Why Websites Are Lost (and How They're Sometimes Found)

Frank McCown[1], Catherine C. Marshall[2], and Michael L. Nelson[3]

[1] Harding University
[2] Microsoft Corporation
[3] Old Dominion University

Abstract. We have surveyed 52 individuals who have "lost" their own personal website (through a hard drive crash, bankrupt ISP, etc.) or tried to recover a lost website that once belonged to someone else. Our survey investigates why websites are lost and how successful individuals have been at recovering them using a variety of methods, including the use of search engine caches and web archives. The findings suggest that personal and third party loss of digital data is likely to continue as methods for backing up data are overlooked or performed incorrectly, and individual behavior is unlikely to change because of the perception that losing digital data is very uncommon and the responsibility of others.[4]

1 Introduction

The Web is in constant flux- new pages and websites appear daily, and old pages and sites disappear almost as quickly. One study estimates that about two percent of the Web disappears from its current location every week [2]. Although Web users have become accustomed to seeing the infamous "404 Not Found" page, they are more taken aback when they own, are responsible for, or have come to rely on the missing material.

Web archivists like those at the Internet Archive have responded to the Web's transience by archiving as much of it as possible, hoping to preserve snapshots of the Web for future generations [3]. Search engines have also responded by offering pages that have been cached as a result of the indexing process. These straightforward archiving and caching efforts have been used by the public in unintended ways: individuals and organizations have used them to restore their own lost websites [5].

To automate recovering lost websites, we created a web-repository crawler named Warrick that restores lost resources from the holdings of four web repositories: Internet Archive, Google, Live Search, and Yahoo [9]; we refer to these web repositories collectively as the *Web Infrastructure* (WI). We call this after-loss recovery *Lazy Preservation* (see Section 2 for more information). Warrick can only recover what is accessible to the WI, namely the crawlable Web. There are numerous resources that cannot be found in the WI: password protected content, pages without incoming links or protected by the robots exclusion protocol, and content hidden behind Flash or JavaScript interfaces. Most importantly, WI crawlers do not have access to the server-side components (i.e., scripts, configuration files, databases, etc.) of a website.

Nevertheless, upon Warrick's public release in 2005, we received many inquiries about its usage and collected a handful of anecdotes about the websites individuals and organizations had lost and wanted to recover. Were these websites representative? What types of web resources were people losing? Given the inherent limitations of the WI, were Warrick users recovering enough material to reconstruct the site? Were these losses changing their behavior, or was the availability of cached material reinforcing a "lazy" approach to preservation?

We constructed an online survey to explore these questions and conducted a small set of in-depth interviews with survey respondents to clarify the results. Potential participants were solicited by us or the Internet Archive, or they found a link to the survey from the Warrick website. A total of 52 participants completed the survey regarding 55 lost websites, and seven of the participants allowed us to follow-up with telephone or instant messaging interviews. Participants were divided into two groups:

1. *Personal loss*: Those that had lost (and tried to recover) a website that they had personally created, maintained or owned (34 participants who lost 37 websites).
2. *Third party*: Those that had recovered someone else's lost website (18 participants who recovered 18 websites).

The results of our findings are shared beginning in section 3. The next section provides more in-depth background on Lazy Preservation.

2 Background on Lazy Preservation

As the Web becomes a hub for our daily activities, curation and preservation of Web-based material imposes an increasing burden on individuals and institutions. Conventional Web preservation projects and techniques require a significant investment of time, money, and effort and thus are applicable only to collections of acknowledged value. The limited scope of such projects may leave many potentially important Web collections unprotected.

Lazy Preservation addresses the recovery of these unprotected collections [9, 10]. Lazy Preservation does not require an institutional commitment to a particular archive; rather it is achieved by the ad hoc, distributed efforts of individual users, web administrators and commercial services. This strategy takes advantage of a growing *Web Infrastructure* (WI), which includes the harvested holdings of search engine companies (e.g., Google, Yahoo, Live Search), non-profit organizations (e.g., the Internet Archive's Wayback Machine) and large-scale academic projects (e.g., CiteSeer, NSDL). The WI refreshes and migrates web content in bulk as a side-effect of user services; these holdings can be mined as a useful, but passive preservation service. Although recovery results for a specific object sometimes can be disappointing, the aggregate performance for a complete website is usually very good. Like RAID (Redundant Arrays of Inexpensive Disks) systems, where reliable storage is built on top of individually unreliable disks, the WI provides a dependable resource for content recovery, even if individual elements of the resource are missing. However, unlike RAIDs, the WI elements are not under our control.

