WILD WEST 2.0

HOW TO PROTECT AND RESTORE YOUR ONLINE REPUTATION ON THE UNTAMED SOCIAL FRONTIER

MICHAEL FERTIK & DAVID THOMPSON

U.S. $24.95

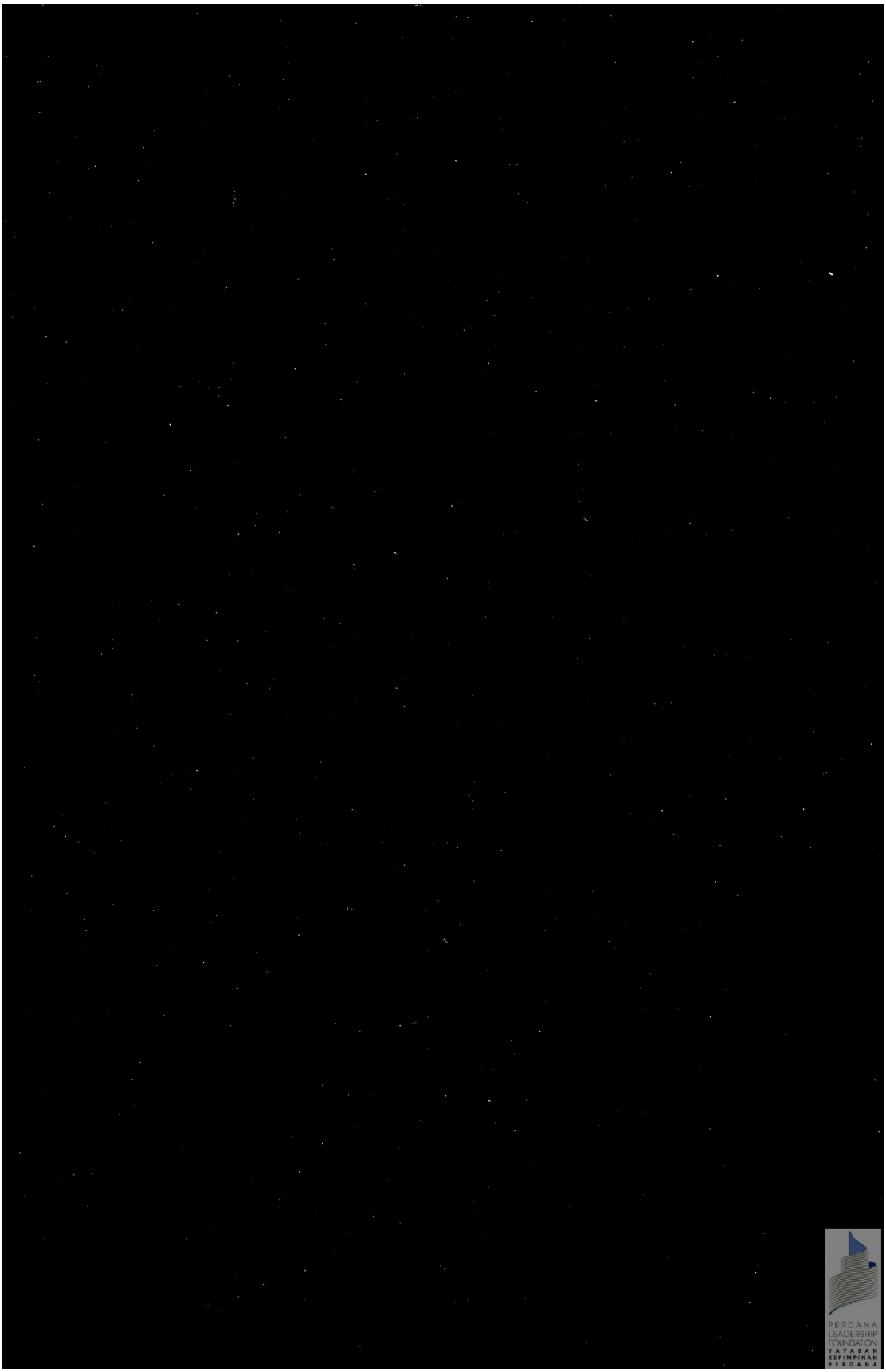
The Internet is a new Wild West: a free-for-all of abundant opportunities and serious dangers where familiar rules don't apply. There is no law enforcement to stop anonymous cowards from defaming your character, few social conventions to prevent it, and no mechanism to get lies and smears removed from the Web. One disgruntled employee, unhinged customer, jealous competitor, or bitter ex can trash your reputation in just a few keystrokes—leaving you to clean up the damage.

