William Mitchell Law Review

Volume 27 | Issue 3 Article 22

2001

# Webjacking

Robert J. McGillivray

Steven C. Lieske

# WEBJACKING

Robert J. McGillivray†
Steven C. Lieske††

I. INTRODUCTION ..... 1662
A. *Changes In Commerce Have Made On-Line Consumers Vulnerable To Webjackings* ..... 1663
B. *A Webjacker Can Now Steal The Whole Store* ..... 1664
II. THE EVOLUTION OF DOMAIN NAME MANAGEMENT ..... 1665
A. *A Brief History Of The Internet And The Emergence Of Domain Names* ..... 1665
B. *The Explosion Of Domain Names Results In New Management* ..... 1668
III. WEBJACKING—A TWENTY-FIRST CENTURY CON JOB ..... 1669
A. *Recent Webjackings In The News* ..... 1670
B. *How A Webjacking Occurs* ..... 1671
1. *The Whois Database: Planning The Attack* ..... 1671
2. *Fakemail: Sending The Counterfeit Request* ..... 1673
3. *Authentication: Having The Registrar Incorrectly Determine That The Request Is Real* ..... 1674
4. *Laundering: Transferring The Registration To A New Registrar* ..... 1677
C. *What Do Webjackers Gain?* ..... 1678
D. *What Do Victims Stand To Lose?* ..... 1680
IV. OPTIONS FOR WEBJACKING VICTIMS ..... 1681
A. *Work With The Registrar* ..... 1681
B. *Consider Using The UDRP—Even Though It Was Not Intended For Webjackings* ..... 1683
C. *Work With Authorities* ..... 1686
D. *Seek Expedited Relief In Court* ..... 1687

† Robert McGillivray is a commercial litigation partner in the Minneapolis office of Oppenheimer Wolff & Donnelly, LLP and a member of the firm's domain name dispute team.

†† Steven Lieske is an associate in the Minneapolis office of Oppenheimer Wolff & Donnelly, LLP. He practices in Internet, trademark, and patent law.

1. *The Computer Fraud And Abuse Act* ..... 1687
2. *The Electronic Communication Privacy Act* ..... 1688
3. *The Anti-Cybersquatting Consumer Protection Act* ..... 1690
4. *The Federal Lanham/Trademark Act* ..... 1692
5. *Unfair Competition* ..... 1693
6. *Copyright Act* ..... 1694
7. *Other Causes Of Action* ..... 1695
E. *Seek Relief Against Registrars?* ..... 1695
V. REGISTRARS' (RE)ACTIONS TO COMBAT WEBJACKING ..... 1696
VI. WHAT SHOULD BE DONE? ..... 1698
A. *ICANN Should Improve Policies* ..... 1698
B. *Law Enforcement Should Be Given Sufficient Resources To Combat Computer Crimes* ..... 1699
C. *Registrants Should Take Preventative Steps* ..... 1699
VII. CONCLUSION ..... 1701

*"The Internet is like a vault with a screen door on the back. I don't need jackhammers and atom bombs to get in when I can walk through the backdoor."*[1]

## I. INTRODUCTION

Amid all of the hype over Internet security with respect to computer viruses,[2] denial of service ("DOS") attacks,[3] and consumer privacy issues,[4] one of the Internet's "screen doors"-web hijacking, also known as webjacking—has been overlooked. By definition, the term "hijacking" refers to the seizure of a moving vehicle by use of force, especially to reach an alternate destination.[5] By extension, the term "webjacking" refers to the seizure of a domain name to force web traffic to an alternate website location.

1. Anonymous, *at* http://www.quoteland.com.

2. Mark Landler, *A Filipino Linked to 'Love Bug' Talks about his License to Hack*, N.Y. TIMES, Oct. 21, 2000, at C1. The Love Bug virus caused an estimated $10 billion in damages. *Id.*

3. Matt Richtel, *Canada Arrests 15-Year-Old in Web Attack*, N.Y. TIMES, Apr. 20, 2000, at C1. In a denial of service attack, a computer is bombarded with large amounts of meaningless data to bog the computer down so that it cannot respond to legitimate requests. *Id.*

4. Erik Lipton, *2 Hired to Calm Fears for Web Privacy*, N.Y. TIMES, Mar. 8, 2000, at B3. DoubleClick announced these new hirings a week after it announced its intentions to use its vast amount of information about how individuals use the Internet. *Id.*

5. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 854 (3d ed. 1992).

A webjacking is often accomplished by the webjacker sending a counterfeit e-mail message to the registrar controlling a domain name registration. The counterfeit message appears to have been sent from someone with authority over the domain name, and the message instructs the registrar to "connect" the domain name with a new Internet Protocol ("IP") address. Once this connection is set up by the duped registrar, any Internet user who types the domain name in his or her web browser is taken to whatever website the webjacker has installed at the new IP address. Sometimes the webjacker's website is a fraudulent copy of the original website, causing Internet users not to notice the webjacker's scam.

Webjacking is a surprisingly easy way to take control of a website. While website owners fortify their systems with firewalls and other security measures, some have lost control of their sites as a result of a webjacker simply e-mailing the registrar. Unless the door that allows webjacking to happen is closed and locked, no amount of front-facing security will protect websites from such a rear attack.

### A. *Changes In Commerce Have Made On-Line Consumers Vulnerable To Webjackings*

Websites and the e-commerce that they provide have truly changed the structure of commerce. While shopping has become increasingly easy, advances in commerce that have provided this ease of use have at the same time removed many indicators consumers formerly relied upon to judge the integrity of a merchant. Thus, consumers may not know when they have been webjacked to a fraudulent website.

The traditional brick and mortar store or financial institution was quite safe to deal with. Customers could meet the people with whom they were dealing, physically inspect goods before buying them, and visually inspect the store or bank itself. Although the relatively recent advent of catalog shopping or phone banking provides less opportunity for inspection, the consumer still has ways to evaluate the transaction. As with the brick and mortar store, running a mail order company is expensive. Mail order companies produce well-designed, glossy catalogs in order to be accepted as "authentic" vendors. Each catalog is so expensive to produce that consumers have a high degree of certainty that the vendor is legitimate.

E-retailers have tried to extend catalog value-indicators to the

web. Although Amazon.com and a few other giants have successfully forged new brands on-line, many of the e-retailers operate under established brand names that consumers trust.[6] Just as catalogs rely on glossy pages to sell goods, e-vendors have built graphic-intensive websites full of slick animations and eye candy design[7] to convince the consumer to buy. Unfortunately, appearances are not always as trustworthy on-line as they are in the store or catalog. Although good web design requires an artistic hand coupled with a programmer's mind, and even though many companies pour large amounts of development money into their websites, often a website can as likely be built (or fraudulently duplicated) by a multinational corporation as by a high school student.[8] Thus, consumers cannot easily detect when they have been webjacked to a fraudulent website.

### *B. A Webjacker Can Now Steal The Whole Store*

Before the Internet, although a crook could hold up a cashier for the money from the register, a thief could never take over an entire department store and pose as the owner. Generally, it would have been too costly for a scam artist to mail counterfeit catalogs. In contrast, websites are not hard to create. In fact, someone with intermediate computer skills can, in short time, create a forged duplicate of another website. Such forgeries have been reported several times. For example, the AJ Park law firm in New Zealand discovered that someone copied the code for its website at http://www.ajpark.com, changed the "New Zealand" references with references to Russia and routed three domain names to the bogus site.[9] Although these forgeries could be by some kid trying

6. For example, Land's End can be accessed at www.landsend.com; Sears is at www.sears.com; BestBuy is at www.bestbuy.com; and Target is at www.target.com.

7. For example, http://www.balthaser.com won "Best of Show" at the @d:Tech World Awards in May, 2000; http://www.videofarm.com won the 2000 Webby for "Best Broadband Website;" and http://www.10socks.com won the Gold for "Best Branding Campaign" at the @d:Tech Europe Awards in October, 2000. The Webby Awards are presented by The International Academy of Digital Arts and Sciences and hailed as the "Oscars of the Internet." *Webby Awards, at* http://www.webbyawards.com.

8. The following websites are 2000 ThinkQuest Internet Challenge Finalists, an international program for students ages twelve through nineteen: Van Gogh at Etten, http://library.thinkquest.org/C001734; Forces of Nature, http://library.thinkquest.org/C003603/intro2.shtml; Eyesight, an Insight, http://library.thinkquest.org/C001414.

9. Reported by Damian Broadley (dbroadley@ajpark.co.nz) to the Interna-

to learn HTML, they also could be by some start-up law firm trying to get a web site up as soon as possible. Whatever the reason, these forgers do not pose a huge threat because when AJ Park's clients type "www.ajpark.com" in their web browsers, they are not misdirected to the forged website, but are correctly steered to AJ Park's real site.

Webjackers, on the other hand, do pose a threat. Should AJ Park's website be webjacked, its clients would surreptitiously be sent elsewhere. If the webjacking was done for political reasons, the client might be sent to a web page condemning the legal system, legal fees, and attorneys. However, if the webjacking was done, for example, in an attempt to gain credit card or other information from unwary clients, clients could be redirected to a doppelgänger, forged copy of the original, authentic site. Because the clients have typed in the proper domain name and are presented with what appears to be the proper website, they are easily fooled into revealing their private information. Because webjacking a domain name is not very difficult to accomplish, and does not require much computer skill, it may become a favorite con game of the twenty-first century.[10]

## II. THE EVOLUTION OF DOMAIN NAME MANAGEMENT

In order to understand webjacking, it helps to first understand how domain names are managed, and how that management has changed over time.

### *A. A Brief History Of The Internet And The Emergence Of Domain Names*

While the United States was involved in the Cold War, with the threat of nuclear attack an ever present possibility, the military funded projects in the 1960s related to packet-switching. This form of communication splits data into many small packets, sending each packet individually through a network and re-combining them at the destination. Because the packets travel through the network out-of-order and by way of any number of paths to the destination,

---

tional Trademark Association ("INTA") newsgroup on August 12, 2000. After AJ Parks complained to the registrant of the domain names, the registrant blamed a third party. The registrant has since instructed its ISP to redirect all web traffic for the three domain names to AJ Parks' legitimate website.

