Privacy for Business:™
Web Sites and Email

Privacy for Business™: Web Sites and Email

ISBN 0-9724819-0-7

Published in the U.S.A. by:
Dreva Hill, LLC
P.O. Box 3792
Saint Augustine, FL 32085
www.drevahill.com

Printed in the U.S.A. by:
Signature Book Printing
Gaithersburg, Maryland
www.sbpbooks.com

Cover Design by Dreva Hill Graphics.

For press review copies, sales inquiries, volume purchases, and corporate editions of this book, please contact drevahill@yahoo.com.

Library of Congress Catalogue data is available.

Privacy for Business Web Sites and Email

Stephen Cobb

Dreva Hill

For Brothers

C.A.C

1923-1973

D.T.C.

1921-1999

Contents-at-a-glance

Table of Contents

ACKNOWLEDGMENTS

I don't know about other writers, but this is one part of the book I really enjoy writing, and not just because it means the book is finished. This is where I get to thank those whose words of encouragement and wisdom helped make the book a reality.

In many ways, a book like this is a rich brew of other people's ideas and observations, distilled by the author, with a few of his own ingredients stirred in for good measure. My esteemed colleagues at ePrivacy Group will certainly recognize in these pages points they have made and insights they have graciously shared. Many are attributed in the text, but some are already so ingrained in our "group think" that I am unaware of their precise origins. Needless to say, I owe a huge debt of personal and professional gratitude to the following gentlemen, whom I am proud to count as friends as well as co-workers: Vincent Schiavone, David Brussin, Michael Miora, James Koenig, Terry Pittman, Ray Everett-Church. I feel particularly privileged to count one special person as friend, co-worker, and brother. Thanks Mike.

I don't know if there is a good woman behind every good man, but I do know there are several good women behind this book and its author. For inspiration and support, no man could ask for more than I have in Chey, whose own example as an author rekindled my determination to put on paper what I had talked about for so long. For inspiration and editing, no son could ask for a better mother than mine. Dorothy's love of the language and her knowledge of Fowler made my original words considerably more effective and much less of a chore for you to read. For the inspiration of good news I must acknowledge Erin, who supplied me with so much of it during the writing of this book. Thanks daughter.

Finally, let me make it clear that the opinions expressed in this book are mine alone, and do not necessarily reflect the views of my employer or my publisher. Furthermore, any errors or inaccuracies you find within these pages are also mine alone, and I apologize for them in advance. If you point them out to me, at scobb@cobb.com, I would be most grateful. In the next edition I could be acknowledging you as well.

INTRODUCTION

The goal of this book is to help businesses and their employees learn what they need to know about privacy as it relates to company Web sites and email. Most businesses today operate at least one Web site; some large companies may have dozens of sites. Most Web sites come into contact with information that is considered personal by the people to whom it relates. Most of today's business also make use of email, to communicate with customers, both current and prospective. Most people who have email addresses consider them to be in some way private, and therefore to be treated with respect.

Many people today are very sensitive about how their personal information is handled. This sensitivity is reflected in recent laws and lawsuits, as well a media coverage and opinion polls, all of which imply that violating personal privacy has negative consequences. For businesses, these negative consequences can include lost revenue, reduced customer and investor confidence, burdensome government oversight and intervention, hefty fines, and possibly jail time.

Much of the current concern about privacy can be attributed to the increased ability of companies, governments, and even individuals, to collect, collate, and disseminate information digitally, as data. Some of that data is *personally identifiable information*, or PII. In other words, it is data that relates to a person who can be identified from the data, the *data subject*.

The Internet and the World Wide Web have been on the cutting edge of an enormous increase in the collection, processing, and distribution of PII by businesses. Unfortunately, technology is not perfect, and neither are its users. When a business handles PII, not only is the privacy of data subjects at risk, but so is the business itself. The goal of this book is to help your company minimize that risk, especially in the context of operating a Web site and sending email, thereby avoiding the unpleasant consequences that can arise from the inappropriate handling of personally identifiable data.

Is This Book for You?