Warrick is a web-repository crawler which uses Lazy Preservation principles to recover lost websites [9]. Warrick "crawls the crawlers;" it begins with a seed URL of a lost website and makes requests to four web repositories: Internet Archive, Google, Live Search, and Yahoo. Of these repositories, only the Internet Archive retains the web resources in their original format; the other repositories may store modified versions of non-HTML content such as images, PDF, and Microsoft Office

documents. The most recent version of the resource or the resource stored in its original format is saved to disk, and HTML resources are mined for links to other missing content. Warrick continues to recover resources until its queue is empty; checkpoints are set if daily query quotas are exceeded. A queuing system that runs Warrick jobs on a network of machines hosted at Old Dominion University [6] currently averages approximately 100 jobs a month[5].

Initial experiments with Warrick have confirmed the utility of using multiple web repositories to reconstruct websites [9]. Figure 1 shows how the four web repositories contributed widely varying amounts to reconstructions of 24 websites. For example, Google's cache provided 95% of the resources for recovering website 2 but only 22% for website 1. More extensive experiments reconstructing 300 randomly selected websites over a period of three months have shown that on average 61% of a website's resources (77% textual, 42% images and 32% other) could be recovered if the website were lost and immediately reconstructed [7].

One challenge of Lazy Preservation is that the WI only has access to the surface web; deep web content and website server components (CGI scripts, databases, etc.) cannot be recovered in the event of a loss. We have recently investigated methods for recovering the server components of a website by breaking the components into smaller encoded pieces (using erasure codes [11]), suitable for injecting into crawlable portions of the site [8]. In an experiment, we encoded and stored a website's source code and database in the HTML pages it produced. When the HTML pages housing the server components were discovered and stored by the WI, recovering a small subset of the pages allowed all the of server components to be recovered. Our initial experiments revealed 100% of the website's server components were recoverable from the WI just two weeks after the website came online, and it remained recoverable three months after it was "lost".

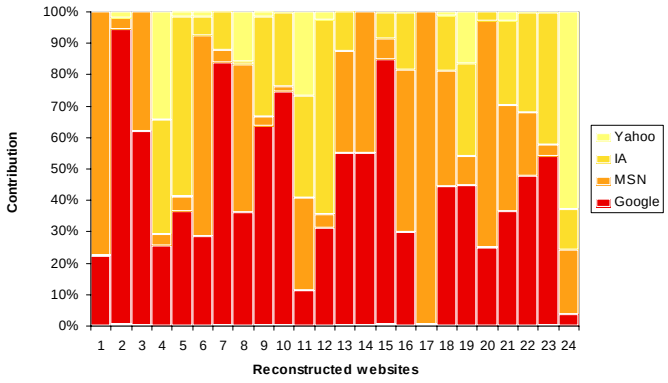

Fig. 1. Web repositories contributing to each website reconstruction.

Table 1. The nature of the 55 websites (categories are not exclusive)

Category	Personal loss $N = 37$	Third party $N = 18$	Examples
Hobby	16 (43%)	5 (28%)	Photographs of cemeteries
Family / personal	12 (32%)	1 (6%)	Political blog and article archive
Education / training	9 (24%)	8 (44%)	Typography and design
Commercial	8 (22%)	2 (11%)	Irrigation technology
Entertainment	7 (19%)	3 (17%)	Christian music e-zine
Professional	7 (19%)	1 (6%)	Painting business
Other	3 (8%)	1 (6%)	Opera commentary

3 What Was Lost (and Found)?

One might imagine that the lost websites occupy a minor niche, that they are small or have a very limited audience, and do not represent significant financial value. The survey results contradicted these expectations. Nor were the websites limited to simple static pages; they were often complex, with socially or programmatically-generated content. Furthermore, the losses were extensive, usually involving entire sites. Recovery was equally complicated, owing not only to 'deep web' or 'Web 2.0' content, but also because there were sometimes gaps between when the website vanished and when the recovery commenced.

The lost websites covered a broad range of subjects (Table 1). Websites about hobbies and interests ran the gamut from Frank Sinatra to Indian movies. Educational sites covered an array of subjects such as humanistic Judaism, women's health, and ancient Roman history. Many of the family/personal websites contained photos, articles or blog postings, and other content of emotional value. One participant described his lost content as "sort of my personal blog, so it is valuable to me for the same reason that old photos are valuable. For sort of nostalgia. Looking back and seeing how you've grown. Reminiscing."

