Introduction

If It's on the Internet, It Must Be True

Anne P. Mintz

During the Winter Olympic Games in February 2010, actor Michael C. Hall narrated a television commercial:

> President's Day commemorates the day George Washington bought his first car. He was 16. And it was a Hemi V8 Dodge Charger. Then he met Martha and her kids and bought himself a seven-seater Dodge Caravan. And it was only when he moved back to Mount Vernon that he got an all-wheel drive V6 Journey.
>
> At least that's what it said on the internet.[1]

Even my 93-year-old mother laughed. She understands the unreliability of information found online.

The internet is a petri dish for the growth and spread of misinformation. While some incorrect information is either innocent or harmless, such as the clever ad for Dodge, that is not the focus of this book. Rather, I hope to shed light on the misinformation spread via the internet that is intentional, harmful, and manipulative in nature.

The Larger Context

Misinformation on the internet is dangerous and part of a much larger picture. Bending the truth or telling outright lies is not new. It's just the messenger who has changed, and this messenger spreads the word lightning fast and to far-flung places. In just the past decade, we have witnessed government leaders and chief executives of major corporations misinform the public in ways that have had enormous consequences, some involving life and death, and others contributing to financial ruin.

In 2002, the U.S. invaded Iraq based on reports that Saddam Hussein's government was stockpiling weapons of mass destruction, although scientists and inspectors tasked by the United Nations could not confirm their existence. The then-president of the U.S. addressed the American people and declared that he knew for a fact that these weapons existed. The contrary was later confirmed to be true. As of late 2011, U.S. troops are still in Iraq. Thousands of soldiers have lost their lives, and tens of thousands have suffered loss of limbs and psychological damage from serving in this war. The human cost extends to their families. The financial costs helped escalate a deep recession that began in 2008, costing millions of people their livelihoods and, in many cases, the roofs over their heads.

Enron, once a major utility based in Houston, routinely filed misleading federally required documents that investors and regulators failed to notice or investigate. In 2001, a reporter for *Fortune* magazine who thought some of the financial reports didn't add up questioned Enron executives. She wasn't satisfied with their answers. She kept digging, and the result was that Enron's then-chief executive and chief financial officers were convicted on 10 counts of fraud, conspiracy, and banking violations.[2] Their intentional misinformation resulted in thousands of Enron employees losing their jobs and shareholder investments being wiped out. The multinational accounting firm Arthur Andersen went belly-up, the result of its Houston office's failure to discover the fraud; the ripple effect touched thousands who worked at other companies doing business with Enron. Needless to say, the economic impact was deep and widespread.

In October 2010, pharmaceutical giant GlaxoSmithKline settled a federal lawsuit in which it acknowledged that it had knowingly manufactured and distributed ineffective pharmaceuticals to patients.[3] The company had intentionally misinformed patients about the efficacy of the diabetes drug Avandamet, the antidepressant Paxil, and the antibiotic Bactroban, among others, all of which had been manufactured at one plant from 2001 to 2005. An employee whose job had been eliminated blew the whistle on the pharmaceutical giant. It took more than 5 years for the company to accept legal responsibility and to agree to pay damages.

Even credit agencies that rate the viability of major corporations and other investment vehicles have come under fire for failing to check facts independently and failing to avoid conflicts of interest. Standard & Poor's, Fitch Ratings, and Moody's Investors Service were heavily implicated in the financial crisis that began in late 2008. Agencies that assessed risk in mortgage pools ignored what the *New York Times* described as conclusive evidence of dubious loans.[4] Failing to act on credible information at their disposal, the agencies awarded ratings that were woefully inaccurate. According to D. Keith Johnson's testimony given to the U.S. Financial Crisis Inquiry Commission in 2010, the agencies' reports calling mortgage pools "safe investments" intentionally misinformed the public. The ripple effects are still being felt by each U.S. taxpayer.

Connecting the Dots

There is a growing digital divide between people who are close to the facts and people who aren't. Historically, journalists and other information professionals have been the disseminators of the facts. It was their job to connect the dots and offer explanations. Even more critical, it was their job to tell us where the dots were and why they were important. Today, however, because of economic distress, major media organizations have cut back on investigative reporters, expert researchers, and fact-checkers. More than ever, we need help locating and connecting those dots, understanding when to believe authorities and sources, learning when to dig further to expose falsehoods, and determining where and how to locate accurate information. We must learn where to find quality information, how to evaluate the sources we encounter, and how to avoid being manipulated and victimized by online criminals.