10. *DNS Intrusions Spotlight Security Debate*, NETWORK NEWS (EUR.), May 3, 2000, *available at* 2000 WL 7833925.

the goals of packet-switching were to offer communication that was difficult to intercept and that could continue to function if part of the network was destroyed under a large scale attack.[11]

In the late 1960s, the Defense Advanced Research Projects Agency ("DARPA") chose a group of researchers from the University of California Los Angeles ("UCLA") to install and run a computer network. Around Labor Day 1969, the group configured a four-node network (later to be called ARPANET), linking UCLA to Stanford Research Institute, University of California Santa Barbara, and the University of Utah in Salt Lake City.[12]

Over time, DARPA expanded its ARPANET by linking to networks of other government agencies.[13] In the 1970s, DAPRA funded a program to expand ARPANET by building a "network of networks."[14] This later became known as the Internet.[15]

In those days, Transmission Control Protocol ("TCP") was one standard communication method that was used to transfer messages among the ARPANET computers. In January 1983, TCP was divided into two parts. This new protocol, called TCP/IP, became the standard for all computers using DARPA's network. In this dual protocol system, the TCP protocol was used to guarantee reliable delivery of data, while the IP protocol managed the delivery of data packets from a sending computer to a destination computer using Internet Protocol addressing (IP addressing).[16] An IP address is a set of four numbers, each separated by a period, such as "63.11.55.123."[17] This format is called dotted-decimal notation.

When TCP/IP was introduced in 1983, there were only a few hundred computers connected to what is now called the Internet. However, even with such a relatively small number of hosts, it was difficult to distinguish all of the individual computers by their IP

11. History of the Internet, *at* http://www.internetvalley.com/archives/ mirrors/davemarsh-timeline-1.htm (last visited Jan. 3, 2001).

12. Virginia Cerf, *How the Internet Came to Be, in* THE ONLINE USER'S ENCYCLOPEDIA (1993), *available at* http://www.internetvalley.com/archives /mirrors/cerf-how-inet.txt.

13. *Id.*

14. *Id.*

15. Of course, today, "describing the Internet as the network of networks is like calling the space shuttle, a thing that flies." John Lester (unconfirmed source), *at* http://cyber.law.harvard.edu/people/reagle/inet-quotations19990-09.html (last visited Jan. 3, 2001).

16. Cerf, *supra* note 12.

17. A simple way to determine your own IP address when connected to the Internet is to go to http://www.whatismyipaddress.com (last visited Jan. 3, 2001).

addresses. Because names are easier to remember than numbers, in 1984, Paul Mockapetris designed the DNS ("domain name system"), which is a hierarchical, global network of computers acting as name servers that translate domain names into their numerical IP addresses.[18]

For example, each ISP maintains a local name server. When a web user types the URL "www.attorneys.oppenheimer.com" into his or her browser, the browser first checks its own listing of local domain names. Usually, the website is located elsewhere and so the local name server sends a request to the highest level of the DNS hierarchy—the root server. The root server resolves the top level portion of domain names—".com" in this example. The root server gives the local name server the address of the ".com" name server and the local name server sends a request to the ".com" name server asking for the domain name to be resolved. The ".com" name server can resolve as far as the second level domain name and so points the local name server to the name server for "oppenheimer.com." Finally, that "oppenheimer.com" name server can fully resolve the "www.attorneys.oppenheimer.com" to the proper IP address. In this hierarchical fashion, domain names are routinely resolved to IP addresses by the DNS.

Throughout the early history of the ARPANET, Dr. Jon Postel and the Information Sciences Institute, under contract from DARPA, maintained the list of assigned Internet numbers and names used by the DNS.[19] In 1991, the National Science Foundation ("NSF") took over the coordination of much of the Internet infrastructure. At the beginning of 1993, NSF agreed to have Network Solutions, Inc. ("NSI") manage the domain name registration services, including the registration of domain names, and maintaining the primary server in the root file server system (which is the authoritative database of Internet domain name registrations and their corresponding IP addresses).[20]

Current users of the Internet often believe that it has always looked as it does now. This is not true. It was not until 1991 that a hierarchical method of accessing information over the Internet was

18. Kristin Windbigler, *Exploring the Domain Name Space* (Jan. 24, 1997), *at* http://hotwired.lycos.com/webmonkey/webmonkey/geektalk/97/03/index4a.html.

19. Cerf, *supra* note 12.

20. *Id.*

introduced.[21] The new application, which was named Gopher (after the University of Minnesota's mascot), was the first really friendly Internet interface allowing users to access files on the network through a simple menu system.[22]

### *B. The Explosion Of Domain Names Results In New Management*

Also in 1991, a new protocol (which had been proposed in 1989) slowly began to be adopted. It became known as the World Wide Web. The protocol—Hypertext Transfer Protocol, or HTTP for short—supported text having embedded links to other text.[23] In 1993, Mosaic[24] was developed as the world's first graphical user interface.[25] Mosaic used HTTP as its protocol and allowed users to access World Wide Web webpages that were interconnected by hyperlinks. Although not a standard, many in the Internet community began prefixing domain names to be used for the World Wide Web with "www.", such as "www.oppenheimer. com". In 1993, there were about 600 web sites—referenced by about 600 domain names. By 1994, that number had grown to 10,000 and to 100,000 by 1995. As of November 2000, there were over thirty-one million domain names registered worldwide.[26] Although some experts predicted in June 2000, that domain name registrations may grow to 160 million by the year 2003,[27] the approval in November 2000 for seven new top level domain names—including ".biz" and ".info"[28]—may certainly cause the number to be higher. This explosive growth in registered domain names has led to an evolution in how to manage them.

As mentioned above, before the domain name explosion, the government through an agreement with NSI handled domain name registrations. However, by 1997, the Internet had become more international and commercial, making it less appropriate for

21. Cerf, *supra* note 12.

22. Walt Howe, *A Brief History of the Internet, at* http://www.delphi.com/navnet/history.html.

23. *Id.*

24. Marc Andreessen led the team which developed Mosaic. *Id.*

25. Cerf, *supra* note 12.

26. The current statistic on the number of registered domain names can be found at http://www.domainstats.com (last visited Jan. 3, 2001).

27. *Domain Name Game,* COMPUTERWORLD, June 12, 2000, at 71(1).

28. Press Release, ICANN, *Approval for Seven New Top Level Names* (Nov. 16, 2000), *at* http://www.icann.org/announcements/icann-pr16nov00.htm.

U.S. research agencies to manage and fund the Internet.[29] President Clinton directed that the DNS be privatized so that competition and international participation would be fostered.[30] The result was the formation of the Internet Corporation for Assigned Names and Numbers ("ICANN"), a coalition that has assumed, among other things, responsibility for the Internet's root server system.[31] Domain name registration is now handled by a number of independent registrars accredited by ICANN. There are currently over 120 accredited registrars.[32] The registrars accept domain name registrations from the public and report the registrations to the independent registry. The registry is the entity that receives domain name service information from domain name registrars, inserts that information into a centralized database and propagates the information in Internet zone files on the Internet so that domain names can be found by users around the world via applications such as web browsers and email clients.[33] Currently, the registry for ".com" ".net" and ".org" registrations is maintained by a division of Network Solutions, which was renamed the VeriSign Global Registry Services when VeriSign acquired Network Solutions in March 2000.[34]

## III. WEBJACKING—A TWENTY-FIRST CENTURY CON JOB

A webjacking occurs when a registrar is tricked into connecting a domain name with the name server that resolves the domain name to the webjacker's IP address, thus sending unknowing consumers to a website controlled by the webjacker. Although Internet trademark infringement issues and cybersquatting have received more publicity, webjacking promises to be another serious e-commerce problem. A number of webjackings have recently been reported and undoubtedly, many cases go unreported.

29. Cerf, *supra* note 12.
30. *Id.*
31. ICANN's website is http://www.icann.org (last visited Jan. 3, 2001).
32. List of Accredited and Accreditation-Qualified Registrars, *at* http:// www.icann.org/registrars/accredited-list.html (last modified Dec. 27, 2000).
33. *VeriSign Global Registry Services' Glossary of Terms, at* http:// www.nsiregistry.com/glossary/gt3.html#regy (last visited Jan. 3, 2000).
34. *Id.*; Press Release, Verisign, *VeriSign Acquires Network Solutions to Form World's Largest Provider of Internet Trust Services* (Mar. 7, 2000), *at* http://www.nsol.com/news/2000/pr_20000307.html.

### A. *Recent Webjackings In The News*

In May 2000, a webjacker stole the web.net domain name. The domain was registered by a small Internet service provider to 3,500 nonprofit organizations. It took the Internet service provider a week of battling with the registrar to regain its domain name.[35] In the same month, a tourist portal for Bali lost its website due to webjacking This caused the portal to lose substantial business.[36]

The next month, nike.com was webjacked. Until the webjacking was reversed, consumers who typed www.nike.com in their web browsers were automatically directed to a website in Scotland maintained by a group called S-11 and hosted by Firstnet On-Line Ltd.[37] The redirected traffic overloaded Firstnet's server, making the company unable to serve its legitimate customers.[38] After the company billed Nike for the use of the servers, Firstnet considered suing Nike for neglecting to secure its domain name registration.[39]

The following month—in June 2000—a $500 million public net media company had internet.com, 1,300 other domain names, and virtually all of its business stolen.[40] This large scale webjacking was accomplished with just a fax machine.[41] The thief faxed a request to the registrar and the registrar promptly switch control of the domain names to the webjacker. Although the sites were regained in several days, the company's confidence in its registrar was not.[42]

One of the longest publicized webjackings is still underway. In 1994, Gary Kremen registered the domain name sex.com. In October, 1995 the sex.com site was allegedly stolen via a forged letter to the registrar.[43] The webjacker, Stephen Cohen, developed a pornographic website connected to the domain name and made millions.[44] It took Kremen two years of litigation before a court

35. K.K. Campbell, *Internet Domain Names Stolen: Businesses are Crippled After Pirates Take Over Their Web-Site Addresses*, THE GAZETTE (MONTREAL), June 2, 2000.

36. *Hijacking Going High-Tech*, THE LONDON FREE PRESS, June 9, 2000, at D3.

37. Ann Harrison, *Companies Point Fingers Over Nike Web Site Hijacking*, NETWORK WORLD FUSION, June 30, 2000, *available at* 2000 WL 9443184.

38. *Id.*

39. *Id.*

40. *NSI's Webjacking Epidemic*, Wired News 3:00 a.m. (June 8, 2000).

