PASSWORD THEFT: RETHINKING AN OLD CRIME IN A NEW ERA

DANIEL S. SHAMAH

GEORGETOWN UNIVERSITY LAW CENTER

TABLE OF CONTENTS

Introduction

We live in a world of passwords. We use them for everything: to access our e-mail and credit cards; to read content on LexisNexis and ESPN.com; to chat with our friends on America Online and Yahoo!. We have so many of them, it can be easy to forget which password belongs to which service. Because of their ubiquity, we also tend to reuse our passwords. The password to access my e-mail, for instance, is the same password I use to access LexisNexis. The ubiquity of passwords, however, has given rise to an entire criminal enterprise focused on acquiring them. Criminals reason, rightly so, that if they have acquired one password, they have access to much of what you do. Consequently, security experts have suggested for years that to increase security, computer users should vary their passwords frequently, and use different passwords for different services.[1] Few take this advice. In a world built on access and information, the password has become the ultimate skeleton key.

While stealing passwords is not a new crime, in the world of Internet theft, it has taken on new dimensions. In general, identifying the victim of criminal behavior on the Internet has become increasingly difficult. Traditional notions of criminal deterrence—from both economic and sociological perspectives—have become skewed in a world where even the criminal does not necessarily know who he is criminalizing.[2] The anonymous nature of the Internet, where the identity of criminals can be obscured, and the identity of the victims is often unknown even to

[1] *See*, *e.g.*, *Password Usage Guidelines*, THE UNIVERSITY OF TORONTO COMPUTING AND NETWORK SERVICES, www.utoronto.ca/security/UTORprotect/passwd.htm (last visited Aug. 16, 2005).

[2] *See* Gary Becker, *Crime and Punishment: An Economic Approach*, 76 J. POLIT. ECON. 69 (1968) (analyzing criminal behavior from an economic perspective); Michel Foucault, DISCIPLINE AND PUNISH (1975) (a sociological perspective on criminal behavior).

the criminals, has elicited proposals from both scholars and law enforcement.[3] The threat of stealing a password—a sequence of digits that may contain access to an individual's entire life savings and private thoughts—has given these concerns a heightened sense of urgency.

In late 1999, the world got its first glimpse on a mass scale of the difficulties Internet crime poses. Napster, with access to millions of Internet users who had billions of directories containing countless amounts of copyrighted material, created the world's largest marketplace for music theft. The astonishing feature of the Napster revolution, however, was not just its sheer size; it was the kind of people involved. College students, who otherwise would not shoplift a candy bar, engaged in widespread copyright theft, rationalizing their behavior on a variety of factors. While many griped about the expense of albums, the ease of access, or the effect of peer pressure, the fundamental issue was quite simple, if unstated: no one thought it was a crime. Put bluntly, copying your friend's music files was widely considered victimless, harmless.

Five years later, there has been an astonishing turn around in the public perception of music downloading. According to a recent study, legal music downloading has tripled, while illegal downloading has grown at a far slower pace.[4] A 2004 Pew survey showed that illegal music downloading is on the decline.[5] Something has happened between 1999 and the present that has changed people's minds about music downloading. What was once an acceptable action, committed by almost every college and high school student with a high-speed Internet connection, is now viewed by millions as criminal.

---

[3] *See generally*, Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001); Lawrence Lessig, CODE, 46-7 (1999).

[4] E-CommerceTimes.com, *Study: Legal Music Downloading Triples Worldwide* (2005), http://www.ecommercetimes.com/story/44871.html (last visited Aug. 16, 2005).

[5] Techweb.com, *Survey: Illegal Music Downloading Declines*, http://www.techweb.com/wire/26803753 (last visited Aug. 16, 2005).

Clearly a part of what happened in the Napster story is that people began to view the act of downloading music freely as illegal. A significant part of this was accomplished by shifting victimhood—instead of thinking of it as harmlessly taking the music from someone's computer, people began to think of music downloading as stealing directly from the record companies. By putting themselves out in front as the victims, the Recording Industry Association of America (RIAA) helped reshape the governing norms of the times, and as a result, people viewed the act of file-sharing differently. [6] By forcing people to see music downloading as a form of theft, the RIAA was quite successful in deterring it. In the process, they also proposed a radical view of theft that changes our basic economic understandings of the action.

The Napster story serves as a useful template for thinking about password theft. If Tom steals Mary's password to access her LexisNexis account, there are two possible victims: Mary and Lexis. At first glance, we would probably say Mary is the primary victim, but that is not altogether clear. After all, Tom would probably argue that Mary can still access LexisNexis even as he is using her password. And even if Lexis were to design their software so that each password can only log on once, depriving Tom and Mary of simultaneous use, Tom is likely to argue that he is not really harming Mary because he is only depriving her of the short period of usage when he is online: the deprivation is not permanent. This problem is further complicated if rather than stealing her Lexis password, Tom borrows it from Mary with her permission. In this case, Mary is no longer a victim, she is a co-conspirator, and the real victim has become even further obscured. If we think of LexisNexis as the victim in both scenarios, however, the answer becomes clearer: in both cases Tom's actions were criminal, and Mary was his co-criminal in the second scenario.

[6] *Cf.* Katyal, *supra* note 3, at 1033 (arguing that harnessing third parties, like credit card companies, can make music theft less profitable and thereby deter it).

This paper argues that the RIAA's model for deterring music theft could be successfully used to deter many other forms of computer theft, and, specifically, stealing passwords. By focusing on the victim, content-providers can alter people's views of their actions, thereby properly bringing what was once an innocuous activity into the realm of the criminal where it belongs. To accomplish this task, however, we have to comport our traditional views of theft to the realities of the Internet. First, economic notions of rivalry and nonrivalry are undermined in a digital world where data is infinitely copyable, and these notions need to be updated appropriately. Secondly, finding real space analogues to password theft is important in locating an existing legal framework with which to work. This Note attempts to do both.

