Lies, Damned Lies, and the Internet

Anne P. Mintz

When you log onto www.martinlutherking.org you expect the site to be sponsored by an organization with official connections to the family of Dr. Martin Luther King, Jr. You expect factual information that a schoolchild could use in a homework assignment. You expect information about his life and his work. You do not expect to find a page alleging that King plagiarized his doctoral thesis. You do not expect to find a speech entitled The Beast as Saint: The Truth About “Martin Luther King, Jr.” that refers to him as a “modern-day plastic god.” You do not expect the site to suggest purchasing books such as My Awakening by David Duke or Holiday for a Cheater by Michael Hoffman.

This book is about information on the Internet that is intentionally wrong or misleading. It is about deception on the Web, dangerous data in your future, the age of misinformation to come. Intent is the focus of this book. What does the sponsor of a Web site intend for you to see, intend for you to think, or intend to host? Information is no longer inviolate just because one can view it on a computer screen. We can no longer count on its legitimacy because the technology tools for giving created works the imprimatur of appropriateness are in the hands of millions of computer owners. The Internet has made self-publishing possible for anyone with a computer and a modem, requiring no editing or checking for factual accuracy.

This situation is especially alarming when children and other students use the Internet for their education needs. People of all ages, but particularly kids who don’t have training in evaluation and criticism, become targets for organizations or individuals with deception in mind. The absence of an authority on the presented facts can pose dangerous problems to kids and teenagers who may come to believe
things to be true that are not. Intermediaries such as editors, teachers, or librarians usually fill those roles in the world of bricks and mortar, but in cyberspace it seems that just about anything goes.

Worse than that, even the press is being duped. According to the *American Journalism Review* ("The Real Computer" by Carl M. Cannon, May 2001), the mainstream press is beginning to publish stories with unchecked factoids that its staff found on the Internet that it accepted as fact. When journalists rely on unchecked information for source material and republish it in their own pieces, the erroneous information gets spread as fact. Cannon predicts that these problems are only going to get worse unless Internet users (and journalists) become more careful.

In this age of Internet nomads and mass acceptance of online information on the World Wide Web, what if new dangers emerge not from a lack of competence by database publishers or searchers but from a malevolent competence? Dangers like deliberate deception, deliberate misinformation, and half-truths that can be used to divert a seeker from the real information being sought. How many ways can people find to use new technologies to support lies, deception, misdirection, fraud, spin control, propaganda, and all other forms of misinformation? Do any protections exist for online searchers?

Internet nomads often lack the background and training to evaluate or criticize basic information sources. Since many of these nomads are knowledge workers or university students, making wise decisions on sources and searching is clearly not a matter of intelligence. Even experts can find themselves gulled by smarter experts working behind the scenes. Well-trained and suspicious information professionals constitute one level of protection. But how available are they, and for whom? Even legal protections may not hold. In most cases, Web-based data comes free to searchers. No contract, no liability? You get what you pay for? Is there any liability involved and for whom?

The entire subject of the validity of data on the Web is beginning to spawn a new industry. There are advertising-sponsored Web sites that debunk online myths and legends, magazines and newsletters that evaluate Web material—and even this book! The subject of deception on the World Wide Web extends into a variety of disciplines and aspects of daily life. We’ve chosen just some of them. We share tips for avoiding scams, phony charities, hoaxes, and identity theft. We tell you how to evaluate a Web site for authority and how the search engines got you to that site in the first place. We list Web sites of government offices to contact for remedies when you’ve been defrauded on the Internet. Most of all, we hope that this book provides a perspective on where the misleading and deceptive information comes from and how to avoid using it inappropriately.
Better Type That Again!