A surprising number of lost sites were of commercial value. Some were used directly to sell products or services, for example an e-commerce site for a major jewelry retailer. Others were geared towards marketing or communication. One website served as the primary information source and social nexus for a city-wide kickball league and another as the primary marketing tool for an irrigation business. Several websites respondents categorized as entertainment or professional were also of commercial value, and loss of the website meant loss of revenue in one form or another for the owner. The owner of a small house-painting business told us that his website "is on my business cards; it's on all my signs. And I've gotten people from Ohio... from Chicago [who] get my web address, look at my jobs, and call me because they're coming out to buy a condo."

A majority of the website owners (67%) paid for hosting services. Four owners had their sites hosted on free services like geocities.com; three had a website on their university's web server; one used an ISP, and one used his own personal server.

The size, makeup, and audience of the lost websites varied considerably. More than half were extensive resources: twenty-nine percent had between 11 and 100 web pages and 38% were larger

[5] `http://warrick.cs.odu.edu/`

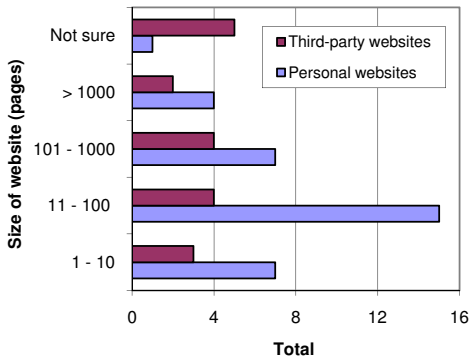

Fig. 2. Distribution of lost website sizes (number of web pages).

than 100 web pages (Figure 2). Furthermore, many of them had user-contributed or dynamic content. Twenty-one percent of the sites had a blog, 6% had a wiki, and 31% had a forum. Although many of the websites were a collection of static files, 43% of them contained content that was generated using CGI, PHP, databases, or other programmatic means. The effect of the loss may have been widespread as well, extending far beyond the original owner: more than half of the participants (56%) believed the websites were used by at least 50 people before the loss.

The losses suffered were substantial. Ninety-two percent of the participants claimed the website of interest was completely lost or almost completely lost. Yet despite the magnitude of loss and apparent value of the websites, the losses were not always discovered immediately. Although 65% of the participants discovered the loss in a week or less, 29% required at least a month to discover the loss. This temporal gap is a significant obstacle to recovery because inaccessible resources may begin to drop out of search engine caches just a few days after they are no longer accessible from the Web [9]; the window of opportunity to recover the lost resources may have passed for more than a quarter of the participants.

The problem was even worse for those involved in third-party recoveries; 65% of those who recovered someone else's website did not learn of the website loss until more than a month had gone by. It was not always clear to these respondents that the loss was not due to a temporary outage: "They thought [the site outage] was because of their web host company... Then the staff changed over and it just became this line of, um, I guess not keeping a track record of what's going on."

Once a loss was discovered and indeed perceived as such, were respondents able to recover the portions of the website that mattered to them? Thirty-three of the 52 participants had finished trying to recover their lost site or someone else's lost site before they took our survey. Of these, almost half were able to recover most or nearly all of the lost site (Figure 3). Unfortunately, 52% of the participants said there was an "important" part of their website which could not be recovered. Half of the respondents indicated the items permanently lost were the server-side components of their sites; others claimed their mp3s, forums, images, and other content were unrecoverable. According to one participant, "[There were] lots of missing holes in the content which is very frustrating. Archive.org didn't catch everything." Another participant noted that there was no way to tell whether he had

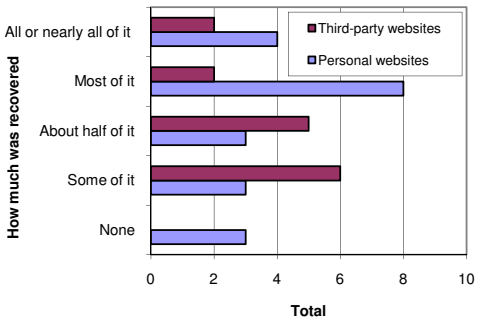

Fig. 3. Distribution of perceived recovery.

recovered all of his blog posts: "There're literally hundreds of posts. And not to mention the fact that I wouldn't even necessarily have a perfect memory of whether a post existed or not."

4 The Blame Game

It's easy to see that multiple parties may be involved in a website's disappearance: the owner is not necessarily the designer, nor does the Information Architect have any control over the ISP's policies. Larger institutional, social, and legal issues may come into play as well.