In its 2011 annual State of the Net survey, *Consumer Reports* concluded that almost four in every five households use social networks, nearly twice as many as in 2009. It reported that one-third of the 2,089 respondent households had experienced some sort of online abuse such as malware infection, scams, identity theft, or harassment—more than double the percentage from 2010. *Consumer Reports* estimates that malware cost consumers $2.3 billion in the past year and caused them to replace 1.3 million PCs.[5] This is big business—not "much ado about nothing."

People using social media and the internet commonly make mistakes in judgment. Sometimes people unintentionally explore subversive websites, and sometimes people forget the potentially public and permanent nature of their online communications. Two members of the U.S. House of Representatives (Christopher Lee and Anthony Weiner, both of New York state) resigned in 2010 and 2011 after injudiciously sending photos of themselves using craigslist and Twitter. But that's not why we wrote this book. Our concern is that some unsuspecting internet users are not aware that they are engaging in risky behavior and that they are unknowingly encountering scams, downloading viruses, and purchasing stolen goods that help criminals launder money. How complicit are we in furthering the flood of intentional misinformation? And, more importantly, how can we counter it?

In this context, we will explore a number of key areas in which internet users often find intentional misinformation, in order to see the larger picture of how these lies and falsehoods are spread and how online criminal activity operates, so we don't become victims. The book is not intended to document every incident of intentional misinformation in these areas; the specific examples are not the problem but rather the symptom. We want to portray the larger picture of an international, unregulated canvas where these examples are the small dots. We also want to help you connect those dots and better understand the results of your internet searches.

Social Media and Unintended Consequences

In September 2010, police in Nashua, New Hampshire, arrested three men on burglary and related charges.[6] According to police, the property owners whose homes had been burglarized had posted their travel plans on Facebook. Police said they recovered from $100,000 to $200,000 worth of stolen property. By now, most Facebook users are aware of the dangers of posting such information, but there's much more to know.

Driven by younger, technologically savvy students, Myspace and Facebook have grown exponentially into sites where people can and do pretend to be who they aren't. Sexual predators and thieves who prey on the unsuspecting can pose as potential friends, with a goal of abusing or bilking the unwary. Given the broad coverage of the dangers in recent years, it's surprising that some users of social media networks are not more careful when it comes to "friending" or connecting with people online. But trusting others seems to come naturally to many of us.

The *Consumer Reports* survey also found that many social network users naively and routinely post their personal information and that of their children. For example, 26 percent of parents using Facebook had potentially exposed their children to predators by posting their photos and names. According to the survey, in 25 percent of households with Facebook accounts, users were unaware of or didn't use Facebook's privacy controls.

In order to protect themselves, online users must learn to ignore messages from strangers who ask for settings, passwords, or personal information.

With social media, there are few editors, and hardly anyone seems to corroborate the "facts" before posting them. Tweets and retweets aren't fact-checked. Social media are neutral technological tools that don't care if you are spreading lies. For example, during the riots in London in August 2011, James Cridland of Media UK found that Twitter wasn't reliable as a source for his articles and that even mainstream media weren't as reliable as he would have hoped:

> On the map, I asked people to get in contact with a verifiable source. It's surprising how many people think that a photograph or a video is verifiable: one compelling video sent to me last night was captioned "riots in Liverpool", but was actually from Woolwich in London. Surprising, too, how "a friend told me" was deemed reliable enough to pass on to me (it wasn't reliable enough for me to post.)
>
> It's curious how few people know how to check whether the news they're being told is verifiable.[7]

In Chapter 1, Meg Smith takes us through the world of Facebook, Myspace, Twitter, and other social networks, and points out the dangers of interacting online.

Identity Theft

By now you know not to post updates on Facebook about leaving your home unoccupied during your vacation. But it's more complicated than that. You also shouldn't post children's birth dates, your mother's maiden name, and other data requested when filling out all of those networking site quizzes. Not only are burglars looking to steal your china and furniture, they would also like to steal your identity and wipe out your lifetime savings.