41. *Id.*

42. *Id.*

43. *Sex.com Ruling: It Wasn't Stolen*, Wired News 3:00 a.m. (Aug. 25, 2000).

44. *Judge Returns Valuable Porn Site to Original Owner*, THE MINNEAPOLIS STAR TRIB., Nov. 29, 2000.

ruled on November 27, 2000 that Cohen was guilty of webjacking the site.[45] Pending a final decision on potential damages, the judge has frozen $25 million in Cohen's business assets.[46] A related lawsuit against the registrar for allowing the webjacking to happen was dismissed.[47]

As one would expect, often it is the more 'famous' domain names that become the target of webjacking. In addition to internet.com and sex.com, the domain names for Addidas, LucasArts.com, Viagra.com, Croatia.com, Washington.com, and Canada.com have all been webjacked.[48] Even aol.com[49] has been stolen.

### B. *How A Webjacking Occurs*

Every registrar has a procedure for registering domain names as well as a procedure by which the registrant can update its registration information, which usually can be done on-line or by sending an e-mail message.[50] Webjackings can be divided into four primary phases: (1) planning the attack, (2) sending a counterfeit request to the registrar, (3) having the registrar incorrectly determine that the request is authentic, and (4) transferring the registration to a new registrar so that the rightful registrant has a more difficult time of recovery from the webjacking.

#### 1. *The Whois Database: Planning The Attack*

Registrars allow several fields in a domain name registration to be modified through a change request. Registrants can update their registration record with a new legal name or a new address. At first glance, one might assume that webjackers are concerned with these. However, a website is not based on the real or alleged name or street address of the registrant. Thus, these fields are not

45. Clint Boulton, *Sex.com: A Chapter of Prurient Jurisprudence Closes*, INTERNET NEWS, Nov. 28, 2000, *available at* http://www.internetnews.com/bus-news/article/0,,3_520901,00.html.

46. *Judge Returns Sex.com Domain to Owner*, USA TODAY, Nov. 28, 2000, *available at* www.usatoday.com/life/cyber/tech/cti845.htm.

47. *Sex.com Ruling: It Wasn't Stolen*, Wired News 3:00 a.m. (Aug. 25, 2000).

48. Bob Sullivan, *Web Sites 'Stolen' by Cyberthugs*, ZDNET NEWS, May 31, 2000, *available at* http://www.zdnet.com/zdnn/stories/news/0,4586,2580039,00.html.

49. Leslie Walker, *Fake Message Sends AOL E-Mail Astray; Security Breach Changes Net Address*, WASH. POST, Oct. 17, 1998, at G01.

50. *E.g.*, http://www.networksolutions.com/makechanges (last visited Jan. 3, 2001).

of concern.

Contacts are the second set of fields that can be added, deleted, or modified. Contacts are agents, either individuals or a group of individuals who all act in a specific "role," who represent the registrant on matters related to the registrant's domain name.[51] The registration lists the administrative, the technical, and the billing contact. For example, although the administrative contact may be listed as "John Doe" with an e-mail address of john.doe@company.com it may just as well be listed as "Administration Group" with an e-mail address of admincontact@company.com. The entity listed as one of the three contacts should be the entity best able to answer questions about that particular aspect of the domain name registration and should be authorized to represent the domain name registrant. The administrative contact is usually the owner of the domain name or a representative of the company who owns it. Some registrars operate under the rule that the administrative contract *is* the actual registrant.[52] The billing contact should be the person to whom the invoices for registration and renewal should be sent. The technical contact should be the person able to answer questions about the website's host servers.

Webjackers are very interested in the contact information for it is this list of people who are authorized to change the domain name registration information. Some webjackers may already be listed as one of the contacts because they are current or former angered employees of the domain name registrant who were previously set up as a contact. Otherwise, the webjacker chooses to impersonate one of these contacts during the webjacking.

The name servers are the third set of fields on the registration that can be updated. As discussed above in Section II (A), a name server is a computer that works as part of the DNS to resolve domain names to their corresponding IP addresses. Each domain

51. http://www.networksolutions.com/cgi-bin/glossary/lookup?term=Contact/Agent (last visited Jan. 3, 2001).

52. This causes problems when the administrative contact leaves the company and the company then tries to get the registrar to update the records with a new administrative contact. Domain name administrators say that in the past, registrars have stated that the only way such a change request would be approved is if the request was made via the former employee's e-mail address. In response, domain name administrators have had to set up a temporary mail account in the former employee's name and send the change request from this dummy account. Carole Fennelly, *Domain Name Hijacking: It's Easier Than You Think*, JAVAWORLD, July 18, 2000, *available at* 2000 WL 14587742.

name registration lists an IP address for both a primary and secondary name server. In practice, when a web user types a URL (such as http://www.oppenheimer.com), the hierarchical DNS is contacted and the primary name server assists in resolving the domain name to the proper IP address. If the primary server does not respond, the secondary name server is used.

Because the name server controls where web traffic is directed for the domains within its network, a webjacker usually seeks to change the listed names servers as ones within his or her control. All of the registration information for a given domain name is publicly available through the registrar's whois database.[53] Planning a webjacking attack is easy because the contract information and name servers for a domain name can be discovered in less than a minute.[54] Based on the whois database, the webjacker knows *who* to impersonate in order to get the name servers changed. The webjacker must now figure out *how* to accomplish the impersonation.

### 2. *Fakemail: Sending The Counterfeit Request*

E-mail is often used as the impersonation tool because it is not difficult to do. Fake e-mail messages have been nicknamed "fakemail" and the process of sending them is known as "spoofing." Fakemail messages are altered so that the message appears to have been sent by someone else. Webjackers configure fakemail so that the administrative contact appears to be the sender.

Unfortunately, sending fakemail is easy. There are several websites that allow anyone to create and send a rudimentary fakemail message.[55] Such websites alter the headers that are traditionally attached to the beginning of e-mail messages. The header information includes data about the sender—including his or her name and e-mail address—and the route the message followed during delivery.

Most fakemail websites produce e-mail the average reader

53. The "whois" name is quite descriptive of the database, since its purpose is to tell "who is" the registrant of a domain name. Network Solution's whois database can be accessed at http://www.networksolutions.com/cgi-bin/whois/whois (last visited Jan. 3, 2001).

54. *Domain Name Game,* COMPUTERWORLD, June 12, 2000, at 71(1).

55. Fakemail can be sent from, *inter alia,* http://www.cyborg.net/mail-html; http://www.hughesclan.com/fakemail.htm; http://www.virtualdrawing.com/fakemail; and http://fakemail.itgo.com (last visited Jan. 3, 2001).

would accept as real. However, to create a first-rate fake message requires more knowledge. Hackers can learn how to do this from the many documents available on the Internet.[56] There is even a "Fake Mail FAQ."[57] These tutorials point out that fakemail is possible because all Internet e-mail is managed with SMTP (Simple Mail Transfer Protocol).[58] A hacker only needs to gain access[59] to an Internet-connected server. Once connected to a server, the hacker can manually issue SMTP commands[60] to fool the server into believing it received such SMTP e-mail instructions from another computer.[61]

Hackers say university servers in the ".edu" domain are the best ones to try for access, because colleges and universities often have lazy security.[62] And because the Internet is not hampered by distances, a hacker does not need to limit his or her search for a server. A server in Europe or Asia works just as well as a server in America. Of the hundreds of thousand servers worldwide, the hacker only needs to find one with inadequate security measures. From this server, the hacker can create and send a fraudulent service request through a fakemail message instructing the registrar to modify the registration information for the desired domain name.

### *3. Authentication: Having The Registrar Incorrectly Determine That The Request Is Real*

Before any modification is made to a registration, the registrar should first authenticate the request – verify that the e-mail message was truly sent by the sender, and check that the sender is one of the authorized contacts. As more registrars enter the market, it is difficult to state that all registrars have equally adequate authen-

---

56. *E.g.*, http://hackersclub.com/km/library/hack99/Mail.txt; and http://hackersclub.com/km/library/hack/gtmhh1-2.txt (last visited Jan. 3, 2001).

57. Rourke McNamara, *The Fake Mail FAQ, at* http://www.hackerscatalog.com/mailfaq.htm (last visited Jan. 3, 2001). "FAQ" stands for "frequently asked questions."

58. *Id.*

59. Access is gained via "telnet," a protocol that allows a user to log on to a remote computer system and then to issue commands as if the user were physically located at that other computer system.

60. STMP commands are simple; for example, "mail from" and "rcpt to" are two STMP commands.

61. McNamara, *supra* note 57.

62. The Mob Boss, a.k.a. Mafia-man777, *The Wonderful and Evil World of E-mail: The Art of E-mail Forging and Tracing Explained in One Simple Text, at* http://hackersclub.com/km/library/hack99/Mail.txt (last visited Jan. 3, 2001).

tication policies. Although it is possible that some lax registrars may process service requests without even looking up the list of authorized contacts, it is more likely that most webjacking takes place because although the registrar checks the list of contacts, the registrar is fooled into believing that the fakemail message was sent by one of the contacts.

Registrars must each determine how to determine that an e-mail message is authentic. For example, Network Solutions has set up Guardian—an authorization and authentication system which helps protect domain name registration records from unauthorized updates.[63,64] During the initial registration process, the registrant chooses from one of three Guardian methods: (1) mail-from, (2) crypt-password, or (3) PGP.

Mail-from is the first and the least secure Guardian method. For domain name registrations protected by this method, all registration contacts provide NSI with their e-mail address. Whenever NSI receives an e-mail message requesting change to the registration record, the e-mail's headers are checked and the "mail from" field must match the contact's e-mail address that is listed in the whois database. Of course, because the e-mail addresses are publicly available through the whois database and because fakemail easily modifies the "mail from" field, this Guardian method is simple to use, but not very secure. Network Solutions now advertises that it has additional measures built in its policies to further authenticate users having the Mail-From Guardian method. However, as with most authentication policies, registrars do not release details of the policies to prevent against hackers devising ways to circumvent the policies.

Crypt-Password is NSI's second Guardian method, where the contact chooses a password and all request messages must include that password. When the contact first chooses his or her password, Network Solutions encrypts it as the master password. Each e-mail request must then be accompanied by a password. Network Solutions encrypts the password and compares it to the contact's previously encrypted master password. If they match, the request is processed.

---

63. *Frequently Asked Questions about Authentication*, NETWORK SOLUTIONS, *available at* http://www.networksolutions.com/en_US/help/guardian.jhtml (last visited Jan. 3, 2001).