Accordingly, the participants' reactions to losing their sites were mixed. One third of the participants made it clear the loss was major: "Devastated. Months and months of code was lost." Others complained of important content that was gone, loss of countless hours of work, and interruption of "very important sales." The other two thirds thought the loss was less severe or minimal; one participant said that although the lost site only affected himself, he "felt kind of sad" since it was the very first website he had ever created. A few seemed more ambivalent, sardonically shrugging off the loss: "I'm sure my future biographers [will] lament the loss."

When asked why their websites were lost, 43% of the participants blamed the hosting company. Free hosting companies deleted two of the websites for unknown reasons; six more sites were lost when the hosts experienced disk failure and had a corrupted backup or no backup at all. Several hosting companies were apparently the victims of hackers or viruses, and several others went out of business and removed their customers' content without notice. One ISP was hosting a website dealing in pirated software and movies, and the respondent's site was lost along with the offending site as the result of a Swedish police raid.

Other sites were lost through owner negligence. One website was deleted months after the owner forgot to renew his hosting services (the renewal notification was inadvertently caught by his spam filter). Another owner accidentally deleted her website. A few others experienced hardware failures when hosting the sites on their own servers. In one case, the owner of the site purposefully let the site die out but then changed his mind several years later.

Sites may also be lost through changing circumstances or relationships. When institutional affiliations change, websites may get lost in the shuffle; one site owner forgot to move the site to another

location when he left school and the system administrators deleted his account. Another site was lost when the site's owner and site's maintainer had a falling-out: "I contacted [my friend who had developed the site] and he said that if I gave him a hundred dollars an hour that he could go ahead and pull it up for me and get it back online. And I thought that was kind of a slap in the face." Two websites were recovered by interested third parties when the sites' owners died and left no backups. Two other sites were lost when the companies they represented went bankrupt, one the victim of the dot-com bubble. Finally, sometimes larger social forces are at work: a site documenting the medicinal and recreational cultivation of marijuana was taken down by Canadian police; the recovered site was never re-hosted but instead used by the recoverer as a personal resource.

5 Backups, or Lack Thereof

Our survey revealed that many individuals did not backup their websites and relied instead on the hosting company to protect their files from loss. Fifty-nine percent of the participants *never* created a single backup of their websites, and of the eleven individuals that did, a third of them performed the backup process manually (which is error-prone). Most found their backups somewhat (73%) or very (18%) useful in recovering their website, and in these cases Warrick was able to supplement the recovery by finding additional lost resources.

Participants who paid for hosting services tended to have higher expectations of their hosting provider than those who received free services. One participant lashed out at the hosting company's "incompetent system admins", and another voiced his frustration that the hosting company never replied to any of his emails.

Although most individuals know that they *should* backup their data, they rarely do. It is not uncommon for individuals, even those who work on storage backup techniques, to admit they do not backup their personal files [1]. Although researchers have proposed a number of methods to make backup simple and affordable for the masses (e.g., [1]), such systems are not yet in widespread use. Commercial backup systems are prohibitively expensive for some (Backup.com offers 1 GB of storage for $15 a month), and so backup is therefore generally confined to the organization, not the individual. One of our respondents who did not back up his website, even though it was hosted on his own server, exclaimed, "Whose fault is it? I mean, is it the user's fault for not backing up? Or is it technology's fault for not being more tolerant and failsafe, right? In ten years, maybe hard drives and PCs will be so invincible and the Internet will be so pervasive that the concept of backing up will be quaint, right?"

When they do create backups, individuals tend to backup their important files using a number of ad hoc techniques (e.g., emailing themselves files, retaining old systems with important files, or spreading the content across free services to mitigate risk) which may or may not allow complete recovery in the face of disaster [4, 5]. Because it is so rare for a hard drive to crash or for a web hosting company to go out of business, individuals are not sufficiently motivated to keep their important files backed-up. For those performing third-party reconstructions, the owners' backup practices are inconsequential since third parties do not normally have access to private backups.

6 Doing Things Differently

Given the nature of some of their losses, we might expect respondents to be quick to assert that they are going to change their ways. Indeed, several participants said they were transferring their websites

to hosts that promised reliable backups. Others said they would continue to use free hosting services, but only services from larger companies with the expectation that the larger companies will be more responsible. Several participants said they would perform backups more regularly, use automated backup tools, or keep more backup copies, even when using another web hosting company. One participant who lost the server components of his dynamic website said he was going to backup both the server files and perform a full crawl of the website, just in case the server files would not run in the future. In spite of these good intentions, several respondents had not yet implemented their new failsafe strategies in the four months between the survey and interviews.