Part I of this Note gives a brief background and explication of rivalrous and non-rivalrous theft, and the problems that the Internet poses, specifically in the music downloading area. In so doing, I propose a new way of conceiving of rivalry that fits into the realities of digital networks. Part II is an analysis of password theft, in particular the distinction between first-party and second-party password theft. First-party password theft concerns actions—stealing personal identification numbers and the like—that are probably familiar to most readers. Second-party password theft, however, is a far more radical notion that is crucial for understanding why password theft in general is criminal, and why it can be so damaging. I analogize first and second-party password theft to larceny and embezzlement, respectively; the purpose of this is to provide a legal framework for analyzing password theft as a criminal activity. Additionally, I show how the updated views of rivalry proposed in Part I allow us to evaluate properly the harm that password theft causes. Finally, Part III argues that by following the model of the RIAA, the government, content-providers, and law enforcement can effectively deter password theft in a variety of ways.

I. Rivalrous versus Non-Rivalrous Theft

Economic theory distinguishes between two forms of theft: rivalrous and non-rivalrous.[7] Rivalrous theft is traditionally understood as theft that deprives the victim of using whatever it is that was stolen. So if John steals Frank's car, the theft is rivalrous because John has taken the car and deprived Frank of its usage. Non-rivalrous theft is theft that does not deprive the victim of any usage. The classic example of non-rivalrous theft is information. If Tom tries to sell information, and Frank steals it, theoretically he is not depriving Tom of selling just as much information as before. The theft, in other words, causes no depletion.[8] The two models of theft therefore reflect two forms of goods: those that deplete and those that do not.

Concordantly, theft that is not rivalrous, under the common law, is not theft.[9] The traditional laws regarding theft always required some form of permanent deprivation, whether the theft was characterized as larceny or embezzlement.[10] Unauthorized use of information is usually protected by copyright or intellectual property laws designed to encourage innovation

---

[7] For a general introduction, *see generally* David A. Besanko & Ronald R. Braeutigam, MICROECONOMICS 749 (2002).

[8] *See* James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 L. & CONTEMP. PROBS. 33, 41 (2003) ("By contrast, a gene sequence, an MP3 file, or an image may be used by multiple parties; my use does not interfere with yours. To simplify a complicated analysis, this means that the threat of overuse of fields and fisheries is generally not a problem with the informational or innovational commons"); *see also* Robert P. Merges et. al., INTELLECTUAL PROPERTY IN THE NEW TECHONOLOGICAL AGE, 13 (2d ed. 2000).

[9] *See*, *e.g.*, Kansas v. Allen, 917 P.2d 848, 853 (Kan. 1996) ("Theft...is not concerned with mere occupation, detention, observation, or tampering, but rather requires permanent deprivation. The intent required for theft is an 'intent to deprive the owner permanently of the possession, use, or benefit of the owner's property'").

[10] William R. LaFave, CRIMINAL LAW, §§ 19.2, 19.6 (4th ed. 2003).

while preventing usurpation of ideas and free-riding.[11] So if Frank photocopies Tom's book and attempts to sell it as his own, his actions are criminalized by copyright law, not the traditional laws of theft, because, theoretically at least, Tom has not been deprived of anything—he can sell just as many books as he had before. In contrast, if Frank walks into a bookstore and steals Tom's book from the store, his theft has deprived the bookstore of a book it could have sold. Because the law recognized the important public good that information represented, goods that do not deplete with theft—like information—are not accorded the same level of protection as goods that do deplete with theft.

In a digital world, however, this dichotomy begins to find itself on shaky ground, as it becomes unclear who the law is supposed to protect. In real space, information can easily be protected by copyright law, because it is readily apparent whom we are protecting—the innovators, creators, and disseminators of that information. Digitization, however, has allowed information to be replicated and disseminated faster and wider than ever before. Buying and selling information is no longer prohibitively expensive, and copyright law has proven insufficient in protecting holders.[12] Furthermore, on digital networks it is harder to determine who owns the copyright. In real space, when a consumer purchases a book or CD, the copyright owner's mark is stamped on the product, and the consumer readily recognizes ownership of the copyright.[13] The protection that the law accords to copyright material in this setting is therefore lower than that accorded to rivalrous goods. On the Internet, however, the copyright owner is not readily apparent; information appears as anonymous digital files that may not bear any mark or

[11] *See*, *e.g.*, Mark A. Lemley, *Property, Intellectual Property, and Free Riding*, 83 TEX. L. REV. 1031 (2005).

[12] *See* Katyal, *supra* note 3, at 1031-32.

[13] *See* Jane C. Ginsburg et. al., TRADEMARK AND UNFAIR COMPETITION LAW 45 (3d ed. 2001). As Ginsburg points out, one purpose of trademark law is to aid in consumer identification.

distinguishing feature, and users have no easy way of determining who owns that particular file, let alone the copyright. The real space level of protection accorded to copyrighted material is not sufficient in this environment.

What actually happened in the Napster story was a profound shift in an understanding of rivalrous versus non-rivalrous theft. From a traditional standpoint, downloading music should be viewed as non-rivalrous theft—when Tom downloads music off of Frank's computer, he never deprived Frank, or anyone, of listening to that song or purchasing that song. Theoretically, just as many songs could be purchased after the download. The trouble with this construction is that it views Frank as the victim, when in reality he is hardly a victim; if anything, by making his music available on his computer, Frank is an enabler.[14] When Napster took off, this question of who the victim was had no apparent answer, and that in large part fueled Napster's popularity: music downloading, because of its non-rivalrous nature, was viewed as a victimless crime. However, just because Frank is not the victim, it does not mean there is no victim in the music downloading area. Indeed, music downloading is non-rivalrous with respect to the computer from whom the user is downloading. But what the RIAA convinced people of was that *music downloading is rivalrous theft with respect to copyright holders and the RIAA*. An act of theft, in

---

[14] At this point, a brief primer on online file sharing may be helpful. On Napster and peer-to-peer music networks, music is made available by users placing their files in a designated directory—a shared music directory. Other computers log onto the network, and when searching for a desired song, can scan that specific directory during its query. When the searching computer finds a desired song, it then links to the destination computer and can download the song directly off of the other computer.

The above structure only works, however, if people are willing to put music into shared directories—if Tom downloads music onto his computer, and immediately moves the files into another non-shared directory where other computers cannot access them, he undermines the network. Consequently, many peer-to-peer networks search for ways to encourage users to share their music: tactics include rating systems based on the number of files shared, or offering different levels of accessibility based on the number of files shared.