Web hoaxes, counterfeit sites, and other spurious information on the Internet can give even the most discriminating of searchers a hard time. In November 2000, Nancy Yanofsky, President of ProChoice Resource Center, a national nonprofit organization that provides information about reproductive rights, health, and activism, logged on to her ProChoice Resource Center Web site. She inadvertently typed prochoiceresource.com instead of .org as the top-level domain in the URL. She instantly found herself (and anyone else who made that error) at Abortionismurder.com, a Web site that graphically depicts mutilated fetuses and equates supporters of a woman’s right to choose with the eugenicistic Nazis. Her organization promptly made a federal case out of it—literally—and sought relief, including a permanent injunction forbidding the use of its name, by filing suit in New York. The suit was based in part on the 1999 Anticybersquatting Consumer Protection Act, that among other things prohibits “cybersquatting,” the unauthorized use of another’s domain name with a different top-level domain, exactly what abortionismurder.com did when it used “prochoiceresource.com.” Abortionismurder.com immediately capitulated; it redirected the prochoiceresource.com domain name to the ProChoice Resource Web site, transferred the domain registration and consented to a permanent injunction. Although cybersquatting is against the law, the law works only if invoked, which can be a long and expensive process. That said, we can assume that cybersquatting, along with other forms of unreliable and potentially harmful Internet content, will be with us for a long time.

E-Commerce Fraud on the Internet

The Consumer Sentinel network of agencies gathering data on e-commerce fraud reports that in 2001 there were 204,000 complaints, compared to 138,900 reported in 2000. This 47 percent increase demonstrates the growing nature of the problem. The FBI announced in May 2001 that 62 people had been arrested or have pleaded guilty to charges that they defrauded tens of thousands of consumers out of $117 million using Internet scams as varied as bogus sales offers and fraudulent investments. The Associated Press reported that over 56,000 consumers were victimized by online fraud schemes uncovered via the code-named “Operation Cyber Loss,” conducted by the FBI and law enforcement agencies throughout the U.S. In that case alone, 39 people were indicted.

In February 2002, Scambusters notified subscribers about the Internal Revenue Service (IRS) Audit Scam. It warned that “taxpayers receive a fraudulent e-mail saying that they are under audit. (The
e-mail uses the term ‘IRS e-audit’ in the subject line.) The taxpayer is instructed to fill out a questionnaire, which supposedly must be completed within 48 hours to avoid penalties and interest. The taxpayer is asked for his/her social security number, bank account numbers and other confidential information.

“However, the IRS does NOT notify taxpayers about pending audits via e-mail. Nor do they conduct ‘e-audits.’ And, the IRS certainly does NOT ask for this kind of confidential, personal information. In other words, this e-mail is NOT from the IRS.”

“The old adage that you can’t believe everything you read also holds true for what you read on the Internet” stated Tom Pickard, deputy director of the FBI, on May 23, 2001. That is particularly true of the Nigerian letter and its imitators that have defrauded thousands of consumers, as we tell you in Chapter 6.

Web Sites Playing Doctor

Do you really trust the medical information you find on the Web? How can you evaluate which sites are giving you valid impartial information on a subject and which ones have a hidden agenda to get you to buy a particular pharmaceutical or treatment? We will tell you about a site that recommends (after analyzing the results of an online quiz) that a 5-year-old boy suffering from low libido take Viagra. We will also tell you of a site that recommends, as a preferred life-style, that one choose to be anorexic/bulemic, a dangerous condition that can lead to death.

With estimates that vary from as few as 20,000 pages to as many as 2 million, cyberspace is filled with e-health sites. The results of a study commissioned by the California Health Care Foundation (a healthcare philanthropy) and conducted by RAND indicate that almost 100 million Americans go online to find health-related information and that 70 percent of them said that what they found influenced their treatment decisions. According to the foundation, the study found that answers to important health questions are often incomplete, and although the accuracy of much of the information was fairly high, many of the sites contained contradictory information.

Some of the claims of efficacy for treatments have not been proven, and some may even be dangerous, such as the one that suggests a self-administered intravenous treatment with 35 percent hydrogen peroxide solution. Many of these sites do not present balanced views of the issues, choosing instead to promote their agendas to a sometimes gullible readership. We have just begun to explore the ramifications of this freedom of speech on the Internet as it applies to health and medicine.
Stealing Your Identity

The Internet has made identity theft easier for the thieves. This crime has become so prevalent that early in 2002 the Federal Trade Commission (FTC) unveiled a model identity theft affidavit that will streamline the process by which victims can alert firms where a new account was opened in his/her name rather than require the victim to report each incident separately. The FTC reported that in 2001, 42 percent of the 204,000 complaints entered into a consumer fraud tracking database were related to identity theft. It was also in 2001 that lawmakers in various states began making progress in the drive to protect consumers from identity theft. Arizona has prohibited merchants from printing complete credit card numbers on receipts, a common way thieves have of assuming the identity of card holders and incurring debt. Washington state and Idaho have enacted laws toughening penalties for identity theft, while California did so as early as 1997.