64. Other registrars have similar authentication systems, but only NSI will be covered here.

To ensure that hackers cannot gain passwords from its system, after the master password is encrypted Network Solutions destroys the plaintext version of the password. From this point forward, even Network Solutions cannot determine what the contact's correct password is. If the contact forgets his or her password, the contact can ask NSI to reset the password. Network Solutions then follows a policy to attempt to ensure that the contact is legitimate before resetting the password. Of course, a hacker could abuse this password resetting procedure as part of his or her webjacking scheme. The webjacker could also try to guess the password or find an electronic or paper copy of the password kept by the contact.[65] For these reasons and other reasons, the crypt-password is not without its security concerns.[66]

The third and most secure Guardian method is PGP. PGP, which stands for Pretty Good Privacy, is a dual key, digital signature methodology. The specifics of PGP are beyond the topic of this paper and only a simplified explanation will be offered here.[67] PGP operates by a contact setting up his or her digital signature. The digital signature has two parts: a public key and a private key. The contact can freely distribute its public key to anyone who may receive digitally signed e-mail messages from the contract. To make distributions of the public keys simple, they are often posted on certification servers throughout the Internet. Although the public key is widely distributed, the contact must keep the private key confidential.

When the contract composes an e-mail request to Network Solutions, the contact 'signs' the message before sending it. To 'sign' the message, the entire e-mail message is encrypted with the contact's private key. The encrypted message is e-mailed to NSI and NSI attempts to decrypt the message using the contact's freely accessible public key. If the message is successfully decrypted, then

65. The FTC noted that "[m]any consumers use the same password at multiple places, or leave themselves reminders on yellow stickies, or use obvious passwords that are easily guessed, for example, one of the most commonly used passwords of all is 'password'." FTC Advisory Committee on Online Access and Security, Final Report - Second Draft, *at* http://www.ftc.gov/acoas/papers/ acoas-draft2.htm (May 8, 2000).

66. Webjackings have allegedly occurred even when password security has been in place. Harrison, *supra* note 37.

67. For a more comprehensive explanation of PGP and digital signatures, see *How PGP Works*, NETWORK ASSOCIATES, INC., *available at* http://www.pgpi.org/doc/pgpintro (last visited Jan. 3, 2001). This document is chapter 1 of the document *Introduction to Cryptography* from the PGP 6.5.1 documentation.

NSI is assured that the message is truly from the contact because the public key is the *only key*, which will decrypt messages encrypted with the contact's private key.

Using PGP can be bothersome because contacts are accustomed to the ease of traditional e-mail messaging. Thus, some registrants choose not to rely on PGP. Additionally, Network Solutions does not currently support PGP digital signatures from Windows-based computer systems. Only Unix-based systems are supported. This further limits the usage of PGP.

The three tier Guardian system is NSI's security strategy. Other registrars have their own ways to provide registrant protection. For example, Tucows' OpenSRS registrar system provides registrants with a username and password. All changes to the domain name registration must be accompanied by the proper username and password. While not as technologically hip as PGP digital signatures, passwords are easier to use and provide some safety. Of course, passwords are only safe as long as they are not easily guessed and are kept from disclosure. Tucows believes in its username/password method because it is unaware of any fakemail that has caused the OpenSRS to turn a domain name registration over to a fraudulent party.[68]

Once the registrar uses its internal procedures to authenticate the e-mail message, the registrar responds by carrying out the request. If a webjacker's fakemail message evades detection and is authenticated, then the registrar may unknowingly replace the current contacts with fake contacts having e-mail addresses controlled by the webjacker. Then the registrar may fulfill the webjacker's request to change the address of the name server to one that will resolve the domain name to the webjacker's website. Once these changes are processed, the domain name has been webjacked. All web traffic will be automatically directed away from the legitimate website and to the webjacker's website. The legitimate registrant will not be able to easily recover from the webjacking because its legitimate contacts are no longer authorized to make changes to the domain name registration.

*4. Laundering: Transferring The Registration To A New Registrar*

After the webjacker is successful in gaining control of the do-

68. Telephone Interview with Ross Rader, Director of Product Management, TUCOWS (Nov. 6, 2000).

main name, webjackers usually attempt to cover their tracks by 'laundering' the domain name. Transferring the registration to another registrar accomplishes the laundering.[69] Once the registration is transferred to a new registrar, the legitimate registrant must gain the assistance of both the original registrar and the new registrar in order to recover the domain name registration from the webjacker. This addition of another third party adds complexity to the recovery of the registration, thus slowing down the process.

Unfortunately, transferring registrars is quite easy. The webjacker contacts a new registrar and requests that the registration be transferred. The new registrar compares the credentials of the requesting party against the whois database. If the information matches—which of course it does after a webjacking—the new registrar submits the transfer request to the registry and the transfer is automatically completed. The former registrar, to whom the webjacker sent the fakemail message and duped into turning over control of the domain name, is sent an information message that the domain name will be transferred. However, the former registrar is either not asked for approval, or else the transfer occurs before the rightful registrant discovers that the domain name has been webjacked.

Although Network Solutions and other registrar recognize that the current registrar transfer policy assists webjackers in their con games, ICANN—who controls the transfer policy—has not yet acted to improve the transfer system.

### C. *What Do Webjackers Gain?*

As with any improper conduct, there are a multitude of reasons why webjackers do what they do. The International Trademark Association ("INTA") researched why cybersquatters knowingly register domain names that are confusingly similar to known trademarks. The term "cybersquatter" refers to a person who buys a domain name hoping to resell it for a large profit when the company wants to open a website with that domain name.[70]

Although not all webjackers are cybersquatters, there are many similarities between the two and thus the reasons for their actions

69. K.K. Campbell, *The Anatomy of a Domain Name Hijacking*, THE TORONTO STAR, June 8, 2000.

70. COMPUTER USER HIGH-TECH DICTIONARY, *available at* http://www.computeruser.com/resources/dictionary (last visited Jan. 3, 2001).

may be similar as well. INTA found that cybersquatter conduct is usually associated with: (1) extracting money from the trademark owner; (2) offering to sell the domain name registration to third parties; (3) using the well-known domain name in connection with a pornographic site; or (4) engaging in some sort of consumer fraud, including counterfeiting.[71] In addition to these four reasons, webjackers may also gain (5) revenge and (6) counter-culture respect.

Selling a domain name can be quite profitable. Warner Brothers was offered warner-records.com and other similar domain name for $350,000.[72] In January, 1999, Bank of America bought the domain name Loans.com for $3 million, and in 1999, ECompanies spent $7.5 million buying the domain name Business.com.[73] As proof that domain name sales are big business, a number of commercial websites exist that conduct domain name auctions.[74]

Selling a domain name is not the only way to make money. The webjacker turned cybersquatter may also gain money from the domain name as part of the booming on-line pornography industry. In the year 2000, experts predict the on-line sale of pornographic videos, pornographic web site subscriptions, and the like will generate $1.4 billion.[75] By capturing the registrant's domain name, the webjacker can easily redirect all traffic intended for the registrant's website to a pornographic website, in hope of encouraging more sales.

Not all webjackers plan on making money from the heist. According to registrar representatives, many the webjackers are just angry current or former employees who want to meddle with the

71. *Cybersquatting and Consumer Protection: Ensuring Domain Name Integrity, Before the United States Senate Committee on the Judiciary* (July 22, 1999) (statement of Ann Chaser, President of International Trademark Association), *at* http://www.senate.gov/~judiciary/72299ac.htm [hereinafter *Testimony of Chaser*].

72. *Id.*

73. Lisa Meyer, *URLiquidation*, REDHERRING.COM (Nov. 10, 2000), *at* http://www.redherring.com/investor/2000/1110/inv-url111000.html. The days where domain names sell for such large amounts may be over with the cooling of tech stocks. As evidence, the average sales price for a domain name from on-line auctioneer GreatDomains.com in August 2000 was $5,150; this is a 72 percent decrease from just one month earlier. *Id.*

74. For a list of domain name auctions, see Google Web Directory, *at* http://directory.google.com (last visited Jan. 3, 2001).

75. Kenneth Li, *Silicon Valley: Porn Goes Public*, THESTANDARD.COM, Oct. 31, 2000, *available at* http://www.thestandard.com/article/display/0,1151,19696,00.html (Datamonitor's estimate).

website and domain name to retaliate against the registrant.[76] Other webjackers are political protestors, such as when several domain names were taken over and the corresponding websites displayed a coat of arms bearing the title "Kosovo is Serbia."[77] Still other webjackings are done for fun, challenge, or obtaining respect from other hackers. As one expert said, "These [webjackers] are not 50 year olds. They're just showoffs."[78]

### *D. What Do Victims Stand To Lose?*

When a commercial website is webjacked, the company registrant is harmed. The company loses on-line contact with its customers. If the domain is redirected to an offensive site, such as a pornographic site, customers may be offended and turn away. Even if the domain name is quickly recovered, a company may lose customers as a result of the confusion and doubts about security.

Financial institutions and other companies transferring funds on the Internet may be vulnerable to direct monetary damage after a webjacking. For example, merchants who receive funds via the Internet could have their websites mirrored by the webjacker. A customer or client might unknowingly make payments to the webjackers. If a financial institution has its domain webjacked, the fraudulent website might ask clients for password information or other financial information that would allow the hacker to later access the client's accounts or fraudulently obtain credit in the client's name.

In July 2000, the Office of the Comptroller of the Currency ("OCC")[79] issued an alert to financial institutions, warning the banks to ensure their domain names are registered to them, under their control, and clearly communicated to their customers.[80] The alert pointed out that a webjacking could result in the loss of a bank's on-line identity and a misdirection of its customer communications.

---

76. Interview with Phil Sbarbaro, Chief Litigation Counsel, Network Solutions (Nov. 2, 2000).

77. Alana Juman Blincoe, *DNS Intrusions Spotlight Security Debate*, NETWORK NEWS, May 3, 2000, *available at* 2000 WL 7833925.

78. Sbarbaro, *supra* note 76.

79. The OCC charters and regulates approximately 2,400 banks in the U.S., which account for over half of the nation's banking assets. OCC News Release, NR 2000-53, July 19, 2000.