These online attacks have real repercussions. Every day, people search for your name on the Internet, and all too often trust the "Google Truth"— the collection of search results selected by a computer for their popularity rather than their veracity—to decide whether to do business with you, or even just associate with you.

The result? Gossip, lies, and embarrassing accusations are anonymously lobbed into cyberspace. Google makes these smears permanent and spreads them around the world. Real reputations and businesses are destroyed. Fortunately, you can protect and restore your hard-won reputation by following the simple steps outlined in *Wild West 2.0.* This groundbreaking book explains why you are vulnerable to attack, and supplies proven strategies for building a storm-proof reputation. The book:

- Draws intriguing parallels between the Internet's culture of expansion, speculation, and lawlessness and the gold rush mentality of the Old West frontier.
- Uncovers hair-raising stories of attacks made under a cloak of anonymity.
- Reveals new threats, including websites that broadcast your phone number, political contributions, family history, and more.
- Provides tips for locating every reference to you or your business in blogs, forums, and social networking sites.

(continues on back flap)


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA

Wild West

How to Protect and Restore

Your Online Reputation on the

Untamed Social Frontier

Michael Fertik and David Thompson

AMACOM
American Management Association
New York • Atlanta • Brussels • Chicago • Mexico City • San Francisco
Shanghai • Tokyo • Toronto • Washington, D.C.

Bulk discounts available. For details visit: www.amacombooks.org/go/specialsales
Or contact special sales: Phone: **800-250-5308**. *E-mail: specialsls@amanet.org*
View all the AMACOM titles at: www.amacombooks.org

Library of Congress Cataloging-in-Publication Data

Fertik, Michael.
Wild west 2.0 : how to protect and restore your online reputation on the untamed social frontier / Michael Fertik and David Thompson,
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-8144-1509-2
ISBN-10: 0-8144-1509-1
1. Personal information management. 2. Online identities. 3. Rumor. 4. Internet in publicity. 5. Public relations. 6. Corporate image. I. Thompson, David, 1979- II. Title.
HD30.2.F495 2010
659.20285'4678—dc22

2009042255

About AMA

American Management Association (www.amanet.org) is a world leader in talent development, advancing the skills of individuals to drive business success. Our mission is to support the goals of individuals and organizations through a complete range of products and services, including classroom and virtual seminars, webcasts, webinars, podcasts, conferences, corporate and government solutions, business books and research. AMA's approach to improving performance combines experiential learning—learning through doing—with opportunities for ongoing professional growth at every step of ones career journey.

Printing number
10 9 8 7 6 5 4 3 2 1

Contents

Wild West


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA


PERDANA
LEADERSHIP
FOUNDATION
YAYASAN
KEPIMPINAN
PERDANA

CHAPTER

Welcome to the New Digital Frontier

Imagine a place where anonymous vandals can spray repugnant graffiti about you or your business without any consequence. They may call you a criminal, accuse your business of fraud, or reveal your most personal secrets. And this graffiti is viewed not only by a handful of passersby—instead, it is spread worldwide and instantly broadcast to anyone who looks for information about you. You can't remove the smear, and copies of it are permanently saved around the world.

Sound frightening? You don't have to imagine this scenario. It happens every day on the Internet. The victims are innocent people—parents, teachers, students, managers, workers, craftsmen, business owners, and more. Real personal reputations are being trashed with just a few mouse clicks, real businesses are losing thousands of customers due to false reports online, and real relationships are being destroyed by anonymous gossip.