Other participants, however, expressed they would not do anything differently to protect their websites. The participant who deleted his website said he would just be "a tad more careful with regard to which directory [he was] in." Another said he was going to do backups "sometimes" as opposed to never. One participant who lost a portion of a large community site when the server crashed said there was not much he could do differently since he used an automated backup before the loss.

7 Conclusions

Given the diversity of our respondents' websites and their motivations for using the WI to restore them, we can surmise that trends that are common among them represent general characteristics of digital loss. Four important findings are:

1. The 'long tail' effect is demonstrated by the websites and respondents' motivations for restoring them. Individuals are restoring deep resources that pertain to relatively narrow domains, be they personal, topical, or commercial; these sometimes-esoteric resources are adjudged to be of sufficient value to warrant the restoration effort.
2. People place themselves at considerable risk for loss, partly through circular reasoning (the fallacy of the safe local copy), partly through lack of familiarity with service provider policies and practices, and partly through normal kinds of benign neglect carried over from caring for physical materials (for example, the photos in the cardboard box under the bed).
3. Website salvage that relies on current WI may become more unreliable as we move toward Web 2.0, where content is dynamic, socially generated, or inaccessible to crawlers.
4. Finally, as we create more and more digital content as a normal part of our everyday activities, it seems that we will have less time to curate what we have already, not more. Furthermore, our expectations of automatic data safety will increase. If we don't backup our files now, we shouldn't expect to do so in the future.

The survey results provide several implications for personal digital preservation, for the WI, and for Lazy Preservation tools like Warrick. As the Web becomes more capable and complex, and as we begin to live a greater portion of our lives online, both the WI and the means to extract content from it, will have to become more inclusive too. Technology to assist people in the onerous task of preserving the digital materials that comprise quotidian (yet undeniably important) human activities must interleave seamlessly with these activities; people who don't find time to backup their websites are not apt to adopt anything that requires extra thought and planning. The payoff for curation (the ability to look at digital photos in fifty years) is too far downstream to make anything other than benign neglect seem worthwhile. Tools like Warrick (after-loss recovery) have greater immediate gratification than up-front preservation applications.

References

1. L. P. Cox, C. D. Murray, and B. D. Noble. Pastiche: Making backup cheap and easy. *SIGOPS Operating Systems Review*, 36(SI):285–298, 2002.
2. D. Fetterly, M. Manasse, M. Najork, and J. Wiener. A large-scale study of the evolution of web pages. In *WWW '03: Proceedings of the 12th International Conference on World Wide Web*, pages 669–678, 2003.
3. B. Kahle. Preserving the Internet. *Scientific American*, 273(3):82–83, Mar. 1997.
4. C. Marshall, S. Bly, and F. Brun-Cottan. The long term fate of our personal digital belongings: Toward a service model for personal archives. In *Proceedings of IS&T Archiving 2006*, pages 25–30, May 2006. arXiv:0704.3653v1.
5. C. Marshall, F. McCown, and M. L. Nelson. Evaluating personal archiving strategies for Internet-based information. In *Proceedings of IS&T Archiving 2007*, pages 151–156, May 2007. arXiv:0704.3647v1.
6. F. McCown, A. Benjelloun, and M. L. Nelson. Brass: A queueing manager for Warrick. In *IWAW '07: Proceedings of the 7th International Web Archiving Workshop*, June 2007.
7. F. McCown, N. Diawara, and M. L. Nelson. Factors affecting website reconstruction from the web infrastructure. In *JCDL '07: Proceedings of the 7th ACM/IEEE-CS Joint Conference on Digital Libraries*, pages 39–48, June 2007.
8. F. McCown and M. L. Nelson. Recovering a website's server components from the web infrastructure. In *JCDL '08: Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries*, June 2008. To appear.
9. F. McCown, J. A. Smith, M. L. Nelson, and J. Bollen. Lazy preservation: Reconstructing websites by crawling the crawlers. In *WIDM '06: Proceedings from the 8th ACM International Workshop on Web Information and Data Management*, pages 67–74, 2006.
10. M. L. Nelson, F. McCown, J. A. Smith, and M. Klein. Using the web infrastructure to preserve web pages. *International Journal on Digital Libraries*, 6(4):327–349, 2007. To appear.
11. M. O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM*, 36(2):335–348, 1989.