimates by the US Department of Commerce place global piracy losses by US industries at approximately $250 billion in lost sales.[27] Even if such figures are halved, digital piracy poses a potentially lucrative source of virtually untraceable funds.

Part of the appeal of piracy as a source of illicit funds is the growing underground

---

marks as "spurious" marks). *See also* TRIPS, Art.52, Note 14(defining "counterfeit trademark goods" as "goods, including packagings, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods or which cannot be distinguished in its essential aspects from such a trademark….") In popular press discussions the two terms are often used interchangeably. Both qualify as an intellectual property crime. *See* TRIPS, Art. 61. *See also* Noble Testimony, *supra* note 14. Moreover, pirated goods are often sold with counterfeit marks, thus intertwining the two activities even further. Hence, digital pirates are also generally counterfeiters as well.

22. *See, e.g.* Mark Rose, A*uthors and Owners: The Invention of Copyright* (Harv. U. Press. 1993). (discussing the development of the Stationers' Guilds in England); Carla Hesse, *Publishing and Cultural Politics in Revolutionary Paris, 1789-1810* (Berkeley: UC Press, 1991)(discussing the development of pirated and scatological works during the Ancien Regime in France).

23. For some reason, while the piracy of electronic works has occasionally been reported, including most notoriously pirated copies of Stephen King's on-line novel *Riding the Bullet*, widespread piracy of electronic books remains under analyzed. Piracy of hard copies of books, including textbooks, however, remains a serious concern. Thus, for example, in 2006, the Association of American Publishers reported losses from textbook sales in China (excluding digital piracy) of over $52 million. *See, e.g*, Statement of Patricia Schroeder, President Association of American Publishers, Testimony before the Subcommittee on Trade of the House Committee on Ways and Means (February 15, 2007) (available at http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=5457)(last visited January 4, 2009).

24. At its heart is a dispute over whether the value of the pirated work should be the retail price of the work, or the price charged for the pirated work, which is always substantially lower. *See* note 33 *infra*.

25. BSA Global Piracy Study for 2004 (available at http://www.bsa.org/globalstudy) (last visited January 4, 2009).

26. BSA Global Piracy Study for 2007 (available at http://global.bsa.org/idcglobalstudy2007/studies/2007_global_piracy_study.pdf)(last visited January 4, 2009).

27. Bush creates new post to fight global piracy, http://findarticles.com/p/articles/mi_kmafp/is_200507/ai_n14800278 (July 22, 2005)(last visited January 4, 2009). This figure presumably does not include lost tax revenues, or lost business and employment opportunities. It also does not include lost income opportunities for local distributors and manufacturers who might be employed to create and distribute non-pirated goods. *See, e.g., Movie Piracy Costing Cinemas* by Box Office Losses, The Jamaica Observer (July 10, 2005)[hereinafter "Jamaica Movie Piracy"].

market in copyrighted works that has mushroomed since the development of easy reproductive technologies.[28] While shoplifting is generally perceived as wrongful, the purchaseofpiratedandcounterfeitgoodsisoftenromanticized. Piratesareswashbuckling heroes who sail the seven seas. Jack Sparrow, Blackbeard, Captain Blood. The loss of life and property caused by real life pirates, including today's modern equivalents,[29] is often lost in the fictionalized romance of the high seas. Pirates are often portrayed as modern day freedom fighters, combating the tyranny, bigotry and close mindedness of traditional society. Thus, for example, in the most recent installment of the highly successful Pirates of the Caribbean franchise, the "villain" is the governor of the island of Jamaica and the head of the perceived 18th Century equivalent of today's film and music industry—the Dutch East India company.[30] Digital pirates have been blessed with the same romanticized images. YouTube videos are broadcast on network news. Net groups advocate the illegal file trading in music as a way to wreak "vengeance" on a greedy and overreaching industry, with no regard to the harm to individual artists the lack of any royalty may cause.[31] When the piracy is occurring in the developing countries additional "romantic" excuses for such piracy include the poverty of purchasers combined with the inevitably higher prices of legitimate products.[32]

---

28. *See, e.g.*, Rohan Gunaratna, *The Terror Market: Networks and Enforcement in the West,* Harvard International Review, Vol 27/4 (2004); Doris Estelle Long, *Practical Tips For Combating The Scourge Of Global Piracy,* Intellectual Property Law Committee Newsletter (Fall 2005)(ABA Section on Torts, Trial and Insurance).

29. *See Antipiracy Drive in Malacca Straits* (July 20, 2004)(available at http://news.bbc.co.uk/2/hi/asia-pacific/3908821.stm)(last visited January 4, 2009): ICC Commerical Crime Services, Reported Incidents of Piracy Rise Sharply in 2007 (January 8, 2008)(available at http://www.icc-ccs.org/index.php?option=com_content&view=article&id=148:reported-piracy-incidents-rise-sharply-in-2007-&catid=60:news&Itemid=51)(last visited January 4, 2009).

30. Pirates of the Caribbean: Deadman's Chest (Walt Disney 2006).

31. *See, e.g,* Katie Hafner, *Is it Wrong to Share Your Music?,* New York Times (September 18, 2003) (reporting on diverse views among junior high students regarding their right or intention to continue downloading illegal music); Laura M. Holson, *Studios Moving to Block Piracy of Films Online*, New York Times (September 24, 2003)(reporting on focus group meeting with college and high school students where participants indicated an intent to continue illegally downloading films regardless of legal prohibitions). *See also* Doris Estelle Long, Written Testimony, "Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry," Submitted to the Senate Committee on Governmental Affairs (September 30, 2003), *reprinted in* John Marshall Center for Intellectual Property Law News Source (Spring 2004)[Long Written Testimony]. Interestingly, the use of the term "piracy" to refer to the illegal downloading and file trading of copyrighted works has been questioned as a term that is inappropriate to the use of works which do not result in "harm" to the original work. *See, e.g.*, Richard A Posner, *The Little Book of Plagiarism* (Pantheon 2007). Given its romantic connotations, I agree, but for entirely different reasons. Moreover those who claim that illegal copying of copyrighted works is not the equivalent of "theft" or "shoplifting" because it does not result in "harm" to the original version misperceive the nature of the act. While Judge Posner in his recent book *Plagiarism* referred to illegal file trading as "joy riding," such "joy riding" undoubtedly causes economic harm not only to the owner of the stolen "car" but to the people who earn their living from its rental. If unauthorized P2P file trading is similar to joy riding, then it is the joy riding in the cab of a working cab driver and not the mere inconvenience of borrowing Mom and Dad's car without permission.