This book is for anyone who works with, or is planning to work with, Web sites and personal information. It is also written for anyone who manages people who work with Web sites and personal information. That includes:

- Web site managers, Webmasters, Web content managers
- Employees who design and code Web sites
- Sales and marketing managers and their staff
- Any employee who handles personally identifiable data
- Corporate counsel and corporate compliance officers
- CEOs, CIOs, CTOs, CSOs, and CPOs

A wide range of people to be sure, but privacy encompasses many aspects of a business, as does email and Web site technology. In fact, Web sites and email are often the focal point for privacy concerns within a company, a logical place to start for the business that wants to get on top of this rapidly emerging issue. And while I cannot guarantee that all persons in all of the above categories will like what they read here, this book is written so that, regardless of which category you are in, what I say should make sense to you.

What This Book Is Not

I want you to be happy with your decision to purchase this book, but you won't be if it fails to meet your expectations. Allow me to further refine those expectations by telling you three things that this book does not do:

1. Provide consumer privacy education. This is not the book you buy to help you protect your privacy while surfing the Web. That book has been written already and a colleague of mine, Ray Everett-Church is the coauthor. The book is *Internet Privacy for Dummies*. Don't be insulted or misled by the title—I have a lot of respect for "Dummies" books, particularly since my wife wrote *Network Security for Dummies*.

2. Detail the reasons why citizens are, or should be, concerned about privacy. Although I describe, in broad terms, the background to consumer privacy concerns, the best book dedicated to that task is undoubtedly Simson Garfinkel's *Database Nation*. Although I don't always agree with Simson, we've has some very interesting conversations over the years and I have a great deal of respect for his scholarship and sincerity. In my opinion, *Database Nation*, is required reading if you are planning to do some serious thinking about privacy for business today.

3. Detail the configuration of Web servers and browsers for maximum security. This task has been undertaken by a number of books. Simson's *Web Security and Commerce* is a good place to start. Information about specific Web software is available in more specialized titles, such as *IIS Security*, written by one of my former coauthors, Marty Jost, together with my brother, Mike Cobb.

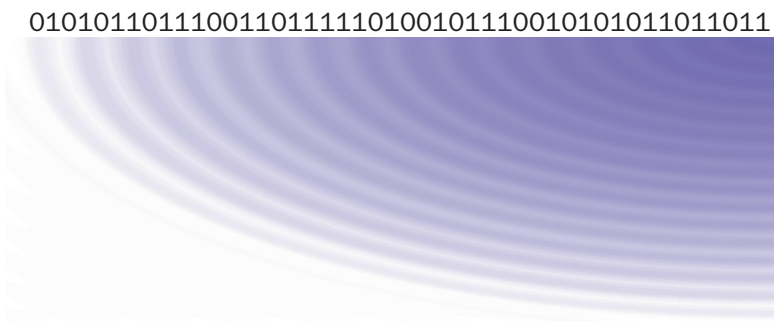
Thank You

At this point, with your expectations suitably adjusted, it only remains for me to thank you for choosing this book to help you answer your questions about privacy for business. Let us proceed—it's time to get down to the business of privacy.

Stephen Cobb

CHAPTER ONE

PRIVACY AND BUSINESS TODAY



2

"Over 80 percent of people surveyed by Harris said that they would completely stop doing business with a company that had misused customer information."

—*The Guardian,* May 2, 2002

1: Privacy and Business Today

Privacy is currently a subject of great concern to many consumers. You probably know this already—you are reading this book—but the point is worth emphasizing. No business today can claim ignorance of the importance of privacy as a concern among consumers, a concern that can have significant business impacts, from increased costs to revenues lost, from brand dilution to stock price depression. Every company that wants to interact with customers via the Internet should know that privacy concerns are the primary impediment to such interaction. In June of 2002, Jupiter Media Metrix calculated that as much as $24.5 billion worth of online sales will be lost by 2006 because Web sites are not addressing consumer fears about privacy and security. The effectiveness of email for consumer communication is threatened by the staggering volume of unwanted commercial email, or spam, which is regarded by many consumers as an invasion of privacy. More than three-quarters of online consumers surveyed in 2002 said that they delete unsolicited commercial emails without reading them. In this chapter I put today's privacy concerns in perspective and relate them to business Web sites and email practices.