The Internet has changed the rules for reputation. Once, reputation was hard-earned and carefully guarded. Today, your reputation can be created or destroyed in just a few clicks. And there are plenty of people who seek to destroy your reputation: bullies, people jealous of your success, competitors for jobs or customers (or even loves), and gangs of disaffected teenagers. The Internet gives them the power to permanently scar your reputation. They harness the power of Google™ and the Web to broadcast false and distorted information about you and your business to your closest friends and most distant customers. They can manipulate your photos, steal your secrets, and ruin your credit. If you are prepared, you can defend yourself from these attacks. But if you aren't careful, you can just make matters worse by fanning the flames.

Don't even think of ignoring the Internet's impact on your reputation. The Internet is not some passing fad; it is here to stay. It is the primary source of information about people, products, services, and companies. Even if you don't use the Internet, your boss, your customers, your neighbors, your friends, and your family do. What they find online will shape how they think about you, for better or worse: they could find slanderous allegations or shocking photos posted by a digital Peeping Tom; your business might be the subject of an online boycott or an urban legend about your business might spread through social discussion sites; or your relationships might be poisoned by false gossip. The worst part is that once false information about you is spread online, it can start a self-sustaining cycle that spreads it further and faster than you thought possible.

Luckily, the well prepared can still prosper on this new digital frontier. The Internet is not something to be afraid of; instead, it is a tremendous opportunity to shape the way that people see you or your business. Careful monitoring of your online reputation (or that of your business) combined with delicate intervention can help you make sure that your online image is a true reflection of reality. Often, by acting quickly you can stop online attacks and set the record straight. And careful seeding of positive truthful content will help

you improve your social standing, get more clients, or grow your business. Thanks to the Internet, *you* have the chance to take direct control of the way people see you.

This book will teach you what you need to know to prosper in the new Wild West of online reputation. It will explain the rules of the new digital frontier, teach you to measure and analyze your reputation, and then give you the tools you need to defend yourself from online reputation attack. It will also explain special considerations and tactics for small businesses and professionals. In short, not all hope is lost: by learning the tricks of online reputation, you can defend—or even improve—your online image.

The Internet Is a New Digital Frontier

The Internet today resembles the Old West of American history. Like the Old West, the Internet is rich with opportunity and hope, but it is also still a rough-and-tumble place with many hidden dangers. There is a chance for individuals to express themselves or strike it rich, but the unprepared also face immense dangers. And, just like in the Old West, law enforcement is weak, and traditional society has not yet adapted to the strange new technology, social norms, and culture of the Internet. In short, the Internet is a new digital frontier that echoes the Wild West of American history. Call it "Wild West 2.0."

Just like in the original Wild West, countless people have struck it rich on the new digital frontier. From the Google founders—now among the richest people on Earth—to microbloggers who supplement their incomes with a few hundred dollars a month in advertising revenues, the Internet has created a modern gold rush. And the frontier is still open: There is still a chance for ordinary people to change their lives forever with new and creative business ventures.

Thanks to the Internet, there are useful new services like powerful search engines capable of finding any document on the planet (Google), the largest and most comprehensive encyclopedia in the

history of mankind ('Wikipedia), and countless other sites that provide news, entertainment, and commerce. With just a few clicks it's possible to find out nearly any information, from the chemical formula for caffeine ($C_8H_{10}N_4O_2$) to the name of the Red Sox third baseman in 1912 (Larry Gardner). Research that would once have required a trip to the local public library can now be conducted online in seconds from anywhere in the world; a student sitting in class in Calcutta can research any topic using the California-based Wikipedia, and a student at home in California can just as easily look up the weather in Calcutta.

The Internet has forever changed politics. Now, it is possible for an anonymous whistleblower to reveal corruption to an audience of millions. Sites that provide outlets for classified documents (such as Wikileaks.org) exist because thousands of people want to reveal the truth about government wrongdoing. Political dissenters in Iran have organized their opposition to their government using e-mail and social sites like Twitter. Closer to home, supporters and opponents of local or national political candidates can anonymously express their deepest and most fervent beliefs. The power to speak anonymously has generated wide-ranging debate on the biggest issues of the day, free from constraints of political correctness and peer pressure.