32. Such prices are inevitably higher because the pirate never has to advertise the product, promote the artist of pay any of the costs involving in actually producing the work in question. Where the pirated

In the early part of the 21st century most of the evidence of the use of digital piracy as a source of terrorist funding was based on largely anecdotal evidence—stories of evidence secured in raids on terrorist bases, offices or the homes of terrorist members that consisted of illicit master disks, information on how to raise money through digital piracy, or stashed of pirated films and software[33] In testimony before the Committee of International Relations, at a hearing on the International/Global Intellectual Property Theft: Links to Terrorism and Terrorist Organizations in the US House of Representatives, Timothy Trainer, then-President of the International Anti-Counterfeiting Coalition (IACC), described numerous instances when private investigators, seeking evidence of trademark counterfeiting, came across flight manuals in Arabic and bridge construction documents which were turned over to the FBI for further investigation.[34] In 2002 the BBC reported the seizure in Denmark of counterfeit shampoos, creams and other consumer goods bound for the UK from Dubai which were ultimately traced to an Al Qaeda member.[35] In 1996 the FBI confiscated 100,000 t-shirts bearing counterfeit marks and determined that the ring behind the operation was run by Sheik Omar Abdel Rahman, later sentenced for plotting to bomb various New York City landmarks.[36]

Aggregation of such scattered anecdotal evidence, however, has gradually led to a growing recognition that digital piracy increasingly serves as a potent source for terrorist funding. In July 2003, Interpol Secretary General Ronald K. Noble testified before the US House Committee on International Relations regarding the link between terrorism and provided examples of the way in which piracy and counterfeiting have been used to fund extremist organizations. He warned: "Law enforcement agencies have to recognize that Intellectual Property Crime is not a victimless crime. Because of the growing evidence that terrorist groups sometimes fund their activities using the proceeds, it must be seen as a very serious crime with important implications for public safety and security."[37] Noble went on to describe the various links between terrorist

product is created through intensive research and development such as software or pharmaceuticals, pirates of course never have to absorb the costs of such R&D.

33. *See generally* Noble Testimony, *supra* note 14; Trainer Testimony, *supra* note 2: Eben Kaplan, *Tracking Down Terrorist Financing* (April 4, 2006)(available at www.cfr.org/publication/10356)(last visited January 4, 2009); Reuters, Counterfeit goods are linked to terror groups, *International Herald Tribune* (February 2, 2007); Jeffrey Williams, *Counterfeiting of Goods: the risks And Links to Terrorist Funding* (available at http://www.osi-philippines.com/articles/counterfeiting-of-goods.html (last visited January 4, 2009); *Testimony of John Stedman, County of Los Angeles, Sheriff's Department, Before the Committee on Homeland Security and Governmental Affairs* (May 25, 2005); Susan Rinkunas, The Hidden Cost of Counterfeit Goods, *The Review* (February 27, 2007); Chris Stewart, Counterfeit Goods A Genuine Problem in US? (available at http://www.nam.org/~/media/Files/s_nam/docs/233400/233394.pdf.ashx)(last visited January 4, 2009); Tony Thompson, Ulster Terror Gangs link up with mafia: Loyalists and republicans in global counterfeit scams, *Observer News* (Guardian Newspapers Limited) at p. 13 (June 15, 2003).

34. *Id.*

35. International Anti-Counterfeiting Coalition, *Facts on Fakes* (available at http://www.iacc.org/resources/Facts_on_fakes.pdf)(last visited January 4, 2009).

36. John Mintz & Douglas Farah, *Small Scams Probed for Terror Ties*, Washington Post, at A1 (August 23, 2002).

37. Noble Testimony, *supra* note 14 at 5.

groups and counterfeiting. These included "direct links" where the group is implicated in the production, distribution and sale of counterfeit goods[38] and "indirect" links where "sympathizers or militants are involved in intellectual property crime and remit some of the funds, knowingly to terrorist groups via third parties."[39] In fact, the acceptance that piracy plays a role in terrorist funding has even reached the level of the general public where articles in 2005 in popular news magazines including Time and US News and Weekly Report included this link as part of their reporting on terrorist funding.[40] The recent terrorist attacks in Mumbai in December 2008 have revived popular discussions of the issue.[41]

Unfortunately the empirical evidence regarding the scope of such funding remains problematic, much as the scope of other funding sources remains shadowy. Even in the absence of hard, if slight, evidence that terrorists are beginning to realize what organized crime realized long ago—there is easy money to be had in piracy, common sense would indicate that piracy is a highly lucrative source for illicit funding. Given the potentially high returns on investment, the ease of reproduction in the face of digital reprography, and the high customer demand, digital piracy has long served as a source for funding, and money laundering by organized criminal groups.[42] It makes sense that terrorist groups would similarly use such sources, particularly since on a global level copyright piracy remains under-enforced. In fact, part of its appeal for criminal organizations has been that such crimes are rarely prosecuted. It is *not* due to lack of evidence, or lack of criminal activity. It is largely due to lack of will on the part of law enforcement to spend enforcement dollars on what is perceived to be an "economic crime" whose only victims are wealthy intellectual property owners.

B. When Consumers Are the Enemy

Fueling the lack of enforcement for this emerging source of terrorist funding is the increasingly entrenched "disconnect" in end users' minds between physical theft and the purchase of pirated works. People who would never engage in shoplifting have no apparent compunction in making and distributing illegal copies of copyrighted songs, movies and software.[43] In fact, as opposed to recognizing that such activities are

38. According to Noble: "Terrorist organizations with direct involvement include groups who resemble or behave more like organized criminal groups than traditional terrorist organizations." *Id*. He cited paramilitary groups in Northern Ireland as an example. *Id*.

39. *Id*. Noble cited Hezbollah as a group that fits within this category. He also provided specific examples of terrorist funding by groups as diverse as the Chechen separatists, Hizbullah, Al-Qaeda, paramilitary groups in Ireland and North African radical fundamentalists in Europe. *Id*.

40. *See, e.g.*, Kate Betts, *The Purse Party Blues, Time Magazine* (August 2, 2004).

41. *See, e.g.*, This New Year, Bollywood Stars Protest Against Piracy (December 29, 2008)(available at http://www.realbollywood.com/news/2008/12/stars-piracy.html)(last visited January 4, 2009).

42. *See generally* note 34 and sources cited therein.