The RIAA recognized that there is therefore a fundamental distinction between uploaders and downloaders: without the uploaders, there would be no network. Consequently, instead of targeting their lawsuits towards downloaders, it began to target lawsuits more at those who upload, characterizing them as enablers in criminal activity. The uploaders are a chokepoint—stop them, and the network fails.

this case music downloading, can be simultaneously rivalrous and non-rivalrous, depending on the point of view adopted.

This notion seems paradoxical at first glance: how can a single action be both non-rivalrous and rivalrous at the same time? Those descriptions are objective, and should not need to take into account other factors like points of view. But it actually makes perfect sense. Compare music downloading to stealing an actual compact disk in real space. Tom walks into Tower Records and steals a CD. Under elementary economics, Tower has been deprived of a CD, while Tom has the CD without having paid for it: it is rivalrous theft with respect to Tower. But suppose five minutes after Tom stole the CD, Mary walks into Tower looking for the exact same CD. If Mary complains about Tom's theft because that CD is now out of stock and she has to walk down the block to another record store, she has no redress under the law, because Tom's theft with respect to her is non-rivalrous. Even though Tom's action has indirectly and minimally affected her, the theft is still non-rivalrous, as it has not permanently deprived her of anything and it has not impaired her interests in any significant way. Tom's theft is therefore simultaneously rivalrous and non-rivalrous, depending on the point of view adopted and who we think the victim is.

The same is true with respect to music downloading. When Tom downloads music off of Frank's computer, he has not deprived Frank of anything, even though his actions may indirectly impact him.[15] Tom's actions, however, are not non-rivalrous to everyone in the universe: the

[15] Perhaps the most significant impact his actions may have is reducing Frank's bandwidth. Bandwidth theft is something not explored in this paper that probably should be at some point. Briefly, access to the Internet is analogous to access to a highway—there are only a certain number of lanes available for all of the data to traverse to get to where they are going. Any action taken over the Internet that involves sending or receiving data—basically everything—uses up bandwidth. Some actions take up very little bandwidth—checking e-mail or viewing a webpage, for instance. Others, like music downloading can take up a great deal of bandwidth. Assuming Frank pays for his Internet access, downloading music off of his computer can actually be rivalrous with respect to him, just not in the sense that he is deprived of music in anyway, but that he is deprived of the complete Internet access he purchased.

various copyright holders have been deprived of sales proceeds. That deprivation will not change with time; once Tom has downloaded the file, he has no need to purchase the music, and the copyright holder's interest is permanently impaired. This harm should not be taken lightly, either. The economic effect of Tom's theft is not just that the record company has lost a sale to him, it is that it could not sell a Tom a record even if they wanted to do so at a loss. Aggregated over millions of users, this amounted to a great deal of harm during the height of the Napster revolution.[16] The theft is therefore simultaneously rivalrous and non-rivalrous with respect to different groups of people based on the point of view adopted.

What the RIAA done has so effectively is convey this message to the general public. The RIAA has essentially answered the question posed earlier—who is the victim—with an answer that aligns victimhood with the person whose interests are permanently impaired. By characterizing music downloading as rivalrous, the RIAA managed to persuade millions of people that a victimless crime had a very real victim.

II. Password Theft

Robert Konop was frustrated with Hawaiian Airlines.[17] A pilot for Hawaiian and a member of the Air Line Pilots Association (ALPA) union, Konop had been following the most recent labor negotiations with great earnest. What he saw upset him a great deal: the ALPA had

---

[16] A study sponsored by the RIAA suggests that music retail sales near college campuses—where the vast majority of Napster usage took place, due largely to the accessibility of high-speed Internet access—plummeted during the years of Napster, by as much as 88%. REPORT OF MICHAEL FINE, http://www.riaa.com/news/filings/pdf/napster/fine.pdf (last visited Aug. 16, 2005).; *see also*, *Q&A: Music Downloading*, BBC NEWS, http://news.bbc.co.uk/1/hi/entertainment/music/3582621.stm (last visited Aug. 16, 2005).

[17] The following fact pattern is based on *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

agreed to almost all of the concessions suggested by Hawaiian management. If this were the 1950's, or even the 1980's, Konop would have no redress other than through democratic means: organize elections to replace union leadership, or perhaps call meetings and the press to put pressure on the ALPA to fight Hawaiian management. But this was 1995, and Konop decided to employ a different tack to get other union members to see his point of view: he started a website.

Konop's website was no ordinary website that average Internet users visit everyday. Recognizing the sensitive nature of his website's content—he could lose his job over this, after all—Konop restricted access to his website. Prior to being able to view any of the website's content, a potential user had to log on by entering his name; that name had to be on a list of Hawaiian pilots and employees composed by Konop. Once the user was logged in, the user created a password that would allow the user to return to the website. Thus, Konop was able to ensure that the only people viewing his website were fellow employees that he selected; no one from the ALPA's current leadership, no unwanted lawyers, and certainly no one from Hawaiian management. In addition, one of the terms for viewing the website prohibited approved users from disclosing the contents of the website to others. Konop, as webmaster, had designed a space where he, and others who shared his views, could freely express their displeasure with Hawaiian Airlines and their union leadership without fear of retaliation.

James Davis was a Hawaiian Airlines vice president when Robert Konop set up his website, and, having learned of its existence, he wanted to see its contents for himself. However, because of Konop's design features, Davis could not do so without literally hacking the site. Instead he did something quite obvious, and quite devious—he used someone else's name. Using the names of two other pilots who were on Konop's approved list—after having procured their

permission—Davis was able to gain access to Konop's site and view its contents for himself.[18] He relayed what he found to Hawaiian Airlines president Bruce Nobles, who contacted the ALPA leadership personally to discuss the matter.[19]

Konop, after having been contacted by the ALPA leadership and temporarily taking his website offline, refused to relent and continued to operate his website as before. His records indicated that over the next four months, Davis logged onto his website at least 34 times as one of the two pilots whose names he was using. Eventually, Konop was placed on medical suspension. As a result, Konop sued, alleging state tort claims, violation of the federal Wiretap Act, the Stored Communications Act (SCA), and the Railway Labor Act. The district court granted summary judgment claim on all but one claim, and entered judgment against Konop on the last one after a short bench trial. Konop appealed to the Ninth Circuit. With the exception of one claim, however, the Ninth Circuit affirmed the dismissal.