The U.S. Supreme Court ruled unanimously in January 2000 to restrict the ability of state motor vehicle departments to sell or disclose personal, identifying information without an individual’s consent (the Driver’s Privacy Protection Act). Although the law does not ban the sale or disclosure of personal information, it does require the disclosure to be with an individual’s consent. But how many of us bother to check the opt-out box on the renewals that would deny consent? Not 18 million Texans, since the state of Texas will still sell its motor vehicle database with the addresses, driver’s license numbers, and birth dates of every one of the 18 million Texans with a driver’s license (who didn’t opt out) for just $1,600 (Houston Chronicle, March 11, 2001). Since much of this information is out of date or inaccurate due to human error, misinformation can be disseminated about consumers without them ever knowing it.

In the 2000 Senatorial election in Minnesota, Senator Mark Dayton’s campaign bought a list of names and addresses for all 224,000 deer hunters licensed by the state and paid less than $15,000 for it. It seems the campaign focused on many issues that related to the outdoors, and he used that list effectively to target people likely to spend time outdoors. It helped him squeak through a victory in a close election. Apparently only a few hundred people have taken the state up on its offer to remove their names from the licensing list. In Minnesota, personal information from driver’s license and motor vehicle records is now opt-in, meaning these people’s names and addresses don’t get included in the files unless they ask to be included—in writing. Fewer than 1,000 have chosen to remain on that list.

On April 30, 2001, federal Judge Ellen Segal Huvelle upheld the government’s interpretation of a 1999 financial privacy law that
restricts sales of personal financial information. As of July 1, 2001, credit bureaus and other major data firms were no longer allowed to sell personal information without consumer consent—opt-in rather than opt-out will be the rule. That information included names, addresses, phone numbers, and Social Security numbers. This ruling has the potential to change the landscape of marketing information available to telemarketers, spammers, and others. In this suit brought by the Federal Trade Commission, the Federal Reserve, and four other government agencies, they prevailed against TransUnion, Equifax, and Acxiom, the three major credit records agencies, as well as LexisNexis and First Data Solutions. You can be sure this will be appealed by the credit industry organizations. Until then, to paraphrase Scott McNealy of Sun Microsystems, “Privacy on the Internet? There is none. Get over it.”

“Charity Creates a Multitude of Sins”

Oscar Wilde’s statement introduces us to a really sleazy activity on the Web: charity scams. Charities that solicit contributions often have elaborate and impressive Web sites that give detailed information on where they spend your money. However, there are some sites that have been used by phony charities, and these can be as elaborate and impressive as the legitimate ones. We give you advice on where to check their validity and how to report those that aren’t legitimate. What clues can you use to distinguish among them? There are numerous sites from legitimate organizations and agencies to help donors through evaluations. Before you give, look at some of the sites we suggest. Please don’t stop contributing to honest charities via the Web—just check to make sure you aren’t donating your money to scam artists.

Information in the Corporate Universe

How can they mislead you? Let me count the ways. A company can post nonexistent job openings on its Web site in order to fool competitors into thinking it is expanding into a certain area. It can use these phony job openings to solicit resumes from employees of competitor firms to see who may be unhappily employed. Uses of this information can be to find snoops or to interview these “candidates” in order to solicit information about what that employer is working on. That’s just for starters. A company can release earnings information to the public in a press release and a few weeks later file dramatically different numbers to the SEC in an official document. Who’s going to check the figures?
Do you really believe everything posted on a company’s Web site? In early 2002 the Securities and Exchange Commission (SEC) posted a phony investment Web site to show investors how easy it is to get scammed, and got 150,000 hits in one week alone. The SEC chairman, Harvey Pitt, suggested that the agency should use the exact same tactics as the crooks in order to demonstrate the danger to a gullible public. The SEC published a fake press release touting an initial public offering. The fictitious company, McWhortle Enterprises, has an SEC-created Web site with offers of 300 percent investment returns in three months and phony testimonials from unnamed executives. People interested in investing in McWhortle investment were given a phone number to call, but before they spent any money they were informed of the scam. The SEC officials taking the calls then offered advice to the callers on how to research potential investments and avoid real scams.