43. *See, e.g., Is it Wrong to Share Your Music?, The New York Times* (September 18, 2003));. *Studios Moving to Block Piracy of Films Online, the New York Times* (September 24, 2003); *US is Only Tip of Pirated Music Iceberg, The New York Times,* (September 25, 2003). *See also Long Written Testimony supra* note 32.

unlawful, there appears to be a growing consensus that piracy is almost a *right* granted to consumers because the cost of a copyrighted work is so high. A common refrain, regardless of the region of the world I am in, is that consumers buy pirated works because the originals are too expensive. The unspoken corollary is that if the price of a work were lower, piracy would disappear. Unfortunately, no one can agree on what that "cheaper" price should be. As a result, there is little, if any, demand by local populations for greater enforcement, and little recognition of the need to prosecute such lucrative crimes.[44] This disconnect has grown even more entrenched with the development of peer to peer (P2P) software which allows end users to "share" copyrighted files regardless of whether the posting or distribution of such materials has been authorized by the copyright holder. From its notorious early days as a web-based distribution system under Napster,[45] to current incarnations of truly end user driven systems such as Morpheus, BitTorrent and Donkey, peer to peer software has enabled end users to rapidly distribute over the internet digital files, including files containing copyrighted works. Most P2P software is distributed without charge to end users, who then communicate directly with one another to seek and obtain digital files, primarily of copyrighted songs and films. Losses due to digital piracy on the internet are virtually incalculable given the untraceable nature of such end user based activities. Current estimates by the Motion Picture Association of America, for example, place losses due to internet piracy at approximately $2.3 billion for 2006 alone, which can only be a guess at best. [46]

Since much of the copyrighted material is distributed without charge by the users of a given system, there appears little opportunity for P2P systems to serve as a source of illicit funds. Such a view, however, may be as narrow and misguided as the early view that Al Qaida was funded by the personal wealth of Osama Bin Laden. While most P2P software providers charge no fees for providing their software to end users, they do earn substantial fees from advertising. Every click on the website to download the software or provide updated information about software modifications or other news, results in substantial revenues for the operator of the "free site." Thus, for example, despite the fact that Grokster charged no fees for its P2P software, its alleged earnings in 2003 exceeded $80 million. Such monies were earned from activities that have been deemed potentially illegal by the Supreme Court of the United States, which recently upheld a suit against Grokster for contributory copyright infringement based on its offering of P2P software used primarily for the illegal distribution of pirated music.[47]

---

44. The exception is the local owner who is the authorized dealer of legitimate goods and can trace business loss directly to lack of enforcement. *See, e.g.,* Jamaica Movie Piracy, *supra* note 34.

45. *See* A&M Records, Inc. v. Napster, Inc., 239 F3d 1004 (9th Cir. 2001). See also Joseph Menn, *All the Rave: The Rise and Fall of Shawn Fanning's Napster* (Crown Business 2003).

46. *See, e.g.,* MPAA, *The Cost of Movie Piracy* (2006)(available at http://www.mpaa.org/leksummaryMPA%20revised.pdf)(last visited January 4, 2009); *Copy Culture, New York Times* C8 (March 28, 2005); Ipoque, P2P Survey 2006 (October 2006)(available at http://www.ipoque.com/userfiles/file/P2P-Survey-2006.pdf)(last visited January 4, 2009).

47. *See Metro-Goldwyn Mayer Studios, Inc. v. Grokster Ltd*, 545 US 913 (2005). AS a result of the Surpeme Court's decision, the site has been taken down, ending Grokster's income stream from the

In addition to potential advertising fees, many P2P websites also provide a potentially more lucrative funding source in the form of stealth advertising programs (often referred to as "adware" or "gatorware" programs) These programs are often downloaded simultaneously with the "free" P2P software.[48] They place software on the end users computers that allow the software provider virtually unfettered access. While some programs are used to place pop-up advertisements on the end users' screens when s/he keys in certain phrases, other programs may include spyware that can be used to support identity theft (providing access to passwords, bank accounts and any other information the end user may keep on his computer), as well as any number of crimes based on illicit access to information stored or transmitted over the end user's computer. Even licit uses of pop-up advertising programs can be a potent source for funding. Gator Corporation, a US corporation which is one of the most successful marketers of this parallel adware software (called "Gator"), downloaded with such well-known P2P programs as Groskter, and Morpheus reportedly earned $90 million in advertising related activities in 2003.[49] Although there is as yet no direct link to these types of quasi legal software programs and terrorist funding activities, it is only a matter of time before front organizations begin to utilize the global legal loopholes governing such activities to increase their coffers.

Blogs regarding a recent seizure of counterfeit goods illustrates the potential public relations issues law enforcement faces when it seeks to spend limited enforcement dollars on controlling counterfeiting. According to posted reports on the Los Angeles Police Department blog the Los Angeles police, conducting a two day raid on a swap meet and a street market, seized $18.4 million worth of counterfeit designer brand merchandise, including handbags, clothes, sunglasses, shoes and wallets.[50] Even though one of the citizen bloggers mentioned the possible support of terrorism in the discussion board, others questioned the importance of spending any money on counterfeiting, stating: "This is a perfect example of the LAPD's wrong-headed thinking. Knockoff handbags and sunglasses aren't a threat to public safety; there are civil remedies to deal with this problem." [51] Another blogger insisted that those who were buying the counterfeit goods were actually supporting American jobs: "[I]f you're worried about lost jobs, then why are you supporting designer goods? Gucci, Prada and other designer leather goods are

site. See www.grokster.com.

48. *See, e.g.,* Thomas Mennecke, *Grokster Goes From Bad to Worse* (December 16, 2004)(available at http://www.slyck.com/story607_Grokster_Goes_From_Bad_to_Worse)(last visited January 4, 2009).

49. *See, e.g., Guess What?- You Asked For Those Pop-Up Ads* (June 28, 2004)(available at http://www.businessweek.com/magazine/content/04_26/b3889095_mz063.htm)(last visited January 4, 2009). Gator Corporation is now Claria Corporation, and ceased distributing the Gator pop up advertising software in late 2006. Present spyware and adware programs include INF/Autorun, Virtumonde, and Toolbar.MyWebSearch.

50. The designer goods in question were generally Tiffany, Louis Vuitton, Prada, Coach, Bebe, Oakley and Gucci. *Police Seized Counterfeit Merchandise* (May 31, 2006)(available at http://lapdblog.typepad.com/lapd_blog/2006/05/police_seized_c.html)(last visited Januaary 4, 2009).