Robert Konop's story is an interesting starting point for a discussion of password theft because it presents some of the major problems facing law enforcement and courts in defining theft in the digital age. Specifically, the Konop story raises two problems that arise in most password theft cases: identifying the victim and evaluating how the victim was harmed.

The victim in this case was obviously Robert Konop. But, as I argue below, when taken out of the context of personal websites and employment retaliation, that question becomes harder to answer initially. Finding the victim in these cases is incredibly important if the law is to effectively deter password theft. James Davis harmed Konop by using two passwords that had

[18] As I argue below, that James Davis was able to procure the pilots' permission should not matter, as in this case, the pilots had no permission to give. *See infra*, pg. 25.

[19] Apparently, Konop had accused Nobles of suspicion of fraud, and published various other disparaging comments.

been lent to him without Konop's permission to log onto his website. In a sense, Davis defrauded the computer—he convinced it that "he" was "someone else"; this is classic fraud in the inducement.[20] Identifying who owns the password becomes critical in answering the first question: who is the victim. As for the second issue, the harm suffered by Robert Konop was very real: he could have lost his job. He may have been placed on medical suspension as a result of this website, which certainly cost him money. More fundamentally, his privacy was invaded. The harm caused by password theft very often impairs a pecuniary or a dignity right.

What we have here, then, is a criminal act: a perpetrator defrauded the victim's computer and impaired the victim's dignity. Password theft, however, is not a unary crime; it comes in two forms, depending on the nature of the password. The discussion that follows details first and second-party password theft.[21] The distinction between the two rests on who holds the password when it is stolen—the person to whom it belongs (the first party), or the person to whom it is entrusted (the second party). First-party password theft concerns crimes that are quite familiar—identity theft, monetary theft, mail theft—and are clearly analogous to the common law crime of larceny. Indeed the jurisprudence that has arisen around first-party password theft has followed that course, and has had relatively little difficulty in adapting to the Internet.

Second-party password theft, however, concerns crimes that are not as obvious—unauthorized access, password sharing, and the like. Two recent famous examples of second-party password theft both coincidentally involve university admission offices at prestigious universities. At Princeton University, an admissions officer hacked into Yale University's

[20] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. REV. 1596, 1654-55 (2003).

[21] There is a third form of password theft that is a hybrid of the first two that is not discussed in this paper.

website to gather personal information about applicants to the Ivy League school.[22] Similarly, a group of Harvard University Business School applicants hacked the Harvard site to learn if they had been admitted or not.[23] In the Princeton case, the admissions officer guessed the access codes based on the applicants' applications to Princeton; while the officer certainly invaded the privacy of those students, his actions also calls into play criminal liability with respect to Yale.[24] His action was a textbook case of second-party password theft. In the Harvard case, a hacker posted instructions on his website on how to hack Harvard's website. While Harvard tentatively has stated that those known to have hacked the website will be denied admission, the school has run into a familiar problem in these kinds of cases: not knowing who committed the crime makes it difficult to apply an appropriate punishment.[25]

Second-party password theft also calls into play the notions of rivalrous and non-rivalrous theft raised by the RIAA in the Napster case.[26] In addition, courts have completely missed second-party password theft's closest real space analogue: embezzlement. If courts are going to effectively criminalize second-party password theft, and if law enforcement is going to effectively deter it, they need to identify these two characteristics.

A. First-Party Password Theft

---

[22] CNN.com, *Princeton Accused of Ivy League Hacking* (2002), http://archives.cnn.com/2002/US/07/25/yale.princeton (last visited Aug. 16, 2005).

[23] Robert Weisman, *Harvard Rejects 119 Accused of Hacking: Applicants' Behavior Unethical at Best*, BOSTON GLOBE (2005), http://www.boston.com/business/articles/2005/03/08/harvard_rejects_119_accused_of_hacking_1110274403.

[24] Indeed Yale considered pressing charges against Princeton, although it never did.

[25] *See infra*, note 23.

First-party password theft involves the theft of a user's password that results in damage to that individual. The harm that results from first-party password theft usually takes on one or both of the following characteristics: (1) the loss of a pecuniary interest; or (2) the deprivation of a dignity or privacy interest. Additionally, another underlying characteristic of all first-party password theft cases is that ownership and possession of the password are located in the same person: the person from whom it has been stolen.

Password theft causes pecuniary harm in rather obvious ways. Just as stealing the key to my safety deposit box is a form of theft, stealing my personal identification number to access my online checking account can be viewed as a form of theft aimed at accessing the contents of that account. Law enforcement and courts have recognized this, and have acted accordingly.[27] The use of a computer is merely a different instrumentality for the same underlying illicit purpose: acquiring someone else's property.

In the case of harm to a dignity or privacy interest, the harm is characterized as an unwarranted invasion of privacy. Stealing Tom's password to read his private e-mail is no different than opening his real space mail. Both involve invading his privacy and harming either or both of his dignity and privacy. Even though his e-mail may reside on a third party's server, he clearly has a reasonable expectation of privacy with respect to its contents, and the law should punish unwanted intrusions.[28]

In both of these cases the harm is directly inflicted on the party who owns the password.

---

[26] *See infra*, pgs. 7-11.

[27] *See* 18 U.S.C. § 1030(a) (2004) (Computer Fraud and Abuse Act). *See also* United States v. Petersen, 98 F.3d 502, 505 (9th Cir. 1996) (holding that defendant violated Computer Fraud and Abuse Act when he hacked into the computer of a financial company and illegally transferred funds into his own personal account.

[28] *See* Quon v. Arch Wireless Operating Co., Inc., 309 F. Supp. 2d 1204, 1211 (C.D. Cal. 2004); United States v. Sims, No. CR 00-193 MV, 2001 U.S. Dist. LEXIS 25819 (D.N.M. 2001).