80. OFFICE OF THE COMPTROLLER OF THE CURRENCY, Alert 2000-9 (July 19, 2000).

## IV. OPTIONS FOR WEBJACKING VICTIMS

Registrants who are the victim of a webjacking have several options to recover the use of their domain name as well as to recover damages resulting from the incident. Each course of action has its advantages and disadvantages. Because webjackings are still a new and infrequent problem, the registrars, the authorities, and the courts are still learning how to respond appropriately.

### *A. Work With The Registrar*

Contacting the registrar is probably always the best first response after discovering a webjacking. Although the registrant and registrar enter into an agreement at the time of registration, the agreements offered by the various registrars offer little assistance to a webjacked registrant. For example, NSI's and Tucow's[81] agreements explicitly state that the registrar makes "no warranty that [its] services will meet [registrant's] requirements, or that the services will be uninterrupted, timely, secure, or error free."[82] In addition, Tucows also makes no warranty that "defects in the Service will be corrected."[83]

Although the registrars do not explicitly agree by contract to help a registrant recover a webjacked domain name, registrars realize that such a situation indeed carries a strong customer service element.[84] This is especially true because the registration business is no longer a monopoly, but rather a competitive field in which dozens of registrars battle for registration revenue. As a result, some registrars have set up special teams, which can be contacted with dispute resolution issues. For example, NSI's special team can be reached at www.domainmagistrate.com or by e-mail at "resolu-

81. TUCOWS operates OpenSRS, a wholesale domain name registration service. An ISP, web hosting company, IT consulting company or other e-commerce business can become a partner of the OpenSRS system. OpenSRS provides access to the domain registry and the tools necessary for the business to become a retail provider of domain name registration services. *See* www.opensrs.org *or* www.tucows. com (last visited Jan. 3, 2001).

82. *Service Agreement*, NETWORK SOLUTIONS, ¶ 18, *available at* http://www.networksolutions.com/legal/service-agreement.jhtml (last visited Jan. 3, 2001); *Form of Registration Agreement, Appendix A of Registration Service Provider Agreement*, TUCOWS, INC., ¶ 17, *available at* http://www.opensrs.org/OpenSRSDRAv3.0.0.pdf (last visited Jan. 3, 2001) [hereinafter *TUCOWS Registration Agreement*].

83. *TUCOWS Registration Agreement, supra* note 82.

84. Interview with Brenda Lazare, General Counsel, TUCOWS (Nov. 6, 2000).

tion@netsol.com." However, it appears that these special services are primarily directed towards trademark infringement disputes rather than for recovery from a webjacking.

Because a webjacking usually includes laundering by transferring the registration to a 'clean' registrar, it is important to try to prevent this transfer from occurring so that the problem can more easily be resolved.[85] Once the registrant contacts the registrar about the webjacking, and after the registrar freezes the domain name registration so that it will not be transferred to an unsuspecting new registrar, the next step is for the registrar to investigate and resolve the issue. The investigation may take seven to ten days, or even longer, to get fully resolved.[86]

Although registrars may certainly see the need to quickly assist with the resolution of webjackings, the registrars can be so overworked that it is difficult for them to more quickly resolve the problem. Unfortunately, by the time that the registration is returned to the registrant, the registrant may have lost both money and customers.

One of the authors has experienced first hand the frustrations that may be encountered in working with a busy registrar after a webjacking. A company purchased the domain name registrations and other assets of an Internet service provider (ISP) and hired the principal to act as president of its subsidiary. After the president failed to properly perform his duties for six months, the company terminated him in the Spring of 2000. The former president, who controlled the server for a number of the domain names, immediately webjacked many of the company's domain name registration through the registrar by changing the domain servers. For some of these changes, the former president was still listed as the administrative contact and so easily submitted a seemingly proper request to the registrar for the registration changes. For other registrations in which he was not the administrative contact, he apparently used fakemail to submit the requests.

Upon capture of the domain name registrations, and rerouting them to servers under his control, the former president was able to obtain and control all of the electronic traffic and e-mails directed to the webjacked domain names. The registrar's customer service department was contacted. However, the registrar was slow

85. *Id.*
86. *Id.*

to respond and not very cooperative. Even after the domain registrations were returned to the company after a number of days, the problems were not fully resolved. Although the domain name registrations had been updated to use encrypted passwords, the former president somehow managed to get the registrars system to again change the name servers. Some of the domain name registrations were changed between the proper registrant and the former president more than once over the course of several weeks. Several months later, the former president attacked again. Although most of the domains were eventually regained, it was only after lengthy struggles with the registrar. Because of this problem, the registrant lost a number of its customers and was forced to abandon certain of its service offerings.

### *B. Consider Using The UDRP–Even Though It Was Not Intended For Webjackings*

In addition to working directly with a registrar, the victim of a webjacking may wish to avail itself of the Uniform Dispute Resolution Policy ("UDRP" or "Policy") adopted by all registrars. The UDRP is a relatively quick and inexpensive way of resolving domain name disputes, although it primarily intended to apply to cybersquatting and trademark infringement issues.

The Policy was adopted by ICANN in response to a report by the World Intellectual Property Organization ("WIPO") that covered several topics, including the recommendation that all registrars follow a uniform dispute resolution policy because of the disputes surrounding cybersquatting.[87] By registering a domain name, the registrant agrees to be bound by the registrar's current dispute resolution policy.[88] Through this Policy, an aggrieved complainant can file a complaint through an approved administrative dispute resolution service provider. The complainant must allege that a registrant registered in bad faith a domain name for which the registrant has no legitimate interest, and which is identical or confusingly similar to a trademark of the complainant.[89] The Policy was

87. *Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy, at* http://www.icann.org/udrp/udrp-schedule.htm (last modified Oct. 17, 2000).

88. *NSI's Service Agreement, Clause 8 "Domain Name Dispute Policy," at* http://www.network.solutions.com/legal/service-agreement.jhtml.

89. *Uniform Domain Name Dispute Resolution Policy*, NETWORK SOLUTIONS, § 4, *available at* http://www.domainmagistrate.com/dispute-policy.html (Oct. 24,

intended to resolve cybersquatting and other trademark disputes in domain names.[90]

Since the adoption of the Policy, three organizations have been accredited as dispute resolution providers:[91] (1) the Disputes.org/eResolution.ca consortium,[92] (2) the WIPO Arbitration and Mediation Center,[93] and (3) the National Arbitration Forum.[94] Through November 2000, at least 230 cases have been decided by Disputes.org/eResolution.ca consortium panelists.[95] Similarly, at least 704 cases have been decided by National Arbitration Forum panelists,[96] and 730 through WIPO.[97] These numbers indicate that the Policy is indeed being used to resolve disputes with domain name registrations.

Although the UDRP was intended to resolve trademark disputes, it appears that in October 2000, the Policy was first used to recover from a domain name that was webjacked after a fakemail request was sent to the registrar.[98] In that case, Gerald Mikkelson, doing business as Internet Host Corporation, registered the domain name HOST.COM. Mikkelson was listed with the registrar as both the administrative and billing contact. On May 24, 2000, nearly six years after Mikkelson first registered the domain name, an e-mail message was sent to the registrar requesting that the administrative, technical and billing contacts be changed. The e-mail also requested that the address of the name servers be altered. The change request was refused–probably because the e-mail message's return address was not the same as the current administrative con-

---

1999).

90. Sbarbaro, *supra* note 76.

91. *Domain Magistrate Providers, at* http://www.domainmagistrate.com/ providers.html#national (last visited Jan. 3, 2001).

92. http://www.eResolution.com (last modified Jan. 4, 2001).

93. http://arbiter.wipo.int/center/index.html (last visited Jan. 4, 2001).

94. http://www.arbforum.com/domains/ (last visited Jan. 4, 2001).

95. *Domain Name Administrative Decisions,* ERESOLUTIONS, *available at* http://www.eresolution.com/services/dnd/decisions.htm (last visited Jan. 4, 2001). Under ICANN Policy, Section 4(j), except for exceptional circumstances, all Domain Name decisions must be made publicly available. *Id.*

96. Decisions can be viewed by going to http://www.arbforum.com/domains and then clicking on the "domain name dispute Proceedings and Decisions" link (last visited Jan. 4, 2001).

97. *Case Results,* WIPO, *available at* http://arbiter.wipo.int/domains /statistics /results.html (last modified Sept. 2000).

98. Agent Host Co. v. Host Dot Com Investments, No. AF-0343 (Oct. 16, 2000), *available at* http://www.eresolution.com/services/dnd/decisions/0343.htm.

tact for the domain name (i.e. Mikkelson).[99]

Five days later, the registrar received a second e-mail message. This message appeared to originate from Mikkelson. The message requested that the contacts and domain name servers be changed. Believing the request to be authentic, the registrar made the changes after approval was given by a follow-up e-mail message, again appearing to originate from Mikkelson. Once the changes were made, the domain name was laundered by being transferred to a new registrar. Some time later, Mikkelson discovered that his domain name had been webjacked.

Mikkelson filed an on-line complaint through eResolution on August 24, 2000. Soon thereafter, an eResolution clerk notified the respondent by an e-mail message sent to postmaster@host.com and the recently changed electronic address for the administrative contact. In addition, the complaint and accompanying materials were sent via registered mail to the respondent in Canada. The respondent did not respond to any of the notices.

The panelist appointed to the case noted in his decision that to obtain relief under the UDRP, the complainant must prove three elements, namely that (i) respondent's domain name is identical or confusingly similar to a trademark in which the complainant has rights; (ii) respondent has no right or legitimate interests with respect to the domain name; and (iii) respondent's domain name has been registered and is being used in bad faith.[100]

In analyzing the allegations before him, the panelist first determined that because respondent controls the identical domain name through which complainant previously performed business, confusion is certain. Although the panelist failed to state that the complainant had trademark rights to the domain name, because Mikkelson operated a business over the Internet with the domain name, it appears that he had indeed obtained common law trademark rights to the mark HOST.

Second, the panelist searched for any legitimate interests by the respondent in the domain name. Noting that a thief does not have good title to what he steals, the panelist checked respondent's actions against the indicia set forth in the UDRP of what demonstrates rights in a domain name. Unable to find any indicia or explanation by respondent, the panelist determined that respondent

99. In fact, the return address was not a genuine address for anyone. *Id.*
100. *Id.*

had no legitimate interest in the HOST.COM domain name.