Even more important, the world has become more closely connected. Electronic mail has replaced postal letters: you can send an e-mail across the globe in seconds for free rather than pay to send a “snailmair letter that might be delivered days or weeks later. Skype and other Internet telephone services have slashed the cost of long-distance phone calls, allowing far-flung families and lovers to connect for pennies (rather than dollars) per minute. The ability to send videos and photos electronically has allowed closer communication between friends, parents, and others. Thousands of Web-based discussion forums allow far-flung people to discuss the issues most important to them and to find like-minded souls spread around the world.

For all the praise heaped upon the Internet for opening up political and social thought, it might be just as useful for the mundane.

The ability to get answers to basic questions has saved countless college students from pink laundry and burnt macaroni; the ability to get phone numbers of local businesses has saved millions in "411" phone charges; and the ability to plot driving routes electronically has prevented countless drivers from getting lost.

The Dangers of Frontier Life Are Real

But, also as in the old Wild West, the frontier has expanded faster than the law and our culture, which have proven unable to keep up. There is no sheriff in town, and Internet users have been left with rough frontier justice. Innocent reputations can be ruined by anonymous attackers, and the victims are often greeted with blank stares by law enforcement. Disputes are settled at the ends of virtual pitchforks and torches instead of at a negotiation table or in a court of law. People suspected of wrongdoing are run out of town on an electronic rail, often before there is time to figure out whether they are really guilty or innocent. And, all too often, the victims are innocent people, who have done nothing wrong other than venturing online without fully understanding the unique culture of the Internet.

The increase in connectivity that allows instantaneous research and positive connections also brings with it the capability to do immense harm. Popular search engines like Google that allow students to research their homework also allow anybody anywhere in the world to search for your name and find nasty commentary written by a bitter ex-lover. Internet forums that empower positive discussions also allow insular communities to gossip and spread lies about outsiders. The power to instantly transmit data also allows malicious software to spread worldwide instantaneously. The power to speak anonymously about corrupt politicians also allows anonymous attacks on private people who have done no wrong.

The Internet has grown too fast for social norms and common sense to keep up. Special software makes it possible for malevolent users to access the Internet anonymously without leaving any digital fingerprints; society has not yet come to grips with truly anonymous

untraceable speech. Social norms have not yet evolved to create a code of conduct for acceptable online behavior—and may never do so. The psychology of the Internet creates a feeling that the targets are somehow distant or unreal and therefore less sympathetic—this problem has been known since the psychologist Stanley Milgram demonstrated the effect of social distance on human behavior, but, has been accentuated and made nearly universally applicable by modern technology.

Law enforcement also lags behind the Internet. In the United States, online law enforcement has generally been focused on major fraud and child pornography. Many victims of ''routine'' online attacks cannot obtain help from the legal system, either because the attackers have disappeared into the digital night or because local courts and lawyers simply don't know how to deal with complex online attacks that might have come from the far side of the world.

Developments in the law itself have also lagged far behind the evolution of Internet technology. Today, the law of the Internet is controlled by two major federal statutes: the Communications Decency Act (CDA) and the Digital Millennium Copyright Act (DMCA). These laws were enacted in 1996 and 1998, respectively, and they have not been updated, even though the Internet today would be unrecognizable to politicians of 1996. A legal loophole in the Communications Decency Act makes it impossible to force a website to remove anonymous attacks, no matter how false and damaging they may be. The result of the CDA and the DMCA is perverse and bewildering: Viacom can send one letter to YouTube and force it to remove 50,000 videos for copyright violations, but if an anonymous attacker were to upload a lie-filled video about your kid sister to the same site, she would have no power to force the site to take the undoubtedly illegal video down.

As a result, false rumors are spreading with lightning speed. Intimate photographs, videos, and personal details are being leaked worldwide. Gossip and innuendo are replacing honesty and truth. And, thanks to the power of the Internet, attackers and gossipmongers enjoy instant global audiences and powerful anonymity. They

work from the shadowy corners of the Web to sabotage reputations, careers, and families. Loopholes in the law protect them from being found or prosecuted.