When Frank signs up for a checking account with Citibank or for e-mail with America Online, a password is given to him by the service provider so that he can access something—in this case his money or his correspondence—that belongs to him. When a criminal steals Frank's password, therefore, he takes something that belongs to Frank; the act contains clear real space analogues to common law larceny. Larceny, according to William LaFave, consists of a trespassory taking of the personal property of another.[29] In the case of first-party password theft, because the user actually owns the password, when it is taken by the thief, the thief's action constitutes a prima facie case of larceny.

The existence of real space analogues has allowed law enforcement to easily adapt larceny to an Internet-based environment in shaping preferences and characterizing first party password theft as criminal.[30] A perfect example of the law's proper adaptation of common law larceny to first-party password theft is *Oregon v. Schwartz*.[31] In *Schwartz*, the defendant used a program to guess the access password to some of the plaintiff's computer systems. The defendant proceeded to store the information he found on his home computer.[32] The court, in upholding the defendant's conviction for violating Oregon's theft statute, recognized that first-party passwords have intrinsic value: "passwords have value only so long as no one else knows what they are. Once defendant had copied them, the passwords were useless for their only purpose, protecting access to information in the [plaintiff's] computers. The loss of exclusive

---

[29] *See* LaFave, *supra* note 10, at §19.2.

[30] *Compare* Mesh v. Elenbogen Safe Deposit Co., 220 Ill. App. 351, 354 (Ill. App. Ct. 1920) (allowing a third party to access the plaintiff's safety deposit box amounts to larceny) *with* Oregon v. Schwartz, 21 P.3d 1128, 1135 (Or. Ct. App. 2001) (holding that access passwords to defendant's computer systems had independent value, and the defendant's unauthorized use constituted theft).

[31] 21 P.3d at 1135.

[32] *Id.* at 1130.

possession of the passwords...is sufficient to constitute theft."[33] While the court used the language of "exclusive possession," this amounts to possession and ownership residing in the same entity. The unauthorized use of such a password, the court recognized, amounts to digital larceny. First-party password theft has easily been criminalized on the Internet, because of the clear analogy to larceny.

B. Second-Party Password Theft

Second-party password theft is distinguished from first-party password theft by the fact that ownership and possession of the password reside in two different individuals or entities. The law has had a hard time identifying criminal behavior in this area, because (1) identifying the victim has proven elusive; and (2) quantifying the harm that the victim suffered has proven problematic.[34] The key to answering the second question, however, is correctly answering the first one. Because the law has had a difficult time identifying the victim, it has taken an overly broad view of damages in second-party password theft in an attempt to deter what it instinctively recognizes as criminal.[35] This section argues that by effectively identifying who the victim of second-party password theft is, and analogizing that action to embezzlement, judges can more effectively evaluate the harm suffered by second-party password theft victims.

---

[33] *Id.* at 1136-7.

[34] *See* Kerr, *supra* note 20, at 1598-1600, 1611. Kerr argues that a distinction should be drawn between unauthorized access in excess of contract-based restrictions on access and hacking to circumvent code-based restrictions on access. The result of this distinction, he argues, would allow courts to deal with cases involving Internet theft more predictably. While I disagree with his proposal—that the former should be governed by civil liability and the latter by criminal liability—his observation that courts have simply looked to harm suffered to find criminal liability is profound and informs much of the analysis that follows, especially in Part II.B.2. Part of the purpose of this paper is to offer an alternative solution to the problem that Kerr diagnosed.

1. Identifying the Victim in Second-Party Password Theft

The distinguishing feature of second-party password theft is that ownership of the password and possession of the password reside in two different entities. This feature of second-party passwords obscures the victim of the theft, making criminal liability difficult to apply. Additionally, the real space analogues to second-party password theft are not as apparent as the analogy between first-party password theft and larceny. This has rendered the legal analysis of second-party password theft unpredictable, and law enforcement has found it difficult to deter second-party password theft.

But it should not be so difficult, if instead of following possession of the password, courts followed ownership of the password in attaching criminal liability. In doing so, courts could follow the lead that has been established telephone fraud cases involving charges of possession of stolen property.[36] In *People v. Johnson*, the New York Criminal Court provided an important insight in this area: that the medium in which access codes (like computer passwords) are stored is irrelevant in a stolen property analysis, since what matters is that the access numbers were used by an unauthorized user.[37] In *Johnson*, the defendant illegally obtained international calling card numbers from an AT&T database and tried to sell them to passersby on the New York City subway system.[38] The defendant showed the number scrawled on a scrap of paper to an

---

[35] *Cf.* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 355 (2004).

[36] *See* Pennsylvania v. Delapaz, 796 A.2d 364 (Pa. Super. Ct. 2002); People v. Johson, 560 N.Y.S.2d 238 (Crim. Ct. 1990).

[37] Johnson, 560 N.Y.S.2d, at 243-244.

[38] *Id*. at 240.

informant, tore the scrap up, and only then dialed the number, showing that it worked.[39] The court, in upholding the possession of stolen property conviction, held that it did not matter that the defendant had torn up the scrap of paper prior to dialing the number, arguing that "[t]he number itself is what is crucial, and not who has the superior possessory interest in the paper on which the number is recorded, or whether the number is written as opposed to being memorized."[40] In other words, Johnson was in possession of a password that belonged to AT&T: ownership and possession resided in two different individuals, and the court followed ownership to find criminal liability.

In the Internet realm, the analysis of second-party password theft should follow a similar path, although the real space analogue to second-party password theft is slightly different. Consider a scenario familiar to most law students: LexisNexis assigns a password to Tom for his use. Just because LexisNexis assigns Tom a password, it does not mean that Tom owns it: he merely possesses it to access their databases. His usage is contingent on certain contractual obligations to which he agrees, one of which is that he agrees not to give the password to anyone else. Therefore, Tom's giving it to a friend to use, innocent though it may be with respect to Tom, is actually a form of conversion, or embezzlement.[41] The purveyor of the password can justify his act just like the Napster user can—the user's use has not harmed anyone. Additionally, the user was unlikely to pay for the service, just as the Napster user, in the service's absence, was

---

[39] *Id*.

[40] *Id*. at 243.