Third, the panelist determined that the respondent had registered the name and was using it in bad faith. Although the UDRP provides factors, which indicate registration and bad faith use, most of these factors relate to situations involving commercial competitors. Because this was not the case, the panelist was forced to look outside of the non-exclusive factors of the Policy. Stating "it would also be difficult to say a thief acts other than in bad faith," and pointing to how respondent gained the registration of the domain name from the complainant (i.e., the fakemail messages), the panelist held that the respondent demonstrated the requisite bad faith.

Because complainant proved all three elements—that the domain name is identical, that respondent had no legitimate interest in the domain name, and that the respondent acted in bad faith—the panelist ordered HOST.COM transferred back to complainant.

With the HOST.COM case, there is now precedent that the UDRP can be relied upon to recover from a webjacking. However, because the intent of the Policy was not for this purpose, it is unknown whether subsequent panelists will allow webjacking cases to be resolved in this fashion. In addition, because the UDRP does not provide for expedited relief and relief is limited to the transfer of the domain name (no damages are allowed), victims of webjacking may wish to rely upon another option for quicker relief and to recover damages. Significantly, by submitting a dispute through the UDRP, the registrant purportedly releases the registrar from liability, which may be the only real source from which to recover monetary damages.[101] It is not known whether this release would be enforced by a court.

### C. *Work With Authorities*

For egregious cases, a victim of webjacking should also contact the authorities, however, as with anything related to the Internet, webjacking is a new and unfamiliar territory for many attorneys, police officers, and federal agents from the Secret Service, FBI, or other federal agencies. As one business consultant noted, "This is like the Wild West days."[102] Thus, although there are now federal

101. *Uniform Domain Name Dispute Resolution Policy*, ICANN, § 4(h), *available at* http://www.icann.org/udrp/udrp-policy-24oct99.htm (last modified Oct. 24, 1999).

102. K.K. Campbell, *supra* note 35.

statutes criminalizing certain Internet activity,[103] authorities may be slow or reluctant to get involved.

### *D. Seek Expedited Relief In Court*

When subjected to a webjacking, in addition to trying to rectify the situation with the registrar and the authorities, the registrant may immediately seek expedited injunctive relief or damages from a court. The disadvantages of suing a webjacker include: (1) it can be expensive, (2) it can take a long time, (3) the webjacker may have no assets, and (4) it may not be possible to identify the webjacker or obtain jurisdiction over him or her.

There are a number of federal statutes and common law causes of action that may provide relief, including:

- the Computer Fraud and Abuse Act;[104]
- the Electronic Communication Privacy Act;[105]
- the Anti-Cybersquatting Consumer Protection Act;[106]
- the Federal Lanham/Trademark Act;[107]
- unfair competition;
- the Copyright Act;[108]
- fraud, theft, or conversion;
- tortious interference with contract and prospective business advantage;
- misappropriation of trade secrets; and
- the Racketeer Influenced and Corrupt Organizations ("RICO") Act.[109]

Thus, depending on the circumstances, a domain name owner may well have state or federal protection. These causes of actions are briefly discussed below.

#### *1. The Computer Fraud And Abuse Act*

The Computer Fraud and Abuse Act was adopted to "strengthen protection against computer crimes."[110] The Act covers

103. Such statutes, such as the Computer Fraud and Abuse Act, are discussed in Section IV (4), below.
104. 18 U.S.C. § 1030 (2000).
105. *Id.* §§ 2511, 2520, 2701, 2707.
106. 15 U.S.C. § 1125(d) (2000).
107. *Id.* §§ 1051-72, 1091-96, 1111-29.
108. 17 U.S.C. §§ 101-1332 (2000).
109. 18 U.S.C. §§ 1961-68 (2000).
110. United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

only crimes involving protected computers of a financial institution or the United States Government, or crimes using interstate or foreign commerce or communication.[111] Therefore, protection under the Act may not be available to some businesses that become webjacking victims, although most Internet transactions will involve computers used in Interstate communications.[112]

Under the Act, a person who "knowingly and with intent to defraud, accesses a protected computer without authorization" and does so in order to continue some type of fraud, and who obtains at least $5,000 in value, is in violation of the Act.[113] A violation is punishable by up to five years of imprisonment, a fine, or both.[114] If the person is convicted under the Act after a prior similar conviction (or even after a prior attempt at such prohibited access), they can be imprisoned for up to ten years.[115] In addition, anyone who is damaged as a result of a violation of the Act may bring a civil action against the violator for compensatory economic damages as well as injunctive or other equitable relief.[116] Thus, a registrant can bring an action (within two years) against a webjacker.

Robert Morris is the most well-known defendant so far convicted under the Act.[117] In 1988, Morris released a worm onto the Internet. Although he was attempting to "demonstrate the inadequacies of current security measures on computer networks," his worm caused many computer systems around the country to crash or hang.[118] Morris was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and costs of his supervision.[119]

### 2. *The Electronic Communication Privacy Act*

The Electronic Communication Privacy Act ("ECPA") was enacted to "address the legal privacy issues that were evolving with the growing use of computers and other new innovations in electronic

111. 18 U.S.C. § 1030(e)(2).
112. The U.S. Secret Service has authority to investigate offenses involving financial institutions. 18 U.S.C. § 1030(d).
113. *Id.* § 1030(a)(4).
114. *Id.* § 1030(c)(2)(B).
115. *Id.* § 1030(c)(3)(A), (B).
116. *Id.* § 1030(g).
117. United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).
118. *Id.* at 506.
119. *Id.*

communications."[120] It was intended to address the new privacy issues brought about by the growing amount of electronic communication, such as e-mail. The ECPA addresses both government surveillance and eavesdropping by private parties.[121]

The ECPA includes, among other things, prohibitions against unlawful access to stored communications[122] and interception and disclosure of wire, oral, or electronic communications.[123] The Act prohibits intentionally accessing, without authorization, a computer system through which electronic communication is provided.[124] Also prohibited is intentionally exceeding one's authorization to access such a computer system, and as a result, obtaining, altering, or preventing authorized access to an electronic communication that it is stored in the computer.[125] If the access was for commercial gain or advantage, or for malicious damage, punishment can be a fine and/or up to one year of imprisonment for the first offense and up to two years for subsequent offenses.[126] If access was for some reason other than commercial gain, commercial advantage, or malicious damage, the party can be fined and/or imprisoned for not more than six months.[127]

The ECPA also provides two private causes of action that the registrant may bring against the webjacker. First, under the ECPA, anyone who is aggrieved by a intentional violation of the ECPA (including a provider of electronic communication service or a subscriber) may recover preliminary and other equitable or declaratory relief, actual damages (including profits made by the violator), punitive damages, and reasonable attorneys' fees and other litigation costs.[128]

Second, any person whose electronic communication is intercepted, disclosed, or intentionally misused, may obtain preliminary or other equitable or declaratory relief, damages (including punitive damages) and reasonable attorney's fees and other litigation

120. *Jones Telecommunication & Multimedia Encyclopedia*, JONES INT'L, *available at* http://www.digitalcentury.com/encyclo/update/ecpa.html (last visited Jan. 4, 2001) [hereinafter *Jones Telecommunication & Multimedia Encyclopedia*].
121. *Id.*
122. 18 U.S.C. § 2701(a)(1)-(2).
123. *Id.* § 2511(1).
124. *Id.* § 2701(a)(1).
125. *Id.* at (a)(2).
126. *Id.* at (b)(1).
127. *Id.* at (b)(2).
128. *Id.* at (b), (c).

costs.[129] A civil action for this relief must be started within two years after which the registrant had reasonable opportunity to discover the violation.[130]

*3. The Anti-Cybersquatting Consumer Protection Act*

Since the mid 1990s, some people have had part-time or full-time businesses registering and then attempting to sell domain names. For example, in May 2000, the "engineering.org" domain name was purchased through an on-line auction for nearly $200,000.[131] These generic domain names are valuable "cyber real estate" for which many companies may compete to use as their domain name. However, many domain names that have been offered for sale are not generic, but rather are trademarks of famous companies.

As discussed above in Section III(C)(1), cybersquatters reserve domain names that are in the form of company names (such as britishairways.com) so they can make money by reselling the domain names to the associated companies or to a competitor of the trademark. For example, in 1999, Amazon.com was offered the "amazon.gr" domain name for $1.6 million.[132]

The Federal government responded to the problem of cybersquatting in November 1999 by enacting the Anticybersquatting Consumer Protection Act.[133] The Act articulated a strong federal policy against registering domain names for the purpose selling those domain names to trademark owners.[134] The Act was also intended to protect consumers from deception. The Act's co-sponsor, Senator Orin Hatch, pointed out:

> If consumers cannot rely on brand names on-line as they do in the world of bricks and mortar store-fronts, few will

129. *Id.* § 2520(a)-(b).

130. *Id.* § 2520(e).

131. Press Release, Robert Balazy, Afternic.com, Most Expensive URL Ever in the Dot-Org Domain is Sold Via Afternic.Com (May 8, 2000), *at* http://www.afternic.com/ index.cfm?a=company&sa=press&tab =display&id=000508.

132. Elizabeth Clampet, *Amazon.com Sues Alleged Cybersquatter*, INTERNETNEWS, Aug. 18, 1999, *available at* http://www.internetnews.com/ec-news/article/0,,4_185111,00. html.

133. The Act amended the end of Section 43 of the Trademark Act of 1946. 15 U.S.C. § 1125.

134. Joel Voelzke, *New Cybersquatting Law Gives Trademark Owners Powerful New Weapons Against Domain Name Pirates*, OPPENHEIMER WOLFF & DONNELLY LLP, *available at* http://www.oppenheimer.com/internet/cybersquatting.shtml (last visited Jan. 4, 2001).

> be willing to engage in e-commerce. Those who do will bear substantial risks of being confused or even deceived. Few Internet users would buy a car, fill a prescription, or even shop for books on-line if they cannot be sure who they are dealing with.[135]

Under the Anti-Cybersquatting Consumer Protection Act, a cybersquatter is liable to a trademark owner if the cybersquatter, in bad faith, intends to profit by registering or using a domain name that is identical or confusingly similar to a trademark.[136] There are several factors enumerated in the Act to be used in determining bad faith. These include, among other factors: (1) the alleged cybersquatter's trademark rights in the domain name; (2) the cybersquatter's intent to divert consumers to a website which could harm the goodwill of the mark or tarnish its image; (3) the cybersquatter's offer to sell the domain name registration without previously using it for bona fide sales or offers of goods or services; (4) the cybersquatter's act of giving false or misleading contact information to the registrar; and (5) the cybersquatter's knowledge that the domain name is identical or confusingly similar to another's distinctive trademarks.[137] In many webjackings, the webjacker may indeed intend to profit by using a domain name that is identical to another's trademark. In these cases, the webjacker is also a cybersquatter and the registrant may seek protection under the Act.