According to the Privacy Rights Clearinghouse, a nonprofit consumer group, more than 347 million records containing sensitive information have been compromised in the U.S. since 2005. In March 2010, identity data on 3.3 million people with student loans was stolen, potentially affecting up to 5 percent of all federal student-loan borrowers:

> Names, addresses, Social Security numbers and other personal data on borrowers were stolen from the St. Paul, Minn., headquarters of Educational Credit Management Corp., a nonprofit guarantor of federal student loans, during the weekend of March 20–21, according to the company … ECMC said the stolen information was on a portable media device. "It was simple, old-fashioned theft," said ECMC spokesman Paul Kelash. "It was not a hacker incident."[8]

This is not an isolated episode. Cynthia Hetherington spells it out in Chapter 2, offering tips and advice geared toward protecting your privacy and preventing identity theft.

Race and Religion

So-called hate sites target the fears people have of those who are different from them. Subtle or not, such sites are subversive. For me, the eye-opener came when I first saw www.martinlutherking.org, which gets traffic from teachers in schools, librarians teaching online users, and—unfortunately—many junior high school students in January of each year who are writing essays about Dr. King and who have yet to learn the lessons of this book. Factually correct, the site is also misleading, referring viewers to suggested readings by white supremacists.

Unfortunately, this phenomenon is not limited to the now-familiar www.martinlutherking.org.

Email messages spread virally, carrying rumors that stretch the limits of believability. Among the rumors listed as false on Snopes.com: that one should send an email to a particular address to protest the depiction of Jesus as a homosexual in an upcoming film; that Alabama redefined the value of pi to 3 to keep more in line with Biblical precepts; that a particular atheist has petitioned the Federal Communications Commission (petition number 2493) to stop the Gospel from being read over U.S. airwaves; that Snapple, Marlboro, and Timberland are all owned by the Ku Klux Klan; that American troops serving overseas are wearing uniforms made by a company owned by the Ku Klux Klan; and that designer Tommy Hilfiger announced on a talk show that he didn't want Asians or blacks buying his clothing.

Even computer games are now in on the act. In the free online video game *Border Patrol*, players aim and shoot at undocumented Mexicans crossing the Rio Grande River, with the goal of killing as many as possible. That's an intentionally bland description.

Canadian organization Media Awareness Network explains hatred in this way:

> Most definitions of hate focus on the ways in which hate-mongers see entire groups of people as the "Other." For example, U.S.-based tolerance.org argues that "All hate groups have beliefs or practices that attack or malign *an entire class of people*, typically for their immutable characteristics." … Canadian communications scholar Karim Karim points out that the "Other" is one of a number of human archetypes common to all cultures. When people transfer their fears and hatred to the "Other," the targeted group becomes less than human. Hate-mongers can then "justify" acts of violence and degradation because they have denied the humanity of their victims.[9]

In Chapter 3, Eli Edwards shows us how to identify these hate sites and rumors for what they actually are.

Ecommerce Fraud

How can you be scammed? Let me count the ways. Or at least here are a few ecommerce scams that you may not have thought of before. More than a few use social media tools to accomplish their goals.

According to CyberSource Corp., which processes credit cards for online merchants, the amount lost by North American merchants to fraud in 2010 was just under 1 percent: approximately $2.7 billion, a decline from $3.3 billion in 2009. (U.K. merchants saw an uptick in their fraud rate from 1.6 percent to 1.9 percent).[10] While there has been some progress in thwarting criminals defrauding online merchants, this type of commercial fraud is still commonplace, international in scope, and involved with merchandise of all kinds.

In a federal lawsuit brought to court in 2008, a woman in Olympia, Washington, was sentenced to 2 years in prison for conspiracy to commit bank, wire, and mail fraud.[11] Her crime? Helping criminals in Lagos, Nigeria, carry out a phony check-cashing scam. Other, similar cases have been filed that shed light on the scope of this activity, such as the 2010 criminal case *USA v. Svechinskaya et al*,[12] which focused on the use of "mules": those who are recruited to open bank accounts under false names and transfer stolen funds into accounts in Eastern Europe.

There are a variety of methods that criminals employ to part you from your money. Pay attention to the way you do business and shop on the internet, and take the advice offered by Ben Fractenberg in Chapter 4.

Information Warfare and Cybersecurity

In 2010, a computer worm named Stuxnet was discovered attacking certain types of Siemens industrial control computers used to manage electrical power grids, nuclear plants, and oil pipelines. It appeared in many countries, including India, Indonesia, China, and Iran, though its origins remain elusive. There has been speculation that the worm was designed specifically to attack Iranian computers used to develop nuclear weapons. However, the story gets ramped up a bit with some deeper skulduggery. In September 2010, news spread that the Israeli government was behind the worm and that it was subversively targeting the heavily secretive Iranian nuclear project. All this was based on the fact that one of the many files in the code was named Myrtus. The suggestion was that the name refers to the Persian Jewish queen, Esther—from the Bible's Old Testament—and that only an Israeli would name a file this way.