Of course, anonymous gossip and lies are as old as civilization. But, thanks to the Internet, smears that would once have been limited to a bathroom stall or a hand passed note can now be seen by employers, friends, families, dates, clients, and anyone else with access to the Web. Before the Internet, a smear campaign based on a personal grudge would last only as long as it took for scrawled notes to find their way to the trash can or as long as it took to paint over graffiti. But today, notes posted on the Web are broadcast to a worldwide audience, preserved into the distant future, and spread to thousands by Google.

For too many people, the Web has become a permanent scarlet letter. Who is going to hire a victim of an online smear when there is a similar candidate up for the job who is not accused, however nonchalantly and anonymously, of being a liar, thief, or cheating husband? Too often, the attack is hard to undo, even if the smears are untrue: how does one rebut an allegation of sexual impropriety? Can one forget the emotional damage caused by being crassly reminded of the loss of a loved one? How is it possible for an everyday person to prove that a photograph is a forgery, let alone inform everyone who has seen it?

The harm caused by electronic attacks extends into the "real" world of flesh-and-blood interactions. Nothing separates the "virtual" and the "real" worlds; an online smear impacts face-to-face interactions just as much as a hushed comment or a passed note. A false claim about your business—accusations of bias or of a lack of patriotism, claims that your product is dangerous, or even claims that employees made offensive comments to customers—can send customers running in droves away from your business and even tie up your phone lines or flood your e-mail with howling protests.

These online attacks are happening more and more frequently. Bullies, jerks, jilted lovers, and sociopaths have realized that they can wreak far more havoc with far less accountability by using the Inter-

net to launch their barbs. The attackers seek explosive revenge for petty differences and jealousies, censorship of their critics through humiliation, destruction of political and business opponents, and sometimes schadenfreude or just nerdy self-celebration from the ability to inflict pain on unsuspecting people hundreds of miles away.

The Machine Is Amoral

The problems caused by the Internet are amplified by its structure. The computers that run the Internet—including the big network switches that control the flow of data and the computers that store the content of websites—do not know or care what information is being transmitted. To a computer, it is all just digital bits. A computer doesn't know if information is true or false, kind or hurtful, public or private. There is no way for a computer to realize that real people are being hurt by a website. A computer is amoral—it just does not have any sense of what is "good" or "bad" (The Internet is not immoral—of bad morals—but rather merely amoral, meaning that it has no regard for morals either way.) If a computer is programmed to repeat information that it finds, then it will do so no matter whether the information it finds is true ("the moon is made of rock"), false ("the moon is made of cheese"), or completely nonsensical ("the moon cheeses the rock").

The most obvious example is Google's search results. No matter what terms you search for, the results you see will be selected by a computer without human intervention. The details of the algorithm used by Google to rank search results are a closely guarded secret, but the general outlines have been made public. In short, Googles algorithm ranks "popular" sites higher and less "popular" sites lower. The algorithm does not make any judgment about the correctness of a page; it just finds the most popular pages. Google is notorious for refusing to alter the results provided by the algorithm, no matter how compelling the circumstances. Sometimes this policy leads to painful results. For some time, a search for "Jew" on Google returned a hateful anti-Semitic site as the first result, rather than information

about the Jewish faith or people. Google apologized and blamed the algorithms result on the popularity of the hate site, but refused to intervene directly.[1] Just because the hate site was popular, Google's algorithm assumed it must be important. Other results of the algorithms single-minded focus on popularity are more comical: A search for 'miserable failure' used to return a link to the White House, and a search for "French military victories" still returns a link to a page suggesting that the user should have been searching for "French military defeats".

The danger of the automated Web is not limited to search engines: The "social Web" or "Web 2.0" is a group of increasingly interconnected websites that are based around active user participation. This "Web 2.0" model relies on users to create large amounts of content, which is then displayed to other users. The new "Web 2.0" model stands in sharp contrast to the older generation of websites (call it "Web 1.0" or even the "old Web"), which relied on a top-down content model: a paid author would write content and then hope that users would read it. The basic functions of sites like CNN.com or FoxNews.com are classic examples of "Web 1.0" sites: content (like news stories and photographs) is developed by a professional staff, and average users play an entirely passive role when reading the site.