There are some dramatic examples of stock manipulation and other illegal activities that have used the Web to make a quick buck, which you can read about in Chapter 3.

**Why Do I Get the Results I Get?**

Ask Jeeves, a search engine company, allows “branded response” ads at the top of editorial answers. Now, you can run a search on something to do with autos and an ad for Honda may appear with the results list. Gator, a piece of software working in combination with another program called OfferCompanion, can enable electronic “coupons” to appear on your computer screen as you search the Internet. As described by Tyler Hamilton in the *Toronto Star* (August 20, 2001), if you are reading an article on Forbes.com about sport utility vehicles, an ad for a Ford Explorer may appear on your screen. Forbes.com, which might have General Motors or Daimler-Chrysler as a major sponsor, can’t do anything to prevent it. In fact, the article says, “Gator will often tailor its banner advertisements to completely cover the other Web site’s advertisements.” Spooky? Just the beginning.

Search engine technology has become so sophisticated as to enable site owners to stack the deck in favor of certain results without the customer knowing. They mislead not by the presence of certain information, but rather the lack of it. They don’t tell you which companies paid for placement of their products, or other benefits. Major sponsors of a site may have their products and services rise to the top of the relevant results because the engine has been programmed to do this, not because the results are more relevant. In *EContent* (May 2001), Greg Notess described how Inktomi takes money from sponsors of Web sites for programs that allow that site to rise to the top of a large results set. The Search/Submit option lets
Web site owners pay by the page to have individual Web pages on their sites included in the Inktomi index. This practically guarantees that the site will appear close to the top of the results listing. The Index Connect option gives larger sites control over how Inktomi indexes their sites, what metadata are used, and how frequently the information is updated. They are public about this process, but most customers of a search engine aren’t going to know which sites paid for placement and which did not.

In July 2001, Commercial Alert formally complained to the Federal Trade Commission (FTC) about deceptive advertising with paid placement and other result-ranking methods. It asked in a letter that the FTC investigate seven popular search engines: AltaVista, AOL Time Warner’s Netscape, Microsoft’s MSN search, Direct Hit Technologies, iWon Inc, LookSmart, and Terra Lycos. The letter says “This complaint concerns the practices of paid placement and paid inclusion without clear and conspicuous disclosure that the ads are, in fact, ads.” These practices mislead and misdirect information seekers by the invisible quality of the information that has been programmed into the process.

Don’t Check Your Common Sense at the Door

Connect to a Web site created by Elizabeth Kirk of Johns Hopkins University, “Information and Its Counterfeits: Propaganda, Misinformation, and Disinformation.” While she defines misinformation as always unintentional in nature, and we define it as always with intent to misinform, it is nevertheless definitely useful to take the exercise on evaluating the information she presents. It can be found at http://milton.mse.jhu.edu/research/education/counterfeit.html.

Examples abound for every one of the topics in the book. Each time we spoke with friends about aspects of the subject, they gave us more Web sites that posed problems or presented data in a misleading fashion. This book is not intended to be all-inclusive. There are many more sites than those mentioned here that intend to mislead or misrepresent data in ways to advance a specific (and many times unstated) agenda. What we do set out to accomplish here is to alert readers to these red flags on the Internet. All of this information may not be on the Web as you read this, but it was at one time. The Wayback Machine introduced by Brewster Kahle in October 2001 (www.archive.org) has captured these pages if they are not still viewable at the URL we cite.

The chapters in this book were commissioned specifically for this book; they also appear in briefer article format as the series in Searcher in 2000–2001 entitled “Dangerous Data Ahead.” They have
been well received by the readership of that journal, and the expanded and updated work is what we present here. Welcome to the chase.

Anne P. Mintz
May 2002