If the registrant can prove the webjacker's bad faith, a court may order the webjacked domain name registration forfeited, cancelled or transferred back to the rightful registrant.[138] This is in addition to any other applicable civil action or remedy.[139] Because it is often difficult for a trademark owner to obtain *in personam* jurisdiction over the webjacker, the Act authorizes a trademark owner to file an *in rem* civil action against the webjacker/cybersquatter.[140] Such an *in rem* action may take place in the judicial district of the domain name registrar that registered or assigned the domain name.[141]

---

135. *Satellite Television and Intellectual Property Legislation: Hearing on H.R. 1554 Before the Senate Appropriations Committee*, 106th Cong. (Nov. 19, 1999) (statement of Senator Orrin G. Hatch, co-sponsor of the Anti-cybersquatting Consumer Protection Act), *available at* http://www.senate.gov/~hatch/sat_statement.html.

136. 15 U.S.C. § 1125(d)(1)(A) (2000).

137. *Id.* § 1125(d)(1)(B)(i).

138. *Id.* § 1125(d)(1)(C).

139. *Id.* § 1125(d)(3).

140. *Id.* § 1125(d)(2)(A).

141. *Id.*

*4. The Federal Lanham/Trademark Act*

The Trademark Act, which is also known as the Lanham Act,[142] protects a trademark owner from trademark infringement. To infringe a registered mark, a party must use the same or a confusingly similar mark in commerce in connection with the sale, offering for sale, distribution, or advertising of any goods or services, in a manner that is likely to cause confusion, or mistake or to deceive.[143]

While use and registration of a domain name without more will not generally constitute trademark usage, a domain name can, under certain circumstances, function as a trademark.[144] To be a trademark, the domain name must identify and distinguish goods, services, and their sources from the goods or services manufactured or sold by others.[145] For example, suppose "Big City Bank" is a registered service mark of a financial services provider operating under the name Big City Bank. Suppose the bank's domain name www.bigcitybank.com assists consumers to distinguish Big City Bank's banking services from competing services offered by other financial institutions.

If a domain name serves as a trademark and the webjacker seizes control of that domain name, causing confusing or deceiving consumers, the webjacker may be liable for trademark infringement. For example, if www.bigcitybank.com is webjacked and the webjacker installs a website which may confuse customers when they are automatically redirected to the webjacker's website, then the Big City Bank service mark has been infringed.

Liability for infringement of a registered trademark may be damages, including costs and attorneys' fees, incurred by the domain name registrant and trademark owner as a result of such action.[146] The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.[147]

Under the Lanham Act, a registrant may also claim that the

142. Strictly speaking, the Anti-Cybersquatting Consumer Protection Act is part of the Lanham Act as well.

143. 15 U.S.C. § 1114(1)(a).

144. The Trademark Office's Examination Guide No. 2-99 (Sept. 29, 1999) (stating "[a] mark composed of a domain name is registrable as a trademark or service mark only if it functions as a source identifier"); *In re Eilberg*, 49 U.S.P.Q.2d 1955, 1957 (TTAB 1998), *available at* 1998 WL 1015894.

145. 15 U.S.C. § 1127.

146. *Id.* § 1114(2)(D)(iv).

147. *Id.*

webjacker is diluting the trademark, if the trademark is famous.[148] A trademark is diluted when the uniqueness of the mark is diminished,[149] or when the mark is "linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context."[150] The trademark owner can seek injunctive relief for dilution.[151] If the trademark owner can prove that the webjacker willfully intended to dilute the mark, the owner of the famous mark is also entitled to other remedies.[152] Unfortunately, noncommercial use of the mark by the webjacker may not be actionable as trademark dilution.[153]

*5. Unfair Competition*

If a domain name is not a federally registered trademark, then the registrant still may have a claim under the Lanham Act for unfair competition.[154] Unfair competition prevents anyone from using a term, name, symbol, or other device in connection with any goods or services that is likely to cause confusion, cause mistake, or to deceive a consumer as to the affiliation, connection, or association of that person with a third party.[155] Unfair competition also prevents such confusion, mistake, or deception with regard to the origin, sponsorship, or approval of the goods or services by a third party.[156]

In a webjacking situation, the webjacker fraudulently takes control of the domain name. For a successful claim of unfair competition, the original registrant must prove that the webjacker's website associated with the domain name is used in some form for commerce of goods or services. Secondly, the rightful registrant must show either: (1) that these goods and services are not the registrant's but that consumers would be confused or deceived into believing otherwise; or (2) that these goods or services are indeed the registrant's, but that consumers would be confused or deceived into believing that there was some affiliation or association between

148. *Id.* § 1125(c).
149. This is known as "blurring." Siegrun D. Kane, TRADEMARK LAW, A PRACTITIONER'S GUIDE, § 8:2.4[B] (PLI 3rd ed. 1999).
150. This is known as "tarnishment." Kane, *supra* note 149 (citing Deere & Co. v. MTD Prods., Inc., 41 F.3d 39, 43 (2d Cir. 1994)).
151. 15 U.S.C. § 1125(c)(1).
152. *Id.* at (c)(2).
153. *Id.* at (c)(4)(B).
154. *Id.* at (a).
155. *Id.* at (a)(1)(A).
156. *Id.*

the registrant and the webjacker.[157]

In addition to the Lanham Act, the Federal Trade Commission ("FTC") is empowered and directed to prevent unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.[158] The FTC may commence a civil action against any entity violating the rules against unfair or deceptive acts or practices, seeking a civil penalty of up to $10,000 per violation.[159] The FTC may also obtain temporary restraining orders against such parties.[160]

The FTC has indeed been interested in Internet related crimes. From 1995 through early 2000, the FTC brought over "100 Internet-related cases, obtained permanent injunctions against dozens of Internet-related schemes, collected over $20 million in redress for victims of online fraud, and froze another $65 million in cases currently in litigation."[161]

*6. Copyright Act*

The Copyright Act protects an author's work when the work is placed in a fixed medium of expression.[162] A copyright owner enjoys the exclusive right to exclude others from such things as reproducing copies of the work, to preparing new, derivative works based on the work, and distributing copies of the work.[163]

Although the Copyright Act would not be used as a primary mechanism to recover from a webjacking, if the webjacker has also created a modified version of the original website (as in the AJ Park example previously discussed), a copyright infringement case can be brought against the webjacker. To prevent the continued infringement, a court can grant both temporary and permanent in-

157. Consumers could be led to believe that there is a connection because after a webjacking, the webjacker appears on the whois database as the Administrative contact for the domain name registration. Some registrars, including Network Solutions, allege that the Administrative Contact is the *actual* registrant. Thus, a consumer might be confused into believing that the webjacker owns the website that advertises the goods or services from the rightful registrant.

158. 15 U.S.C. § 45(a).

159. *Id.* § 45(m)(1)(A).

160. *Id.* § 53(b).

161. *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, A Report of the President's Working Group on Unlawful Conduct on the Internet,* Appendix B, (Mar. 2000), *at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.

162. 17 U.S.C. § 102(a).

163. *Id.* § 106.

junctions.[164] Actual damages, profits gained by the infringing webjacker, statutory damages of up to $100,000, attorney's fees and costs, are also available.[165]

*7. Other Causes Of Action*

Fraud, theft, conversion, tortious interference with contract, prospective business advantage, and misappropriation of trade secrets are some of the other causes of action which may be brought against the webjacker under common law. Under certain circumstances, webjacking may even violate RICO's prohibition against wire fraud, bribery, and extortion.[166] Treble damages for RICO violations are available through civil actions.[167] For example, in 1999, Amazon.com claimed that a Greek company violated federal RICO statutes in connection with its use of the amazon.gr domain name.[168]

*E. Seek Relief Against Registrars?*

A damaged webjacking victim may not be able to identify or obtain jurisdiction over a defendant, or the defendant may have no assets. Such a victim might consider an action against a registrar if the registrar was negligent in allowing the webjacking to occur. For example, some webjacked parties allege that the registrars do not always follow their standard operating procedures and so the registrar should be liable for damages resulting from its own negligent actions. As one victim said, "The fact is that if you pay [the registrar for your registration], you are presuming that in the morning the last thing you have to worry about is whether you own your domains."[169]

Although the case law is not well developed, initial decisions have been reluctant to find registrars liable for their actions in connection with domain name registrations. In the *Lockheed Martin Corp. v. Network Solutions, Inc.* case,[170] the Ninth Circuit likened the role of NSI to that of the U.S. Postal Service and found that the reg-

164. *Id.* § 502(a).
165. *Id.* § 504.
166. 18 U.S.C. §§ 1961-68.
167. *Id.* § 1964.
168. Clampet, *supra* note 132.
169. *Nike Web Hijacking Sparks Finger-Pointing; Company Trades Blame with NSI and Host*, COMPUTERWORLD, July 10, 2000, at 21(1).
170. 194 F.3d 980 (9th Cir. 1999).

istrar could not be held liable for contributory trademark infringement by reason of its registration of a third party's service mark. If the registrant seeks trademark infringement damages, the Trademark Act explicitly exempts registrars from liability absent a showing of bad faith intent to profit from such registration.[171] Similarly, in the *Kremen v. Cohen* case,[172] the court granted NSI summary judgment on a claim that it improperly transferred the domain sex.com pursuant to a forged letter. The court found, among other things, that a domain name is not property subject to a conversion claim. Other courts have likewise been hesitant to find registrars liable.[173]

## V. REGISTRARS' (RE)ACTIONS TO COMBAT WEBJACKING

Statistically, webjackings do not occur very often. Although NSI processes around 30,000 change requests each day, it contends that there are only one or two webjackings (or similar problems) each month.[174] Similarly, Tucows reports that its OpenSRS system handles over 2,000 change requests a day and has not yet experienced a webjacking.[175] Because webjackings account for such a small portion of their transactions, and because the registrars are hounded with other issues needing resolution, registrars have not issued any strong, new policies to combat webjacking, although some registrars have made improvements to their policies.