On the other hand, Facebook.com and its adult cousin, LinkedIn.com, are paradigmatic examples of "Web 2.0" websites in that they are both sites where most of the content comes from active user interactions: the sites both allow people to connect online with friends and co-workers in order to share photos and life updates. There is very little content that is created by employees of Facebook or LinkedIn; instead, the sites simply create an open space where users can determine for themselves how to interact. Discussion sites like Slashdot, Digg, and Reddit are also classic examples of "Web 2.0" sites. These sites allow users to submit news stories for others to view and discuss; there is no editor who picks news stories or puts an official spin on the news—instead, it is up to users to submit news and commentary for other users to view. Hundreds of thousands of people visit

these sites to get an eclectic view of current events and to discuss the social issues of the day, and most of the value comes from other users.

These Web 2.0 sites allow (and encourage) positive user interaction. But they also create grave risks to personal reputation. Back in the days of Web 1.0, the reputation of most private individuals was pretty safe: most highly visible content was created by professional journalists (or at least by serious amateur ones), and a big news website like CNN.com had no reason to spread rumors about individual people (the big sites had other news topics to cover) and a big financial reason not to smear individuals (the threat of a libel lawsuit). But, in the days of Web 2.0, everyone is a publisher, and everyone can distribute content. Your enemies have been armed with new weapons: blogs, easy "WYSIWIYG" website editing ("What You See Is What You Get" editors that allow everyday people to create fancy-looking sites), extensive discussion forums, and a massive social echo chamber to repeat it all. And, most important, all of these enemies have been armed with the power of Google to index everything they say. Disgruntled customers no longer have to rely on professional journalists to carefully research their claims against your company; now, customers can directly blog about their experience or write negative reviews on consumer sites—and then these sites will appear in a Google search for the name of your business. Bitter exlovers or rejected suitors can create online attacks that have the same impact as buying a massive billboard above a freeway, but at a fraction of the price—and with the possibility of doing it anonymously. Kids who would once end their mischief with prank phone calls can now leave a permanent scarlet letter on your reputation by publicizing a rumor or lie just for kicks and giggles. The power of Web 2.0 to create positive connections among its users also creates the danger of misuse to attack and smear reputations.

The open nature of Web 2.0 sites can also create a system of interconnected websites, algorithms, and search systems that no one person or company is responsible for. Call it a "machine" of sorts, with parts spread around the world. Often the system works for

good: information is found, packaged, and presented to users. But, the system can also spin out of control when users feed it false information. With one bad input, the connections between the sites can cause the entire system to amplify and echo false information. The amplification starts when one user copies bad information to a "Web 2.0" site, that website automatically spreads it to others, and then another user repeats the process—the cycle repeats uncontrollably until the false information has been distributed far beyond where it should be. For example, a false story posted on the social news site Digg might be shared by users of the social networking site Facebook, which might be "tweeted" by users of the short-form messaging site Twitter.com, where other users will post it to the news site Reddit, where an automated software "robot" will display it on other popular websites without any human intervention, and so on. The sites start to resemble a game of "telephone"—one person posts a story, which gets transformed a little bit as it is relayed to another site, then a little more, then a little more, until complete fiction has been accepted as reality. Often, the story moves so far away from its original source that readers have no way to find out if it is false or incomplete.

The out-of-control Internet "machine" has caused millions of dollars in real-world losses. One day, a "citizen journalist" participating in CNN's "iReport" experiment posted a prank article claiming that Apple CEO Steve Jobs had been rushed to the hospital after suffering a heart attack. The news automatically spread from CNN's site to others and was quickly visible on hundreds of websites that provide stock news and trading information. Apple stock dropped $10 (nearly 10 percent) on the news, and millions of dollars of value was destroyed. Apple was later able to correct the rumors, but the stock still ended the day lower.[2]