51. *Id*.

all made in Pakistan and China. The knockoffs are made here in the USA… in fact knockoffs are seized in customs, so that's how you know they have to be made here in the US."[52]

C. Phishing,[53] Identity Theft[54] and other "Low Impact" Crimes

Similar to digital piracy, identity theft and phishing have also proven to be terrorist funding bonanzas, largely for the same reasons that piracy has proven so lucrative.[55] Like digital pirates, successful identity thieves do not need a great deal of technological expertise to succeed. In fact, given the largely unregulated nature of cyberspace on a global basis, identity theft has become big business as foreign criminals use spyware and other stealth programs to obtain personal identifying information from unsuspecting end users. This information is then sold to criminals who actually engage in the fraudulent use of the identities, or terrorist cells who use such fake identities to hide otherwise damaging purchase trails. Thus, the first cell to attack the World Trade Center in New York City in 1995 used fake identities to purchase the fertilizer used to make the explosives in the vans that damaged the towers.[56] Similarly, the terrorists identified as being involved in the attacks of September 11, 2001, had opened 14 bank accounts using several different names, all of which were fake or stolen.[57] According to Dennis Lormel, Chief of the Terrorist Financial Review Group at the Federal Bureau of Investigation, the 2002 bombings in Bali nightclubs was partially financed through on-line credit card fraud.[58] Imam Samudra who was convicted of organizing the bombings later wrote a book in which he included a chapter with instructions on how to commit credit card

---

52. Id.

53. Phishing is generally defined as using spam, shadow websites and other internet or digital based methods for enticing consumers to disclose personal identifying information, often financial in nature, that is then used for illegal or fraudulent purposes.

54. Identity theft is generally defined as using stolen or fraudulently obtained personal identifying information, often financial in nature, in order to obtain funds and other benefits. Phishing is a type of identity theft which uses digital media as the almost exclusive method for obtaining the personal identifying information in question.

55. I do not mean to suggest that digital piracy, identity theft and phishing are the only sources of terrorist funding using the internet. To the contrary, the use of threatened denial of service attacks as a form of internet blackmail has been well-documented as a lucrative source of illicit funds, some of which may be practiced by more technologically sufficient terrorist cells and organizations. I do not mean to denigrate the importance of such crimes. Yet generally, these types of crimes have already attracted the attention of law enforcement. By contrast, the "victimless" crimes I am discussing remain largely under acknowledged and/or underenforced.

56. Brian Koerner, *Terrorist Groups Relying on Identity Theft for Funding and Operations*,(available at http://idtheft.about.com/od/useofstolenidentity/p/IDTheftTerror.htm)(last visited December 5, 2008); See also Bob Sullivan, 9/11 Report Light on ID Theft Issues, msnbc.com (August 4, 2004)(available at http://www.msnbc.msn.com/id/5594385)((last visited January 4, 2009);

57. *Id*.

58. Testimony of Dennis Lormel, Chief, Terrorist Financial Review Group, Federal Bureau of Information, before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information Hearing on S 2541, "The Identity Theft Penalty Enhancement Act (July 9, 2002)[hereinafter "Lormel Testimony"].

fraud. [59] More recently, US and British investigators revealed a funding trail in which three British terrorists use stolen credit cards to set up a network of communication forums and websites that hosted computer hacking and bomb making tutorials as well as videos of beheadings and suicide bombings in Iraq.[60]

Like the estimates of the losses caused by piracy, estimates based on identity theft are problematic to say the least. Yet even examining such figures with a healthy dose of skepticism leads to the undeniable conclusion that unchecked identity theft remains one of the most potent sources of economic losses today for the average consumer, and for the financial institutions that are held liable for such losses. According to the US Postal Service, losses in 2006 due to identity theft in the United States alone equaled more than $5billion.[61] This figure does not even include victims' lost time in trying to correct the financial ruin left behind of their personal financial reputations and credit histories. In October 2004, a year-long investigation by the US. Secret Service revealed a group who created an online hub for identity thieves to buy and sell stolen identity information and stolen credit and debit card numbers. The website, shadowcrew.com, also provided information about how to hack into computers and make fraudulent identity documents. Police estimated that the group, composed of 27 US and foreign members trafficked in at least 1.5 million stolen cards with estimated victim losses in excess of $40 million. [62]

Evidence of terrorist use of identity theft as a funding source, like piracy, is largely anecdotal, but inescapable.[63] A recent study on the relationship between identity theft and terrorism conducted by the Michigan State University Identity Theft, Crime and Research Lab indicates that 5% of all identity thieves in the US are connected to terrorism and 2% were specifically linked to al Qaida.[64].

Phishing, is a new technological version of identity theft which has gained increasing prominence, both as a source of illegal earnings and as a potential terrorist treasure house. Phishing has been generally defined as "a method of identity theft that uses fake emails and bogus websites to entice unwary consumers to disclose financial information. This data is captured and used in financial fraud." [65] Generally the target of a phishing

---

59. Id.

60. Brian Krebs, *Three Worked the Web to Help Terrorists, Washington Post* (July 6, 2007)(available at http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945_pf.html) (last visited January 4, 2009). See also Fundraising for Terrorism: Does Phishing Finance Terrorist?, 60-Second Window (July 8, 2007)(available at http://www.60-seconds.com/2007/07/fundraising_for_terrorism.html)(last visited January 4, 2009).

61. *Identity Theft Losses in the United States* (2006)(available at www.usps.com/postalinspectors/idthft_ncpw.htm)(last visited January 4, 2009).

62. Statement of Laura Parsky, Deputy Assistant Attorney General , US House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security, Legislative Hearing on HR 5318, The Cybersecurity Enhancement and Consumer Date Protection Act of 2006.

63. *See* notes 5, 57, 59 & 61 *supra*.

64. See note 57 *supra.*

65. The Guerrilla Bazaar: Lessons from Phishing Networks (November 15, 2005)(available at http://globalguerrillas.typepad.com/globalguerrillas/2005/11/global_guerrill.html)(last visited January

scheme receives a fraudulent email that directs the recipient to a website where they are requested to provide sensitive personal information (social security numbers, credit card and bank account numbers, passwords etc). While bogus websites generally purport to be from banks and other lawful companies, recent schemes have included claims that the information is being sought by a government agency to assist in the fight against terrorism.[66] With the increased anonymity of the internet, the general inability to effectively combat spam through filtering technologies, and the increased ability to create websites that mirror legitimate websites in appearance, phishing is rapidly being acknowledged as a lucrative funding source for terrorists.[67] Furthermore, because of the generally decentralized self-organization of phishing networks, they make the detection of such networks, and the ability to trace them back to the ultimate beneficiaries of the funding efforts, difficult, if not impossible, to trace.[68] Worse, they have proven readily adaptable, altering their approaches to take advantage of the latest information on corporate vulnerabilities and others' successful exploits.[69]

Despite the growing recognition, even in the trade press, of the use of identity theft, including phishing, by terrorist organizations as a funding methodology, laws governing such crimes remain a patchwork at best. Even in the United States, prosecution for identity theft per se remains limited. No single law governs the crime of identity theft.[70] Instead, such theft is governed by a panoply of state and federal laws, including fraud and consumer deception.[71] Similarly, the investigation of identity theft is left in the hands

---

5, 2009)[hereinafter "Guerilla Bazaar"].