Others believe the name was intended to mislead the world into thinking the worm was created by Israel. Either way, there are serious implications when one country or religious group is accused of such behavior, and the intrigue continues. In August 2011, the *New York Times* reported that Chinese computers were the targets of nearly 500,000 cyberattacks in 2010.[13] According to the National Computer Network Emergency Response Coordination Center of China, almost half of the threats originated outside China and used Trojan Horse malware. Many originated in the U.S. No longer just spy vs. spy, this is the dangerous realm of information warfare as it evolves in the nonphysical world, described in considerable detail by Deborah Liptak in Chapter 5. She also explains the technologies of online deception and misinformation in Appendix B.

Political Shenanigans

In July 2010, news releases seemingly sent from the offices of U.S. senators Dianne Feinstein, Frank Lautenberg, and Patrick Leahy announced that each had died of liver cancer. The releases carried correct contact information and appeared at first to be sent from the proper URL for each senator's office. Only upon closer investigation was it revealed that they were fakes. Fortunately, the story that was carried on television and in major newspapers was the one about the hoaxes, not that the senators had died. But in the meantime, the misinformation had spread far and wide on the internet.

It gets more serious than rumors lasting less than one news cycle. There is subtlety and innuendo in many of the sites and advertisements on the internet that cleverly misleads readers. Things are taken out of context and then spread as the whole truth. In one of the most positive developments to come from the ubiquity of immediate online communication, it is now possible to counter viral political misinformation almost as soon as the false claims originate. Several media organizations and some televised Sunday morning conversation shows have instituted routine fact-checking of political sites and on-air pundits. Others joined forces with news fact-checker PolitiFact.

com to cover state elections and candidates. (PolitiFact.com has a "truth-o-meter" with one category named Pants on Fire.) The 2012 election cycle coverage features swift fact-checking of candidates' ads and speeches by both their opponents and by media organizations. The *New York Times* publishes a feature called Fact Check that serves the same purpose as PolitiFact.com; for example, it ran a Fact Check the day after the Iowa Caucus debates in August 2011.[14]

In Chapter 6, Laura Gordon-Murnane elaborates on the world of political "gotcha" and what remedies have been created to debunk that intentionally misleading information.

Charity Scams

It seems that with each new natural disaster there are opportunities to get scammed by nonexistent charities with compelling websites. Whether in the aftermath of Hurricane Katrina in 2005 or the earthquake that hit Haiti in 2010, or the earthquake and tsunami that devastated Japan in 2011, dozens if not hundreds of organizations claim to work on behalf of victims in dire need of materials and money to reconstruct their homes and their lives. Often, these requests tear at our heartstrings, but beware of "opportunities" to donate toys to children in need or to help raise money for breast cancer and other medical research. The useful Snopes.com debunks sites such as those claiming that purchasing Excedrin will help raise funds for Toys for Tots, that Merck will donate to cancer research if you purchase a particular bracelet, or that cellular service providers are raising money for the Susan G. Komen Foundation in support of breast cancer research. In Chapter 7, Craig Thompson shows how you can identify such scams and where to go for dependable sources to evaluate online charitable organizations.

Evaluating Websites

Just as we use electricity without thinking about how it is generated and transmitted to our light switches and sockets, we now use the internet without thinking about the mechanics of how data reaches our screens. In the same way that we carefully avoid being electrocuted, we must be careful not to get scammed, or worse. Amber Benham's guide to evaluating websites in Appendix A should go a long way in helping you avoid being misdirected while traveling the information superhighway.

According to a study by the Pew Internet & American Life Project, 77 percent of Americans were using the internet as of December 2010, a huge number no matter what baseline is used.[15] Many homes have high-speed connections. Many public locations offer free wireless access. Mobile devices such as cell phones connect online. Facebook, Myspace, Twitter, and LinkedIn have become popular social media sites. The internet is no longer just for techies; it's gone mainstream.