Or take the example of the website Spock.com, which was purchased in 2009 by the public records and background-check company Intelius. Spock.com attempts to aggregate information about everyday people. If you were to search Spock.com for the authors of

this book, you would likely find a little profile about each of us. Much of the content on Spock.com is based on a robot's automated exploration of a variety of directories. The site then uses other software to cross-reference the results that the robot finds in order to compile an automated dossier on as many people as it can identify. There is generally no human intervention and no way for the robot to verify whether any content it finds is true. In one infamous incident, the robot mistook John Aravosis (a prominent blogger) for a pedophile, because of the robot's inability to tell whether Aravosis was *writing about* a pedophile or whether he was one himself. (For the record, John Aravosis is not a pedophile.) Nonetheless, the site tagged his profile as "pedophile," and his name appeared whenever somebody searched for "pedophile" on the site. The problem was instantly compounded when news reporters mentioned the robot's error. The robot, lacking any irony detector whatsoever, interpreted news stories about the error—many of which contained the words "John Aravosis" and "pedophile"—as confirmation that it got it right the first time around. The link was reinforced, and Aravosis was reduced to pleading with Spock.com's customer service team to get his name cleared. In that case, Spock.com was willing to override the robot's actions, probably because Aravosis is a powerful blogger and could create massive bad publicity for the company. Future victims might not be as lucky.

Another example of false amplification occurred when Google News—an automatic newsbot that searches the Internet to find the important news of the day without any human intervention—got out of control. The results that the newsbot calculates to be the most important (usually the most popular stories that appear in the most news sources) are displayed on the Google News homepage. One morning in late 2008, a software glitch occurred, and an outdated article about United Airlines 2002 bankruptcy filing suddenly appeared in the Google News system as if it were new. The sudden appearance of a new-seeming article led a writer at the "Income Securities Advisor" newsletter to mention the possibility of a bank-

ruptcy in his own article. That article was then automatically distributed by the Bloomberg wire to hundreds of websites. Once a (false) story about the new United bankruptcy rumor appeared on hundreds of sites, the Google newsbot mistook the story's popularity as confirmation of its importance and made the story even more prominent on the Google News site. The cycle continued. Stock traders immediately reacted, sending UAL stock into a tailspin that ended with a 76 percent drop in the company's value before trading was automatically halted. By afternoon, United was able to deny the rumor, but UAL stock still closed down 10 percent on the day. Of course, all parties involved claim that somebody else was responsible for the error.[3]

These stories are vivid, but they are neither unique nor rare. Similar events happen all the time to everyday people who have done nothing wrong and done nothing to attract attention to themselves. Sometimes these events go without publicity because they are less egregious, but just as often extreme errors go unnoticed by the media because they happen to everyday people and small businesses, rather than to big companies or powerful bloggers. Unfortunately, the effect of one of these incidents on a private individual or small business can be even larger than on a big company or famous person: most everyday people don't have millions of dollars to spend on PR or their own blog through which to correct the record.

The machine can cause great harm even when it is working as designed. A number of well-known companies are in the business of aggregating and selling enormous amounts of personal information: social security numbers, phone numbers, current and old addresses, spousal information, information about children, medical histories and insurance claims, income data, and other revealing details. They often gather this information from widely dispersed sources, ranging from phonebooks to innocent-seeming consumer surveys to state governments. This information is often used for good purposes, such as rooting out credit card fraud and providing background checks for

teachers and medical professionals. But some data brokers also sell their lists to less scrupulous companies, like telemarketers and small-time scammers. Their data has been used by identity thieves and stalkers to help find details about victims. And, because these database companies possess such rich stores of data, they become targets of opportunity for fraudsters and computer hackers.

There Is Hope

Thank goodness, there is hope for the average Internet user. Despite all the threats and changes, millions of people have positive online images and live in peace with their Internet neighbors. Through a few simple steps, everyday people like you can still guard your reputation on the digital frontier and even improve your online image in order to increase your success in dating, socializing, getting a job, or getting more clients. By understanding how the Internet is different from other communications media, you will begin to understand the rules of reputation online and the online reputation dangers faced by individuals and small businesses. Then, by learning specific tactics to measure and analyze your own online reputation, you will be able to assess your online reputation priorities—and the gaps that need to be filled to meet those priorities. Next, by learning the techniques used by professionals to repair and improve online reputations, you will learn the active steps you can take to improve your reputation today—and why you should act *before* you have suffered a reputation attack at all (especially if you hope to get more customers, meet new people, or just generally present a positive appearance to the world). Finally, by discovering steps to take in case of an online reputation attack, you will learn how to protect yourself in a worst-case attack and how to start down the road to reputation recovery.