66. *See, e.g.,* Statement from Wayne A Abernathy, Assistant Secretary of the Treasury from Financial Institutions, *Warning About Recent Fraudulent E-Mail Schemes* (January 30, 2004)(available at http://www.treas.gov/press/releases/js1130.htm)(last viewed January 5, 2009).

67. *See* text notes 62 & 63 *supra. See also* Jeremy Simon, The Credit Card Terrorism Connection: How Terrorists Use Cards for Everyday Needs and to Fund Operations, creditcards.com (May 15, 2008) (available at http://www.creditcards.com/credit-card-news/credit-cards-terrorism-1282.php)(last visited January 5, 2009); Tomer Ben Air & Ron Ryan, Terror Spam and Phishing (August 17, 2007) (available at http://www.crime-research.org/articles/Terror-Spam-and-Phishing)(last visited January 5, 2009).

68. *See* Guerilla Bazaar *supra* note 66.

69. *Id*.

70. Diverse federal statutes currently deal with some aspect of identity theft, including Section 1028 of Title 18, directed toward the knowing transfer, possession, use or production of stolen or false "identification documents" or "authentication features," which includes non-governmental issued identification means, so long as they are "intended or commonly accepted for the purposes of identification of an individual…" 18 USC §1028(d)(4). The statute was amended in 2000 specifically to prohibit electronic transfers of such false documents or document making facilities. See Internet False Identification Act of 2000, codified at 18 USC 1028 (a)(1)&(2). Efforts to enact a federal law governing phishing remain ongoing. Most recently, SR 2661 was introduced in February 2008. Referred to as the Anti-Phishing Consumer Protection Act of 2008, SR2661 would establish jurisdiction for bringing federal suits for phishing in the Federal Trade Commission and would also authorize state authorities to bring local civil suits as well. It is too soon to tell whether the bill will ultimately be enacted, or what its final terms will be.

71. Thus, for example, the thief may be prosecuted for misrepresenting himself to his financial victims under state criminal fraud statutes. Such prosecutions generally would not be based on the illegal acts undertaken to assume the stolen identity, but on the use or attempted use of the identity in question.

of state and local police who generally prefer to spend their resources investigating and prosecuting economic crimes of a perceived greater magnitude, such as burglaries and bank robberies. Like piracy, identity theft is perceived to be an economic nuisance for credit card companies and others who extend credit based on the false information. Until recently, it was generally perceived as being a relatively low impact crime whose victims bore part of the blame for their own victimization. While phishing enterprises may earn large amounts of money with relatively little capital,[72] the loss per victim remains relatively small. Unlike digital piracy, however, the simple nuisance impact of phishing, particularly since it is tied to spam, may explain recent increasing attention by law enforcement, at least in the form of greater efforts to provide the legal infrastructure necessary to begin to combat the problem.[73]

ii. fixing the legal void

The internet, by its very nature, is an international communication medium. Yet the identified problems of digital piracy and identity theft remain largely unaffected by international treaty regimes. The premiere agreement on the international enforcement of intellectual property rights—the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)—was created at a time when the internet was largely perceived as a pure communications medium. Thus, despite its lengthy provisions regarding the "effective enforcement" of intellectual property rights, including "fair and equitable" procedures which all signatories must apply,[74] TRIPS did not directly address the problems of enforcing intellectual property rights on the internet. While Article 61 requires that signatories prosecute willful copyright violations (piracy) with "effective" laws that include criminal penalties which are deterrent,[75] the reality is that even those countries who are signatories to TRIPS provide relatively slight penalties for even hard goods piracy. Even those penalties are infrequently applied so that piracy becomes a "safe" harbor for illegal fund raising. [76] Moreover, while the WIPO Copyright Treaty requires that technological protection measures ("TPMs") applied by copyright owners be protected under a legal framework that allows for both civil and criminal penalties

72. According to a report issued by Garnter Inc in 2007 alone approximately 3,500,000 computer users were victims of phishing with aggregate losses totaling approximately $3.2 billion. See Gartner Survey Shows Phishing Attacks Escalated in 2007 (December 17, 2002)(available at http://www.gartner.com/it/page.jsp?id=565125)(last visited January 4, 2009). This study was relied as part of the impetus for the present attempt to enact a federal law designed to attack the problem of phishing directly. See The Anti-Phishing Consumer Protection Act of 2008, SR2661, Section 2(4).

73. While no federal statute directed specifically to phishing has been enacted as of the writing of this article, numerous states have begun to enact local statutes to fill the gap. For a survey of the most recent state statutes, see National Conference of State Legislatures. 2007 State Legislation Relating to Phishing (available at http://www.ncsl.org/programs/lis/phishing07.htm)(last visited January 4, 2009).

74. Trips, Art. 41.

75. Trips, Art. 61.

76. *See* Special 301 Reports for diverse years (available at www.ustr.gov)(last visited January 4, 2009) (detailing the lack of effective enforcement of copyright laws in diverse countries).

for those who violate such TPMs,[77] the treaty itself has only attracted 68 signatories to date.[78]

If piracy at least has a potential international legal framework on which a harmonized standard of enforcement might be achieved, phishing and identity theft are completely lacking in any such international standard. No international treaty even provides the framework for combating such crimes. Instead, we are left with a patchwork of domestic laws which have been adopted by relatively few countries.[79]

A. The United States

Because of the perceived greater impact that counterfeiting and piracy have on US industries—including its music, film and software industries, the United States has strong civil and criminal federal laws prohibiting hard goods and digital piracy.[80] Recent efforts by the US to strengthen its enforcement efforts include the adoption of new governmental methods to combat piracy and counterfeiting through such interagency efforts as STOP, which includes increased coordination between Customs and police to stop illegal goods at the border and the creation of an "Intellectual Property Enforcement Coordinator" serving in the Executive Branch who will head a multiagency strategic task force with regard to both domestic and international intellectual property enforcement issues.[81] These efforts are largely directed to the hard goods world.[82] While the laws are in place, federal prosecution of piracy has been relatively sporadic. DOJ website review of cybercrimes prosecuted by US attorneys indicate relatively few piracy cases are brought and those usually involve additional crimes such as pornography which has gained the DOJ's attention.[83]

---

77. WIPO Copyright Treaty, Art. 12.

78. The efficacy of TPMs as protective devices for combating digital piracy remains doubtful. See, e.g., Doris Estelle Long, Is a Global Solution Possible to the Technology/Privacy Conundrum,?, 4. Marshall Rev. Intell. Prop. L. 6 (2005)

79. I chose US, India and the United Kingdom for comparison purposes because (1) they are English speaking countries for whom access to materials is easier; (2) they have a level of technological development that makes phishing and digital piracy relatively potentially accessible crimes, and (3) all three countries have faced terrorism and should therefore be considered more sensitive or at least interested in discovering and stopping funding of terrorist activities.