Privacy Today

If you were to ask me what is the single most important thing that businesses need to "get" about privacy right now, I would say: the way customers feel. Most of the privacy challenges that businesses face today are driven by consumer sentiment about privacy and the high level of attention afforded that sentiment by the press, the lawyers, the lawmakers, and the regulators. Any company that is accused of violating consumer privacy, however inadvertently, will soon find this out. As I will explain in detail in Chapter 7, the right response to such accusations can be as critical as the steps you take

to prevent them. But I can assure you right now that "We had no idea people would be so upset" is not an option.

When I conduct privacy seminars for businesses, one of the first slides I present is a collage of magazine covers collected over the last few years. They include both business and consumer publications and all of them feature privacy as the cover story. Here are some of the headlines:

- *PC Magazine*: Privacy War
- *CIO Magazine*: Are Your Medical Secrets Safe?
- *U.S. News & World Report*: The Dark Side of the Internet
- *TIME*: How To Protect Your Privacy Online
- *Red Herring*: Privacy—Why It Will Shape Ecommerce In 2001
- *Business 2.0*: Who Can You Trust?
- *Smart Business*: You're Being Watched!
- *Darwin*: Privacy Showdown
- *Popular Science*: All Eyes Are on You
- *Information Week*: Paranoia—Customers Worry About Misuse of Their Data. Maybe You Should Too

These articles reflect genuine concerns. When the Wall Street Journal and NBC conducted a telephone poll of more than 2,000 adults at the end of 1999 and asked them what they feared most in the coming century, "loss of personal privacy" topped the list; cited as the number one concern by 29 percent of respondents, well ahead of overpopulation, acts of terrorism, and racism. This concern is particularly acute with respect to the Internet; for example, a survey in June of 2002 by Jupiter Media Metrix found that almost 70 percent of U.S. consumers worry that their privacy is at risk online. This is not just a vague sentiment. A Harris survey in February of 2002 revealed the top three privacy concerns of consumers to be that:

(a) their information would be provided to other firms without their permission,

(b) their transactions may not be secure, and

(c) hackers could steal their personal information.

These findings are not just important for Web-based companies. If yours is a "clicks-and-mortar" company, one that combines Web operations with traditional business premises, you should note that, in the same Harris survey, over 80 percent of the respondents said that they would "completely stop doing business with a company that had misused customer information." In other words, as Jupiter analysts have pointed out:

> "With poor online privacy practices, many companies will experience negative effects not only on their online sales over the next several years, but also on off-line sales that shift to more privacy-sensitive competitors."

Privacy and Terrorism: While the tragic events of September 11, 2001, have undoubtedly increased anxiety over terrorism, there is no indication that people are any less concerned about privacy. Indeed, many of the government's responses to 9/11 involve increases in surveillance; and while some of these responses have a sound strategic basis, others have heightened fears about the loss of personal privacy. The overall effect of 9/11 on privacy has been to push it even further up the public agenda. That may be a good thing, because what many consumers and businesses currently point to as privacy problems are in fact privacy paradoxes, issues about which we have not yet, as a society, thought enough to frame the debate, let alone take sides.

Privacy Questions

So why is privacy such a hot issue today? Is it just media hype? Surely the notion of privacy has been around for a long time? These are legitimate questions. The easiest to answer is the one about media hype, because the surveys quoted earlier are only a few of many that indicate pretty much the same thing: People fear their privacy is at risk. While studies have shown that this fear does not always prevent consumers from sharing personal information with companies, studies also show that privacy concerns are getting more, not less pervasive. At the same, evidence of a positive response to respect for privacy is getting stronger.

To understand the causes of current concerns about privacy, think of them as the shock waves and fallout from an unprecedented information technology explosion. There are clear parallels to this phenomenon in the history of other technologies. Consider the internal combustion engine or nuclear energy. An early phase of great enthusiasm was accompanied by rapid and widespread adoption—during which any doubts and reservations were swept aside by acclaim for the technology's benefits—eventually leading to the drawbacks and downsides becoming so obvious as to be undeniable.

During the last twenty years we witnessed an unprecedented increase in the ability of companies, governments, and individuals, to collect, collate, and disseminate information. This clearly resulted in enormous consumer and social benefits. Information technology enabled, largely through productivity gains, many years of strong economic growth accompanied by low inflation and full employment. But what about the side effects? For example, if you tell me your name there is a good chance I can figure out, within minutes, where you live, what your house looks like and how much it is worth. I will know how to get there, what shops and restaurants are nearby, plus where you work and what your email address is. The really scary part is that I can do that, in most cases, with just a Web browser and an Internet connection, no special service or database access fee required.