Registrars state that they do have certain checks that work to detect fraudulent change requests during message authentication. To maintain effectiveness, details of most of these anti-fraud mechanisms are not disclosed. However, one method that at least one registrar has set up is the use of a series of queues for handling change requests, where the queues are used for different types of domain names.[176] The first queue is for open transfers. The majority of domain name registrations have been assigned to this queue. Transfers from the first queue are processed by the registrar's

171. 15 U.S.C. § 1114(2)(D)(iii).

172. No. C 98-20718JW, 2000 WL 708754 (N.D. Cal. May 30, 2000).

173. Beverly v. Network Solutions, Inc., 49 U.S.P.Q.2d 1567, 1574 (N.D. Cal. 1998); Oppendahl & Larson v. Network Solutions, Inc., 3 F. Supp. 2d 1147, 1164 (D. Colo. 1998); Academy of Motion Picture Arts & Sciences v. Network Solutions, Inc., 45 U.S.P.Q.2d 1463, 1467 (C.D. Cal. 1997).

174. Sbarbaro, *supra* note 76; *see also NSI's Webjacking Epidemic*, Wired News 3:00 a.m. (June 8, 2000).

175. Rader, *supra* note 68.

176. *Id.*

automated system.

The second queue is for well known domain names, which might be very appealing for webjacking or other hijinks. Some well known domain names, such as msn.com or att.com, have been placed into this second queue, which is for restricted transfers. Restricted transfers are processed manually to ensure that webjackings do not disturb such busy sites.

Outdated domain name registrations form the third queue. Outdated registrations often are so old that the contact information may not be accurate. Often, the e-mail addresses listed for the contacts are no longer even valid addresses. When a change requests is made for outdated registrations, the registrar uses extra effort to communicate with the listed contacts, including by phone or my regular mail. If there is no response to these inquiries, the change request is not be processed.

Some of the registrars have also discussed among themselves how to more easily help a registrant recover from a webjacking. Because usually a webjacking includes the transfer of a domain name registration to a new, unsuspecting, registrar, some registrars now cooperate with one another, allowing the webjacked registration to be returned to the original registrar. Although this is a lost customer for the new registrar, it allows the original registrar to return to the rightful owner control over the domain name.[177]

Registrars are also reacting to webjackings by educating the public in how to avoid being a webjacking victim. Network Solution's idNames division now offers a continuing legal education class ("CLE") in domain name basics for attorneys.[178] By educating counsel on the importance of security measures for the registrations, Network Solutions hopes to diminish the potential for webjacking problems.

Although the registrars have not issued any major changes to prevent webjacking, that is not to say that the registrars view webjacking as unimportant. As previously discussed, at the very least, registrars view webjacking has an important customer service and public relations issue because registrars suffer from bad press for every webjacked domain name registration that gets published in the news.

In the end, registrars maintain that they are not the proper en-

177. *Id.*

178. See announcement on-line, *at* http://www.nsol.com/news.

tity to issue major changes to prevent webjacking. Many believe that this authority rests instead with ICANN.

## VI. WHAT SHOULD BE DONE?

Unfortunately, there is no one answer on how to end webjackings. It is a multi-faceted problem in which each of the parties—the registrants and their counsel, the registrars, ICANN, and the authorities—must work to take care of their portion of the solution. There are, however, a few "big picture" changes that would help to minimizing the effects of webjacking.

### *A. ICANN Should Improve Policies*

ICANN should be encouraged to consider improvements to certain policies, especially the policy concerning registration transfers, and the policy for domain name dispute resolution.

The current procedure for domain name registration transfers is basically:

- Registrant sends transfer request to new registrar.
- New registrar sends transfer request to the registry.
- Registry checks the transfer request information against the whois database. If the transfer appears legitimate, the transfer is authorized.
- Registry transfers the registration to the new registrar.
- Registry may send a notice of the transfer to the previous registrar.

This procedure fails to protect against webjacking because the previous registrar is not given time to learn of and to report webjackings to the registry. An improvement to the transfer procedure would be to have the registry require a waiting period, perhaps of one week, between any change to the registration and a transfer to a new registrar. While such a waiting period may inconvenience some registrants, it would remove some obstacles currently faced in resolving webjacking situations.

ICANN should also react to the HOST.COM case, which was recently issued under the UDRP and discussed above. The UDRP should be sanctioned (and appropriately modified) for use in webjacking cases in addition to its current purpose for trademark infringement and cybersquatting problems.

### B. *Law Enforcement Should Be Given Sufficient Resources To Combat Computer Crimes*

Given the complexity and technical nature of the means by which webjackers act, authorities may be slow or reluctant in computer related crimes to get involved. Authorities may also be concerned over statutes that restrict their interception of electronic communications.[179]

### C. *Registrants Should Take Preventive Steps*

It would take a large and influential group of Internet gurus to get a more secure protocol developed and approved to replace SMTP, so that e-mail messages would be more difficult to forge. It would take a call center the size of a small town for a registrar to replace their automated procedures with personnel manually checking and approving each change or transfer request.[180] Fortunately, many webjackings can be prevented without resorting to any of these costly measures, although the onus is on the registrant to follow the procedures. As one Ernst & Young expert said, "The solution is look after yourself, because basically the sheriff can't."[181]

To combat webjacking, registrants should execute a four-fold plan by: (1) using a good registrar, (2) maintaining security, (3) managing registrations and paperwork, and (4) educating their counsel and employees. First, registrants should find a registrar that uses good authentication measures.[182] Unfortunately, many registrars have a wholly inadequate authentication system.[183] Although digital signatures have been the promise of the e-commerce for the past several years, digital signature technology has not become user friendly enough to be adopted by the general public. However, a simple password system, although a low-tech alternative to PGP e-signatures, may provide adequate authentication and may counter many webjacking attempts.

---

179. *E.g.*, 42 U.S.C. § 2000aa (2000).

180. The registrar Melbourne IT is marketing itself as a more secure registrar, stating that all domain name registration transfers will be first checked by a human. Jenny Sinclair, *Alarm on Hijackings*, THE AGE, June 13, 2000, *available at* 2000 WL 21652726. This noble policy may be impractical due to the large number of transfers that occur in the world each day.

181. Susan Pigg, *More Web Sites Caught in Net Scam*, THE TORONTO STAR, June 2, 2000 (quoting Chris Anderson).

182. Rader, *supra* note 68.

183. *Id.*

In addition to its authentication policies, registrants should look for a registrar with good customer service capabilities. If a problem does develop with the registration, registrants should be certain that they will be able to contact the registrar and receive quick assistance.

Second, corporate registrants should draft and follow proper security measures. In addition to the passwords remaining confidential and not easy to be guessed, a policy must be put in place to ensure that contact information is updated when the prior contact person leaves the company. Some webjackers are really former employees looking for revenge, and disabling a company's website can be an easy target. To safeguard against an internal attack, registrants should ensure that the registrar is promptly notified to remove the contact person before that person leaves his or her employment.

Another precaution that registrants can take to protect their rights is to manage their registrations and keep associated paperwork. In the 1990's, businesses began creating the role of a CIO (Chief Information Officer). Today, information management has been promoted as a critical task. Securing web sites from webjacking and other hazards is a full-time job.[184] This is especially true now that many large corporations have dozens, if not hundreds, of domain name registrations. Now that registrars offer multi-lingual registrations as well as country level registration in nearly 200 countries outside of the United States, corporations will continue to acquire more domain name registrations. Corporations should set up CIO or other formal positions charged with domain name management and security.

As part of the security program for a corporation, a new service offered by SnapNames may be useful. SnapNames provides monitoring of domain name registrations "to reduce the impact of domain-related catastrophes."[185] As soon as a registration is altered (such as the name server or the contact information), SnapNames' SnapBack system will send e-mail alerts to three pre-designated people. The alerts show what the domain name registration looked like prior to the change and after the change. Such quick notifications may allow the registrant to recover from a webjacking before

184. *Lock Up Your Data*, 5 MATERIAL HANDLING MANAGEMENT 30 (May 2000).

185. Press Release, *SnapNames, SnapNames and Major Registrars Partner in New Domain Protection Technology* (Nov. 15, 2000) (quoting Len Bayles), *available at* www.snapnames.com/press_partnersPR.html.

the registration changes propagate through the Internet.

Part of the domain name management includes maintaining a paper copy of the registration activities. The e-mail notifications that are received when domain names are set up, copies of the requests for registrant data changes, and the like, make a paper trail that can be offered as proof of registration ownership, if necessary. Registrars are surprised when multi-million dollar companies are unable to produce a paper copy of an e-mail that shows their legitimate interests in a domain name registration, especially since domain names are so valuable to many corporations.

Fourth, in-house, firm counsel, and employees who will be the administrative, billing, or technical contacts for registrants must be fully trained regarding the security issues in domain name registration. The Internet is becoming such a fundamental aspect of so many areas of everyday business, that soon all attorneys will need to have more than a cursory understanding of webjacking and other Internet law issues. And because it is easier to prevent a webjacking than to recover from one, employees who are the contacts must be fully aware of the importance of their roles.

## VII. CONCLUSION

Network Solutions processes over 30,000 registration changes a day.[186] Tucows processes over 2,000 transfers daily. If the remaining registrars process just a total of 8,000 changes each day, the current system of registrars must make over ten million changes a year. Because only a handful of webjackings are reported yearly, registrants toss aside concern of being webjacked. Many think that they are just as likely to be hit by lightening or to win the lottery as they are to have their domain name webjacked.

As with lightening, however, webjacking does not seem to be a big deal—until it happens to you. Then webjacking becomes very serious and very expensive. The owner of the bali.com domain name registration estimated it lost $100,000 a week when its site was webjacked.[187]

Registrants are not the only victims who are damaged by webjacking. As webjacking continues, consumers will be hesitant to place their trust in electronic commerce. While such concern remains, growth of the Internet economy cannot be fully reached.

186. *NSI's Webjacking Epidemic*, Wired News 3:00 a.m. (June 8, 2000).
187. *Hijacking Going High-Tech*, THE LONDON FREE PRESS, (June 9, 2000), at D3.

Therefore, webjacking and similar Internet fraud problems must be addressed. As former President Bill Clinton stated, "We must give consumers the same protection in our virtual mall they now get at the shopping mall."[188]

188. *The Electronic Frontier: The Challenge of Unlawful Conduct Involving The Use of The Internet, A Report of the President's Working Group on Unlawful Conduct on the Internet,* Appendix B (Mar. 2000), *at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.