[41] *But see* Kerr, *supra* note 20. Kerr argues that this action should be governed by civil liability, rather than criminal liability. I respectfully disagree with his position. Kerr rests his argument on the assumption that finding criminal liability in this case would criminalize behavior that millions of Internet users engage in everyday. But the same was true of music downloading, and modest gains have been made in that area by characterizing that activity as criminal. In addition, the goal of criminal law should be to deter future criminal behavior, not to rationalize away past criminal behavior.

unable to buy the music. Using embezzlement as a real space analogue to second-party password theft provides the most fruitful way for law enforcement and courts to effectively characterize it as criminal.[42]

Second-party password theft is characterized by a party giving a password to another entrusted user for that user's benefit. In the language of embezzlement, lending an entrusted password to an unauthorized user is a "fraudulent conversion."[43] In real space embezzlement, courts have construed this element broadly to encompass a wide range of fraudulent activities.[44] One court in New Mexico, for instance, has characterized fraudulent conversion as "when a person having possession of another's property treats the property as his own, whether he uses it, sells it, or discards it, he is using the property for his own purpose…the gravaman of conversion is interfering with the rights of the owner, either to the property itself or to the benefit from the manner in which the property was supposed to have been used. The details of the interference are less important than the interference itself."[45] Lending a password that has been entrusted probably falls into this category as well. A password that has been entrusted to a user who then lends it to another is an interference with the owner's rights of distribution amounting to a conversion. Identifying the victim in second-party password theft should follow the same

---

[42] *See* LaFave, *supra* note 10, at §19.6. According to LaFave, embezzlement evolved because the law recognized that requiring a trespassory taking for larceny created a massive loophole in the age of corporate agents: agents, who had rights to use corporate assets, would use them for their own personal benefits, at the expense of the corporation. Because they had access to these assets, their actions could not be characterized as trespassory, a crucial element in a larceny claim. Embezzlement was created to fill that hole. Rather than require a trespassory taking, legislatures required a fraudulent conversion of the property of another.

[43] *Id*.

[44] *See*, *e.g.*, New Mexico v. Archie, 943 P.2d 537, 540 (N.M. 1997) (holding that a convict who took off an electronic monitoring bracelet and threw it away was guilty of embezzlement, because ownership of the bracelet resided with the state, and he was merely entrusted with its use.).

[45] *Id*. [interior quotations omitted]

analytic framework that has been in place for decades in embezzlement cases. The owner, not the possessor, of the password is the real victim.

By using a clear real space analogue, like embezzlement, the law can effectively characterize second-party password theft as a criminal action. What remains, however, is evaluating the harm that the victim suffered. This stage of the analysis relies upon the distinction between rivalrous and non-rivalrous theft presented above.[46]

2. Evaluating Harm in Second-Party Password Theft

Once the victim of second-party password theft has been identified, the next step is evaluating the harm the victim suffered. It is in this area that the law has failed most dramatically, largely due to its misunderstanding of the first issue. In determining liability—criminal or civil—courts have paid overdue attention to the damages portion of the analysis.[47] The analytic approach that courts have adopted has lacked both analytic rigor and any semblance of consistency. As Orin Kerr has rightly pointed out, a finding of harm by a court has become a substitute for a finding of liability.[48]

Congress's incursions into this area have not faired much better. Under the federal CFAA, to be liable for password theft—or any form of computer abuse—the damage caused by the criminal must exceed $5,000.[49] Consistent with their generalized approach, this provision has

[46] *See supra*, pgs. 7-11.

[47] *See* Kerr, *supra* note 20, at pg. 1611.

[48] *Id*.

[49] 18 U.S.C. § 1030(e)(8)(A) (2000).

been interpreted broadly by many courts.[50] The passage of the USA PATRIOT Act has codified this approach, allowing just about any action a victim takes in response to an unauthorized access to be used in calculating damages.[51] This approach has come under attack from a variety of sources.[52] Indeed, as Galbraith points out, the breadth of the PATRIOT Act's scope potentially includes a variety of actions taken by victims that would never be considered damages in real space, and opens the door to grave abuses by victims.[53] Some of the actions considered "damages" by the PATRIOT Act would be ludicrous in real space. If a thief approached Tom's home, tried the door knob, and simply walked away, the thief could probably be convicted of attempted burglary. If, after learning of the thief's attempt, Tom then installed an expensive alarm system and a brand new deadbolt lock system, could he charge the thief for those expenses? Of course not: Tom benefits from the enhanced security, regardless of the last thief's actions. Yet under the PATRIOT Act, the Internet equivalent of installing a deadbolt in response to an attempted burglary—installing a firewall in response to an attempted hack—contributes to the damages analysis of criminal liability. The damage portions of the PATRIOT Act allow for all sorts of inefficiencies in victim behavior.

By properly identifying the victim and the perpetrator of password theft, however, the law need not evaluate the specific damages actually suffered by the victim and it does not need

---

[50] *See* EF Cultural Travel v. Explorica, Inc., 274 F.3d 577, 584-585 (1st Cir. 2001); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) (holding that damage to the integrity of a network that causes the victim to take corrective measures can go towards the damage calculation under the CFAA).

[51] Pub. L. No. 107-56, 814, 114 Stat. 272, 382 (2001).

[52] *See* Galbraith, *supra* note 35, at pgs. 354-55; *see also* Kerr, *supra* note 20, at pg. 1611.