80. *See, e.g.*, 18 USC §2319 (providing strong criminal penalties for copyright piracy without requiring commercial advantage or financial gain); §2319A(providing strong criminal penalties for creating, reproducing or transmitting bootleg recordings);§2319B(providing criminal penalties for unauthorized reproduction of audiovisual works being performed in a motion picture exhibition facility) & §2320 (providing strong criminal penalties for trademark counterfeiting).

81. *See* PRO IP Act of 2008, Section 301.

82. While the responsibilities of the new Intellectual Property Enforcement Coordinator is not limited to the hard goods world, given the agencies involved in the multi-agency task force, including those of the Food and Drug Administration, the Department of Agriculture and the US Trade Representative, it appears that most efforts will be directed toward the problems of hard goods protection, at least initially. See PRO IP Act of 2008, Section 301(3).

83. *See generally* www.usdoj.gov/criminal/cybercrime/reporting.htm (last visited January 4, 2009). *See also* www.stopfakes.gov (last visited January 5, 2009). With the increased attention paid to piracy and counterfeiting as demonstrated by the recently enacted PRO IP Act of 2008, *see* notes 82 – 83 *supra*, it is likely that federal prosecutions for piracy will increase in the future.

By contrast, there is currently no federal law which punishes phishing, per se,[84] although the federal Can Spam Act can be used to attack the fraudulent spam that lies at the heart of most phishing schemes.[85] In addition, federal trademark law has been used successfully to challenge spam on the grounds of its failure to adequately disclose the source of the email in question. Thus, in the use of a false return email address by an email "spam" operation qualified as a false designation of origin and dilution of Hotmail's trademark.[86] Most identity theft, however, is prosecuted at the state level so that state criminal statutes against fraud may be applied and are usually based on individual filed complaints. Unfortunately, prosecutions remain infrequent. Post 9/11, however, federal laws concerning the knowing possession, use or transfer of false federal identification documentation, including social security numbers, in various illegal and fraudulent schemes, including wire transfers, have been enacted which provide for substantial criminal penalties. For example, under the Identity Theft Enhancement Act of 2004 penalties for the use of such illegal documentation were enhanced in connection with a broad panoply of federal crimes, including the use of false documentation to commit state felonies.[87] Under the Identity Theft and Assumption Deterrence Act, knowing transfer or use of a means of identification of another person with the intent to commit, or aid or abet any unlawful activity that constitutes a violation of federal law…includes obtaining anything of value totaling $1,000 or more during a one year time period.[88] Strong penalties include potential prison terms up to 15 years, and, if committed to facilitate an action of international terrorism, up to 25 years.[89]

B. The European Union

There is currently no European Union Directive or regulation regarding criminal piracy enforcement even though piracy remains a concern throughout much of the EU. While the EU has recently enacted an IP Enforcement Directive establishing civil procedures for the prosecution of intellectual property infringements, including those involving copyright,[90] the Directive has been harshly criticized. Moreover, this Directive does not address the critical problem of criminal piracy enforcement. Efforts to create any Union

84. *See* note 71 *supra.* While there is no federal phishing statute, several states have recently enacted laws directed specifically to the problem of phishing. See generally National Conference of State Legislatures. 2007 State Legislation Relating to Phishing (available at http://www.ncsl.org/programs/lis/phishing07.htm)(last visited January 4, 2009).

85. Can Spam Act, 15 USC §§7701 – 7713 & 18 USC §1037.

86. *Hot Mail Corp. v. Vans Money Pie Inc.*), 47 U.S.P.Q. 2d 1020 (N.D.Cal. 1998). S*ee also America Online, Inc. v. IMS*, (E.D.Va. 1998) (improper spam mailing held to tarnish plaintiff 's mark because of use of "aol.com" on the header led to 50,000 subscribers' complaints)(available at http://legal.web.aol.com/decisions/dljunk/imsopin.html)(last visited January 5, 2009). Spam can also be challenged under various state statutes, *see e.g.,* Cal. Bus & Prof. Code § 17538.4. *See also* Can Spam Act, supra note 86.

87. 18 USC §1028.

88. *Id*.

89. *Id*.

90. EU Directive on measures and procedures to ensure enforcement of intellectual property rights, 2004 OJC 63 (February16, 2004)(available at http://eu.europa.org)(last visited January 5, 2009).

wide directive on criminal IPR enforcement remain problematic.[91]

There is also no current European Union directive or regulation which expressly addresses identity theft or phishing.[92] There are, however, several directives and regulations that have proven helpful in combating identity theft, based on consumer protection concerns. Thus, for example, the Consumer Protection Cooperation Regulation establishes a useful model for the sharing of information and enforcement efforts to combat "intra-Community infringement."[93] The Regulation defines covered infringements as "any act or omission contrary to the law that protect consumers' interests" when the act or omission, the seller or supplier, or "evidence of assets pertaining to the act or commission" are found in more than one Member State.[94] An Appendix which is periodically updated lists the relevant consumer protection statutes which are covered by the Cooperation Regulation. These directives cover such diverse subjects as misleading advertising, unfair terms in consumer contracts, e-commerce and the distance marketing of consumer financial services. Unfortunately this cooperation directive is limited to cooperation among EU member countries.[95]

C. The United Kingdom

In 2006 the UK enacted The Fraud Act of 2006, which entered into force on January 15, 2007.[96] The Act was specifically designed to provide the tools necessary to combat phishing. Itcovers diverse types of criminal fraud, including fraudby false representation, by failing to disclose information, and by abuse of position.[97] Section 2, dealing with fraud by false representation, specifically provides "a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)."[98] It is too soon to tell whether the new act will be strongly enforced or will lead to a reduction in phishing activities but it may serve as a model for other EU

---

91. Report on the amended proposal for a directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectualproperty rights (March 3, 2007) (available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2007-0073+0+DOC+PDF+V0//EN)(last visited January 5, 2009).