Much has changed since my earlier book, *Web of Deception*: *Misinformation on the Internet*, was published in 2002, yet much remains the same. Intentional misinformation is still all over the internet. Examples abound for every one of the topics covered in *Web of Deceit*, and it's a moving target. Each time I speak with friends about this subject, I get more examples of sites that pose problems or present data in misleading ways. All of this information may not still be online 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 sites if they are not still viewable at the URLs cited. There are also references to lawsuits and legal proceedings in most chapters. It is possible that appeals and other procedures have overturned or modified these decisions, but they are accurate as we go to press.

A word about the contributed chapters and their authors: First, because the topics do not all fit in neat categories, you can expect some overlap in coverage. In addition, as with any contributed volume, the writing style will vary from one chapter to the next. As the editor, I've attempted to honor each contributor's voice while at the same time trying to present a unified work. Stylistic differences aside, one of my jobs has been to ensure that the research and reporting are of a consistently high caliber. I hope you'll feel that I succeeded.

Unfortunately, *Web of Deceit* will not fix what is broken. It will not identify all of the dangerous or misleading information out there. It will not change everyone's online behavior. But in publishing the book, it is our goal to help you be more alert to charity scams, identity theft, ecommerce fraud, and other criminal activities when using websites and social media tools. It is our goal that you become more aware of subversive activities involving computer worms, political operatives, and charlatans of all stripes and colors. We hope you will learn some valuable lessons and use that knowledge to help others avoid falling victim to misinformation and manipulation in this remarkable digital age we live in.

To all of our readers, we wish you a safe journey.

Endnotes

1. Copyright of BBDO Advertising Agency.
2. Enron Chief Executive Kenneth Lay died of heart failure in July 2006 before he could be sentenced. His conviction was thrown out since his death prevented him from appealing the verdict.
3. *United States of America, ex rel. et al. v. GlaxoSmithKline Holdings (Americas) Inc. et al.*, Case 1:04-cv-10375-JLT filed in United States District Court, Massachusetts District Court in Boston on February 27, 2004.
4. Gretchen Morgenson, "Raters Ignored Proof of Unsafe Loans, Panel Is Told," *New York Times*, September 26, 2010, accessed May 17, 2011, www.nytimes.com/2010/09/27/business/27ratings.html?scp=1&sq=raters%20ignored%20proof&st=cset.
5. "Online Exposure," ConsumerReports.org, June 2011, accessed July 28, 2011, www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/online-exposure/index.htm.
6. "Nashua Police Announce Burglary Ring Arrests," Nashua Police Department, September 8, 2010, accessed May 17, 2011, www.nashuapd.com/PR/11%20st%20Burglary%20investigation.pdf.
7. James Cridland, "What I Learned Mapping the London Riots," paidContent.org, August 9, 2011, accessed September 7, 2011, www.paidcontent.org/article/419-what-i-learned-mapping-the-london-riots.
8. Mary Pilon, "Data Theft Hits 3.3 Million Borrowers," WSJ.com, March 29, 2010, accessed May 17, 2011, online.wsj.com/article/SB10001424052702304434404575150024174102954.html.
9. "What Is Hate?," Media Awareness Network, accessed May 17, 2011, www.media-awareness.ca/english/issues/online_hate/what_is_hate.cfm.
10. "Merchants Hit Back at eCommerce Fraud," CyberSource Corp., accessed May 17, 2011, www.cybersource.com/news_and_events/view.php?page_id=1798.
11. *United States of America v. Edna Fiedler*, Case 3:08-cr-05032-BHS-001 filed in United States District Court, Western District of Washington in Tacoma on January 16, 2008.
12. *United States of America v. Svechinskaya et al.*, Case 1:10-mj-02137-UA-1filed in United States District Court, Southern District of New York in Manhattan on September 28, 2010.

13. Edward Wong, "China: Agency Reports 500,000 Cyberattacks in 2010," *New York Times*, August 9, 2011, accessed September 7, 2011, www.nytimes.com/2011/08/10/world/asia/10briefs-cyberattacks.html?_r=1&ref=todayspaper.

14. Michael Cooper, "Fact Check: The Republican Debate," The Caucus, August 11, 2011, accessed September 7, 2011, www.thecaucus.blogs.nytimes.com/2011/08/11/fact-check-the-republican-debate.

15. For Pew internet, broadband, and cell phone statistics, visit www.pewinternet.org/Static-Pages/Trend-Data/Whos-Online.aspx.

"I just feel fortunate to live in a world with so much disinformation at my fingertips."

©The New Yorker Collection from cartoonbank.com. All Rights Reserved.