[53] Galbraith, at 356 ("[W]ebsite owners…can ensure that they have fulfilled the $5000 statutory threshold. All a website owner need do is to hire a firm to conduct a 'damage assessment' following detection of robotic activity").

an arbitrary threshold of $5,000. For instance, in the LexisNexis example presented above,[54] the proper victim is LexisNexis, and the perpetrators are Mary (the password holder) and Tom (the password borrower) in the case where Mary lends her password to Tom, and the perpetrator is just Tom if he steals it from Mary. The harm of Tom's theft can be grave when replicated on a mass scale, and impossible to quantify. The result of stealing Mary's password is not just that Lexis lost a sale; it is that it could now never sell an account to Tom, even for a penny. If Tom's actions are allowed to continue unchecked, aggregating over thousands of transactions, it can amount to extraordinary damage to Lexis. If Lexis installed a comprehensive firewall after Tom's password usage, therefore, they still benefit from it on a much greater scale, regardless of Tom's behavior; there is no reason to include it in a damages calculation if the sole perpetrator is Tom (or perpetrators are Mary), especially since that single transaction is trivial in comparison to the real damage suffered by Lexis. Finding liability, therefore, should not hinge on crossing an arbitrary threshold that is impossible to quantify accurately: it should hinge on whether an action permanently deprived an owner of his ownership rights. Put simply, if a user embezzles a password, he has committed theft.[55]

Conducting the analysis in this fashion also dovetails nicely with the dual rivalrous and non-rivalrous nature of Internet theft. If Tom steals Mary's Lexis password, we have seen that by following ownership instead of possession, Tom is really stealing from LexisNexis, not Mary. And economically this should be so. Tom's theft is rivalrous with respect to LexisNexis; they are permanently deprived of the account they could otherwise have sold to Tom, and far more in the aggregate. On the other hand, Tom's theft is non-rivalrous with respect to Mary; his theft,

[54] *See supra*, pg. 18.

[55] To avoid economic substitution effects, the law could easily stratify the penalties of password theft based on the severity of the theft.

whether with her permission or without, has deprived her of nothing. At worst, she may have to be reassigned a new password, or be deprived of access to Lexis for a limited time. But the depletion is not permanent, and should therefore not be considered theft with respect to her.[56]

Second-party password theft analysis would also deal with the Konop case far more effectively than the Ninth Circuit did.[57] Robert Konop was clearly the victim in the case, as it was his password to distribute, and his harm was real, even if the pecuniary nature of that harm was *de minimis*. Where the court erred, however, was in mistaking possession of the password for ownership. Had it not done so, the perpetrators of the crime would have been clear: the pilots. James Davis accessed Konop's website with passwords given to him by two pilots who had no right to lend them. By "lending" their passwords to Davis, the pilots embezzled those passwords, interfering with Konop's right to determine *ex ante* who had access to his website. Once a perpetrator is identified, Konop's harm becomes far more real and easy to evaluate, if difficult to quantify precisely—his ownership right was fraudulently converted, and his privacy was invaded.

III. How to Deter Password Theft: Following the RIAA's Lead

In applying the above theory into practice, Internet content-providers like LexisNexis would be wise to follow the RIAA's lead; after all, they wrote the script. The RIAA's actions after the rise of Napster reflect an understanding of the rivalrous and non-rivalrous nature of Internet theft, and a clearer understanding of victim and perpetrator identification.

---

[56] *See* Kansas v. Allen, 917 P.2d at 853.

[57] *See supra* pgs. 11-13.

Comprehensive programs of public education, flexible password usage contracts utilizing price discrimination models, and targeted lawsuits are just three examples of tactics that Internet content- providers could employ in an effort to reduce password theft.

A. Public Education

One of the most effective tools deployed by the RIAA in the wake of Napster was an aggressive public campaign to brand music downloading as a criminal act. Television and print commercials focused on the human side of a multi-billion dollar industry, describing the people whose jobs were lost because of illegal music downloading.[58] Instead of platinum selling artists like Metallica and Britney Spears as the victims, the RIAA used the lesser-known—and more modest—employees of music companies who suffer as a result of rampant music downloading. The consequence of these advertisements was nothing short of staggering: illegal music downloading has plummeted in comparison to the rise of Internet usage since 1999.[59]

Internet content-providers should be deploying a similar campaign. While it may be hard to garner much sympathy for a faceless corporation like LexisNexis, it is amazing what branding something as criminal will do in the court of public opinion. Putting human employees who face job loss or pay cuts out front could also enhance the human factor. In any event, Internet content-

---

[58] *See, e.g.*, *Recording Industry Begins Suing P2P File Sharers Who Illegaly Offer Copyrighted Music Online* (2003), http://www.riaa.com/news/newsletter/090803.asp ("In addition, it [illegal downloading] threatens the jobs of tens of thousands of less celebrated people in the music industry, from engineers and technicians to warehouse workers and record store clerks") (last visited Aug. 16, 2005).

[59] *See infra*, note 5. While some polls indicate that the sheer number of people illegally downloading music has risen since 1999, that number pales in comparison to the increase in the number of people who have since gained Internet access since 2000. According to one poll, that number has doubled in North America alone, and close to tripled in other parts of the world. *Internet Usage Statistics – The Big Picture*, http://www.internetworldstats.com/stats.htm (last visited Aug. 16, 2005).

providers should band together to campaign against password theft; because so few people consider second-party password theft a crime, they can only improve.

B. Flexible Password Usage Contracts and Price Discrimination

One reason illegal music downloading has plummeted is the rise of legal, better, alternatives that harnessed a changing music listening environment.[60] In particular, iTunes, the legalization of Napster, and various other outlets, have provided a legal source for music lovers looking for music files who did not want to purchase full albums. The upshot of these services is that they are simply better than their illegal counterparts. Because the music was countenanced by the RIAA, there was less of a chance of acquiring a spoofed song or contracting a virus. In addition, because these services actually had contracts with record companies, finding obscure songs became far easier on iTunes than on an illegal peer-to-peer network like Grokster. The RIAA essentially bit the bullet in approving of iTunes; they make less per song then they did when they only sold full albums, but by recognizing a new pattern of music listening, and harnessing the technology that enabled it, it has turned rampant theft that did not benefit them at all into a profit making arm of the music industry.

Better technology will obviously solve a lot of problems for Internet content-providers plagued by password theft. Biometric analysis, for example, can identify whether the person typing in a password is the actual person to whom that password is assigned. But what iTunes and other music downloading services represent in the music world is a recognition that a new form of music usage gained traction among listeners. People were tired of the album format, and

---

[60] *See* Study: Legal Music Downloading Triples Worldwide, *supra*, note 4.

wanted to be able to listen to individual songs on demand. At first, the only outlet for that desire was illegal services; but the RIAA adapted, and it has begun to co-opt the medium for itself.