92. The European Commission has established a working group and is currently working on proposed draft directives to deal with both identity theft and phishing. As of the date of this Article, no draft laws have yet been publicly circulated. *See* Tim Ferguson, The EU Wages War on Cybercrime (May 24, 2007)(available at http://news.cnet.com/EU-wages-war-on-cybercrime/2100-7348_3-6186464.html?tag=nw.1)(last visited January 5, 2009); Nicole van der Meulen, The Spread of Identity Theft: Developments and Initiatives within the European Union (May 2007)(available at http://policechief-magazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1190&issue_id=52007)(last visited January 5, 2009).

93. Consumer Protection Cooperation Regulation, Art.3(b)(available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2006:EN:NOT (last visited January 5, 2009).

94. *Id*.

95. Id.

96. The UK Fraud Act of 2006 *reprinted in* Blackwell's Statutes (Oxford University Press 2007).

97. *See* Fraud Act 2006 at Sections 1-3.

98. *Id* at Section 2(5).

and/or common law countries.

D. India

India has consistently been cited for failing to have strong IPR enforcement efforts against pirated and counterfeit goods. Although it has recently revised its copyright laws to provide for longer potential terms of imprisonment in the face of a piracy conviction,[99] enforcement efforts remain woefully inadequate. Such inadequacy includes a failure to protect the works of local film producers, despite the undeniable economic impact on "Bollywood" of such failures. In discussions with directors and producers of Telagu films during a recent trip to India, I was advised that the lack of adequate sales through legitimate marketing channels has slowly reduced the number of films being produced. The reasons given for inadequate enforcement include the same issues that are generally raised: lack of funds, lack of training, too many other crimes to police; and, occasionally, lack of consumer harm because they can get goods more cheaply than through the legitimate goods market.

As internet penetration has increased in India so too has the use of the internet in identity theft activities. In 2005, despite the absence of any nation-wide or province-wide laws directed specifically to phishing the Delhi High Court upheld a civil judgment against a phishing network based on fraud and misrepresentation. The decision in National Association of Software and Services Companies v Ajay Sood & Others was heralded as a significant achievement. In the case, defendants were purportedly operating a job placement service and used spam in NASSCOM's name to elicit personal information for fraudulent purposes. Ultimately the defendants settled the case by admitting liability and paying damages of Rs 1.6 million (approximately $35,556) to the plaintiffs.[100] While the case has been touted as a victory in the fight against spam and phishing in India,[101] and clearly held that use of another's name to secure information was illegal, its reasoning was based on passing off and source confusion analysis and not on the illegality per se of obtaining or using falsely obtained information.[102] It is not clear to what extent other courts may consider themselves bound by the Delhi High Court or may follow its willingness to find phishing illegal despite the absence of specific legislation. Efforts to update India's 2000 Information and Technology Act

99. India Copyright Statute, Art. 63A (available at http://copyright.gov.in/cpract.doc)(last visited January 5, 2009).

100. National Association of Software and Services Companies v. Sood (available at cybercrimes.blogspot.com/2007/02/nascom_sood.htm)(last visited May 31, 2007). See also Talwant Singh, Cyberlaw and Information Technology (2007)(discussing the NASCOM v. Sood decision)(available at http://delhicourts.nic.in/CYBER%20LAW.pdf)(last visited January 5, 2009).

101. *See, e.g.* Dijeet Titus & Sumit Roy, *Phising on the Net* (available at Asialaw.com)(last visited December 30, 2008).

102. This reliance on trademark based principles to combat spam has also been used successfully in the United States. *See, e.g.*, *American On Line v. IMS*, *supra* note 87. Such source confusion principles are useful in challenging the spam used in phishing schemes and should be applicable to shadow sites created in furtherance of such schemes. They do not however reach the harm caused to those whose identities have been used without their knowledge or consent.

continue with the hopes of improving the legal infrastructure for phishing prosecutions. Yet the most recent amendments to Section 66 (involving computer related offenses) do not appear to cover acts relating to misrepresentation, which is at the core of the Delhi's courts decision.

The Information and Technology Act of 2000 prohibits diverse computer related activity, including tampering with computer source code, [103] hacking,[104] and the electronic publication or transmission of obscene materials.[105] It provides for criminal penalties, including "confiscation of the computers, computer system, floppies, compact disks, tape drivers or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened."[106] The Act does not expressly reach spam, unauthorized computer systems intrusions, shadow websites, or even fraudulent activity using computers or computer systems. Amendments to the Act were passed by the Parliament in its last session in December 2008. Included among the amended passages is a new Section 66C which provides criminal penalties against anyone who " fraudulently or dishonestly make[s] use of the electronic signature, password or any other unique identification feature of any other person.."[107] Section 66C provides criminal penalties for "cheating by personation" "by means of any communication device or computer resource."[108] These amendments should provide the necessary statutory basis for identity theft prosecutions that were previously lacking in the 2000 Act.

Most phishing activities in India currently involve fraud involving Indian and multinational banks. Like other countries, the figures on phishing are increasing in India. Figures released by Computer Emergency Response Team indicated an increase from 86 incidents in 2005 to 200 incidents in 2006. Moreover, the attacks are not all launched in India. To the contrary, most phishing attacks were launched from other countries. [109] Given the new provisions that provide a statutory basis for identity theft and phishing challenges,[110] the 2000 Information and Technology Act has the potential to reach these activities so long as the impacted computer is located within India. Section 1(1) of the Act provides: "It [the Act] shall extend to the whole of India and, save as

103. The Information and Technology Act of 2000, Art. 65 (available at http://www.naavi.org/important laws/itbill2000)(last visited January 5, 2009).

104. *Id* at Art. 66

105. *Id*. at Art.67. It also contains provisions that protect digital signatures and other trust systems.

106. *Id.* at Art. 74.

107. The Information and Technology Act of 2000, as Amended in December 2008, Section 66C (available at http://www.naavi.org/ita_2008/index.htm)(last visited January 5, 2009).

108. Id. at Section 66D. The amendments were extensive and included a newly defined crime of "cyberterrorims," id. at Section 66F, as well as new provisions granting the government enhanced right to intercept, monitor and decrypt "any information transmitted received or stored through any computer resource." Id. at Section 69.

109. *Phishing in People's Accounts*, www.cbncwatch.com (last visited December 30, 2008)). *See also* Phishing Incidents in India Grow By 180% (May 2, 2007)(available at http://www.spamfighter.com/News-7677-Phishing-Incidents-in-India-Grow-By-180.htm)(last visited January 5, 2009).