Hold tight; traversing the new digital frontier can still be a rough ride, but the rewards are powerful.

A Note About Notes

For your convenience, the authors have provided many links to additional information or to the full text of sources. In order to save space and avoid the need for you to retype some dreadfully long URLs, all links to additional information are provided through the official website of the book: WildWest2.com. Links of this kind appear in the format "*Go:* http://wildwest2.com/go/101." When you come across one of these links, it is a signal that there is more information available online. Simply type the URL in your web browser and you will be automatically forwarded to the original source of additional information. The authors might not agree with anything (or everything) that a source says, but the links are provided so that you can gather information for yourself. Of course, the authors do not control any linked websites, which may have different privacy policies—please browse cautiously.

Notes

1. Google, Inc., "An Explanation of Our Search Results." Go: http://wildwest2.com/go/101.
2. Eric Schonfeld, "Citizen 'Journalist Hits Apple Stock with False (Steve Jobs) Heart Attack Rumor," *TechCruch,* October 3, 2008. Go: http://wildwest2.com/go/102.
3. Jackson West, "Google News Glitch Helps Cause United Stock Selloff," *Valley Wag,* September 8, 2008. Go: http://wildwest2.com/go/103.

BUSINESS / INTERNET

"An excellent guide to safeguarding reputation from the perils of the open, wild, and often rough-and-tumble Internet. Fertik and Thompson offer sage advice for how people can protect themselves against gossip, falsehoods, bullying, and other online threats."

— Daniel J. Solove, author of
The Future of Reputation: Gossip, Rumor, and Privacy on the Internet

"The Internet does not forget. In an age of comprehensive digital memory, *Wild West 2.0* offers not only first-rate analysis, but real-world practical tips on how to defend your reputation and survive the digital memory storm." **— Viktor Mayer-Schonberger, author of**
Delete: The Virtue of Forgetting

"*Wild West 2.0* should be mandatory reading for businesses—especially in these wild days of social media playing the role of Billy the Kid. Conducting business online without this book is like facing a gang of desperados with nothing but a cap gun. I recommend it highly to guerrilla marketers everywhere." **— Jay Conrad Levinson, the father of guerrilla marketing and author of the Guerrilla Marketing series of books**

"The Internet is a fast, convenient source of false information. Read *Wild West 2.0* to find out how to protect yourself." — Gregg Easterbrook, author of ***Sonic Boom***

"*Wild West 2.0* is a wake-up call to parents everywhere. The Internet is our children's new playground, fraught with online bullies and attackers. Fertik and Thompson remind us that we need to supervise them on this new frontier, and provide tips on how to take action if our loved ones are harmed online. A must-read for anyone with a computer, an Internet connection, or a family to protect." **— Dr. Michele Borba, Ed.D., author of**
The Big Book of Parenting Solutions:
101 Answers to Your Everyday Challenges and Wildest Worries

"Your business reputation and personal privacy are at risk in ways you never thought possible. *Wild West 2.0* compellingly explains the risks and blind spots created by the 'social Internet,' and teaches individuals and businesses how to succeed in the new cyberworld." — Drew Bartkiewicz, author of ***Unseen Liability;***
and vice president of Cyber, Technology, and New Media Risks at The Hartford

"Do you know what Google Truth or the Streisand Effect are? You will and you should. Read this book and prepare yourself for the trench warfare that is *Wild West 2.0*"

—Timothy Ferriss, #1 ***New York Times*** bestselling author of T***he 4-Hour Workweek***

"Michael Fertik and David Thompson have produced an invaluable guide for anyone who is concerned about their reputation in the brave new world of the Internet."

— Jimmy Wales, founder of Wikipedia

AMACOM
American Management Association
1601 Broadway
New York, NY 10019
Visit AMACOM online at: www.amacombooks.org

AMA

ISBN-13: 978-0-8144-1509-2
ISBN-10: 0-8144-1509-1

EAN 9 780814 415092 52495