Internet businesses should recognize that a new pattern is emerging in password usage. People increasingly feel that they own the passwords that are assigned to them as part of a service for which they pay, and feel that lending the password to a friend is a right that attaches to possessing the password. Internet content-providers have unwittingly fostered this belief by allowing users to pick their own passwords in most cases; users will typically pick the same password for everything, regardless of whether they own the password or have merely been entrusted with its use. Assigning passwords randomly is a small step that sends the signal that the password belongs to the service, not the user. Establishing defined, recognizable territorial limits can force people to treat assigned passwords differently much in the same way that clear territorial lines in real space architecture can encourage respect for property ownership.[61]

Rather than stifling password lending, Internet businesses should harness its potential. Businesses should offer flexible password plans—by paying more (but less than the amount for the full service), users can assign their passwords to a certain number of their friends. This kind of arrangement benefits everyone: users can lend passwords under the color of legality, and can do so without paying the regular full fee. Internet businesses can cut down on password theft, while bringing new customers into the fold. By recognizing a new form of consumer usage, this business model mirrors the iTunes model that has arisen in music downloading, which has already proven successful.

An additional benefit this model offers is the ability to price discriminate between single-

---

[61] *See* Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 2261 (2002) (arguing that in real space, one way the law can effectively deter criminal conduct is by establishing clear, physical boundaries between public and private space).

use users and other, higher valuation, users. [62] Price discrimination occurs when a seller can offer different prices for essentially the same good to multiple classes of individuals, based on their preferences. The classic example of price discrimination is the declining price for seeing the same movie.[63] Movie producers take advantage of the fact that certain individuals are impatient and want to see movies as soon as they are released; concordantly, opening day ticket prices for movies are incredibly high. However, as time passes, the price of the exact same movie declines as the potential pool of consumers grows: first it is offered for rental or sale at a video store, then it appears on premium cable channels, and eventually, it is available for free on network television. Impatient moviegoers are "high valuation" consumers: they value the product higher than most others do, are impatient and will pay more to see a movie earlier, and movie production companies are able to trade on that preference by charging them higher prices.

As Michael Meurer points out, three conditions are necessary for effective price discrimination: "(1) the seller has market power; (2) the seller can link prices to individual customer preferences; and (3) customers cannot arbitrage away price differentials."[64] By offering different usage contracts, content-providers can easily identify high valuation users. Content-providers can offer transferable licenses before making content available to the general public, for example: they offer the license at a higher price, and, after a set period of time, users are allowed to transfer that license to a limited number of friends at a discount to those friends. Higher valuation consumers are likely to purchase these transferable licenses as soon as they are made available, and lower valuation users, who otherwise may simply steal or borrow the

---

[62] *Cf.* Michael Meurer, *Copyright Law and Price Discrimination*, 23 CARDOZO L. REV. 55, 84-85 (2001).

[63] *Id.* at 85-86.

[64] *Id.* at 59.

password from a high valuation friend, are able to buy it instead at a discount. Either way, content-providers are able to price discriminate effectively while reducing password theft at the same time. The concern over arbitrage can be dealt with effectively by building into the architecture of the content restrictions on dissemination.[65] In any event, flexible usage contracts can not only deal with some of the problems with password theft, but, with effective price discrimination, may even become a profitable business venture for content-providers.

C. Targeted Lawsuits

Lastly, the RIAA has been incredibly successful in deterring illegal music downloading by attacking downloaders themselves, rather than the peer-to-peer network providers. The reason this tactic has been so successful is that by suing downloaders, it made a costless activity very expensive. As Gary Becker has shown, the rate of detection and the severity of punishment are largely interchangeable variables.[66] Prior to the lawsuits initiated by the RIAA, the chance of getting caught downloading music was zero, and the penalty was also zero. When the RIAA starting suing downloaders, the chance of getting caught was still incredibly small—millions of people were downloading at the time, and Internet Service Providers were loathe to distribute their names—but the severity of the penalty had suddenly skyrocketed, especially compared to the cost of just purchasing the album legally. Illegal downloading dropped immediately.

A similar strategy may be successful for other Internet businesses. It should be said that

[65] This is obviously easier to achieve in software sales than on the Internet. Microsoft, for example, sells a corporate version of its Office suite at a higher price that allows multiple installations, while its home version of Office, while cheaper, only allows for a far more limited number of installations. This feature is built into the code of the software. For a discussion on building restrictions into digital architecture as a tool for law enforcement, see Neal Kumar Katyal, *Digital Architecture as Crime Control*, 113 Yale L.J. 2261 (2003).

[66] *See* Becker, *supra* note 2.

the potential for backlash here is tremendous: over-deterrence can create massive marginal deterrence problems, as people figure that if they are going to lend a password to one friend, they may as well start a website and distribute them to millions. In addition, the court of public opinion should not be underestimated either: if the strategy is to educate people, content-providers should not be too aggressive in prosecuting people who are probably truly ignorant of their criminal behavior. Targeting lawsuits against particularly egregious violators—those who knowingly distribute passwords on a mass scale, for instance—provides a measure of deterrence without compromising position in the court public opinion.

Conclusion

Fortunately, the law has a path to follow in deterring password theft. The RIAA has recognized the threat posed by Internet theft and has made some significant advances in deterring it. While they have sustained a great deal of criticism from certain quarters,[67] they have also been impressively effective, as the percentage of illegal downloaders has dropped since Napster. The law, as well as Internet content-providers, can draw some important lessons from the RIAA about the economics of digital theft in its efforts to deter password theft.

By most measures, incidence of password theft is rising, not declining.[68] As more people gain access to the Internet, and the Internet's reach broadens, the importance of passwords in the daily lives of the hundreds of millions of Internet users is also likely to increase. While

[67] *See, e.g.* Electronic Frontier Foundation, *Electronic Frontier Foundation's defense of Grokster against the RIAA*, http://www.eff.org/IP/P2P/MGM_v_Grokster/ (last visited Aug. 16, 2005).

[68] *Putting an End to Account-Hijacking Identity Theft*, http://www.fdic.gov/consumers/consumer/idtheftstudy/background.html (last visited Aug. 16, 2005).

technological advances are being made in increasing the security of databases, the law has lagged behind in identifying the key features of password theft, and what makes it unique among other Internet crimes. Distinguishing between first and second-party password theft, identifying the victim, and properly evaluating the harm suffered are just the first steps in updating the law to fit the realities of the Internet.