110. *See* notes 108 & 109 *supra*.

otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person."[111] It was not altered or amended.

iii. reducing the cyber safety net: a multi-disciplinary approach

Pirate and phishing networks are international in nature and fact. Spam activity remains largely unregulated around the globe, as does the sale of personal identifying information for use in identity theft schemes. While the United States, the UK and India all evince varying levels of conscious enforcement against such illegal activity, they are by far in the minority. Most countries either lack the necessary legal structure to criminalize (or at least prohibit) piracy and identity theft, including phishing, or lack the willpower to dedicate funds to combating such problems. It is no surprise to discover that most reported prosecutions in London and the US involving phishing networks found perpetrators located beyond their borders, in countries where phishing is unregulated.

To reduce the cyber safety net for terrorist funding activities a multidisciplinary, transborder approach should be developed directed to these "victimless" and "low impact" crimes. This approach requires more than simple transborder cooperation, It requires a new *international* approach to the treatment of digital piracy, phishing and identity theft prosecutions.

As a first step, greater empirical data is needed to demonstrate the link between terrorist funding and the perceived low priority crimes of digital piracy and identity theft. Such data would not only support stronger governmental intervention, it would help raise public awareness of the need for such intervention. Enforcement cannot end on seizure of counterfeit goods or the take down of a spooked website. Instead, efforts *must* be made to trace the funds and the operators of the affected websites. Such efforts will not only provide the necessary evidentiary support of the relationship between these "low impact" crimes and terrorist funding, they will help dry up such funding

Public education programs must be designed to take away the glamour of piracy. This does not mean that the terrorist link becomes the latest unproven tag line to change social conduct regarding piracy and identity theft. Telling consumers that the counterfeit purse they are buying funds terrorist activities does not help alter public conduct without the hard facts to support such claims. Those hard facts must go beyond a few anecdotes or the old adage of "crying wolf" will become a sad reality. In addition to educating the public about the link between these crimes and terrorist funding, public programs must also make consumers aware of the dangers of piracy and identity theft,[112] as well as the steps they need to take to protect themselves.

---

111. The Information and Technology Act of 2000, as Amended in December 2008, Section 1(1) (available at http://www.naavi.org/ita_2008/index.htm)(last visited January 5, 2009).

112. Too often pirated goods lack the quality control or security of legitimate products. Thus, pirated software may contain viruses, while counterfeit goods often contain contaminated and sometimes physically harmful ingredients.

Enforcement activities directed to the tracing and securing of funding obtained from piracy and identity theft must be put on the security agenda, so that money and will power are directed to their successful prosecution. This requires capacity building directed toward creating the necessary infrastructure to support such activities. The legal infrastructure, including model laws and international treaties governing identity theft, must be created. While individual domestic efforts such as those discussed in this Article are important, unless an international enforcement platform is created, terrorists will be able to continue to use the cyber safety net by simply moving their criminal activities to a home base that lacks the necessary infrastructure to stop them.

In addition to model laws prohibiting identity theft and phishing, stricter penalties for piracy and counterfeiting are needed internationally to assure that prosecutions result in effective deterrence. Evidentiary rules must be developed internationally that will allow both the seizure of computer evidence as well as the use of computer forensic evidence in prosecutions. A mechanism for providing funding and appropriate personnel must be developed to assist in the training of enforcement personnel, not just in techniques of investigation and prosecution, but also in the significance of the crimes at issue to the overall goal of reducing sources for terrorist funding. Since the digital environment is constantly changing in response to technological advances, law enforcement must develop new information-sharing models to allow them to stay ahead of the technology curve in this area. The information nets that permit hackers and others to share the latest methods for breaking encryption codes (for example) must be equaled for law enforcement or the technological arms race behind these crimes will be lost regardless of the legal infrastructures in place.

This need for better information nets for law enforcement personnel does not stop at technology sharing. To the contrary, in addition to the creation of the legal infrastructure to support heightened enforcement in this area, perhaps the most critical requirement is the development of new cooperative mechanisms for enforcement. Given the international nature of the groups that are engaged in these crimes, domestic efforts, no matter how well intended, will not be sufficient to close the cyber safety nets. Only well coordinated, international efforts will be sufficient. This requires not only sharing of information across borders, it requires the establishment of international strike forces dedicated to these efforts. Such strike forces must include personnel to provide legal, technical, enforcement and security support so that efforts can be coordinated with other efforts directed to combat terrorism. Information regarding piracy and identity theft must not simply be shared among domestic agencies. It must be shared across borders. Unless law enforcement personnel become as effective at conveying information and coordinating activities against these crimes as the terrorists are, the cyber safety net for funding will remain and grow.

As a first step, in addition to creating teams to begin to coordinate efforts in this area, mutual legal Mutual Legal Assistance Treaties (MLATs) directed to piracy and identity theft should be created. The European Union Regulation on Consumer Protection

Cooperation[113] establishes a useful model for the sharing of information. Such ideas should be put in place now, before more time passes, and more funds slip through the cybersafety net.

conclusion

While the internet may continue to be viewed in popular imagination as a wild frontier where law does not apply, it cannot continue to operate without regulation in fact. Lack of attention has allowed a cyber safety net to develop which allows terrorists and criminal organizations to raise funds and launder money gained through digital piracy and identity theft with little fear of prosecution. The high yield, low threat combination makes these potent funding sources. Securing the cyber safety net requires concerted multinational efforts. The legal and enforcement infrastructure for closing this net must be created on an international basis. Such efforts will not only require enhanced levels of transborder coordination, including information networking, they will require new modes of acting and a dedicated effort to secure public support for such activities. It will take time to develop the necessary support system for this multidisciplinary approach to the problem. This is not about the private harm caused by digital piracy, identity theft or phishing, which is substantial. It is about public security. The time to initiate the proposed multidisciplinary approach is now, before the cyber safety net becomes so securely entrenched it cannot be breached, even for an issue as critical as the reduction of terrorist funding. Yet while we are creating the necessary infrastructure and mechanisms to begin to secure this safety net, we must also be mindful of the need to craft solutions that take into consideration individual rights and information access concerns. The need to secure the cyber safety need is real. But the efforts to combat the crimes that support terrorism must be applied surgically and not as a blunt instrument or public support for such activities, and the necessary will to secure the safety net will rapidly diminish, placing public safety in an even more tenuous position than today's unfortunate era of under enforcement.

113. *See* note 94 and text *supra*.