What can be done with more resources? I can take a name and address list to a specialist and get it analyzed, enhanced, and appended. The analysis does things like determine gender and ethnicity, while the enhancement can add age, number of persons in household, head of household's name and age, estimated household income, single or multifamily dwelling, length of residence, owner or renter status, bank card in household, marital status, number of adults, presence of children. A process known as appending can add things to your data like time zone, latitude and longitude of the five digit ZIP code, county name, and congressional district. All of this is automated and thousands of records can be processed in minutes. A different service can figure out a person's email address at work, in case I have a list of names without email addresses.

Some people have portrayed this sort of technology as inherently sinister, but that misses the point raised earlier: the tension

between what is personal and what is public has been around for a long time. With the possible exception of a few hermits and outlaws, people have always lived their lives as known entities; where they lived and worked and shopped, and what they bought when they shopped, were all facts known to at least a few other people.

Privacy Perspective: About ten years ago my family and I lived for several years in a village in Scotland which, in many ways, exemplified the much sought-after ideal of a caring and supportive community. We soon learned that the sharing of personal information was not only essential to the functioning of such a community, it was also both desirable and unavoidable. For example, one's state of health was widely known—the doctor made house calls and everyone could see at whose house he was calling. If things were serious there might be very specific prayers for you in church on Sunday, followed by offers of care and assistance.

What is different today is the way in which information technology has transformed information. Consider "access to public records." Information technology fundamentally alters the meaning of this term because of what IT does to the speed and distance factors that govern accessibility. One of my favorite movies is *Chinatown*, in which Jack Nicholson plays a private detective who uses public records to figure out a huge property scam. If you know the movie you know it also takes him several days, two fistfights, and at least one illegal act. Obviously, the word "access" means one thing when you have to go down to the local hall of records, find the right piece of paper and literally rip it off; quite another if it only takes few keystrokes in the comfort of your home.

The transformation of information by technology is further amplified when you multiply the number of sources that can be tapped simultaneously in this way. While one piece of personal information alone may not be of much value, adding a second piece often more than doubles its value. For example, you may be able to use one piece to leverage another. Consider your mother's maiden name. If someone knows that, they may be able to get at a lot of other information (many institutions use this name as a form of password—even though it is a lot easier to find someone's mother's maiden name now there are so many genealogy sites on the Web). If you have worked in computer security you will be familiar with the phenomenon that is sometimes referred to as "incremental informa-

tion leveraging." An attacker will sift through company garbage for inside information such as internal phone directories. Armed with one of these, an attacker can then "social engineer" a network password from an employee by pretending to be someone from technical support. As more and more information makes its way onto the Web or is transmitted via email, this type of attack becomes much easier to execute, with less risk of detection.

A very similar mix of analogue and digital techniques is employed by identity thieves, who can parlay a few details about a person into a lot of money, typically in the form of unpaid credit card bills in the name of the person whose identity they have stolen (see Figure 1-1). Identity theft has been called the fastest growing crime in America and it is clearly one of the main reasons that today's consumers are so concerned about how their personal information is handled.

Five years ago I heard a chilling presentation about identity theft at the annual DefCon hacker convention in Las Vegas, delivered by a John Q. Newman, author of *Identity Theft*. His talk related an interview with a man from England who makes his living stealing American identities. Every year this man flies over to the United States armed with personal information about his intended victims that he has harvested from Web sites. By combining this information with data from consumer credit reports, plus a basic knowledge of financial systems and a natural aptitude for social engineering, this man is able to illegally obtain goods, services, bank accounts, and credit cards that he then converts into cash to the tune of $40,000 or more before going back to England. Each summer he leaves behind a handful of victims who may take years to recover from this assault. There will be more about identity theft in Chapter 2.

What is Web Privacy?

High levels of concern over privacy have, as you might expect, fueled debate about the definition of the word itself. The finer details of the debate are beyond the scope of this book but there is a good working definition for people who have to deal with privacy in a Web context, provided by the Electronic Privacy Information Center:

> "the right of individuals to control the collection, use, and dissemination of personal information that is held by others." (EPIC: www.epic.org)

Web privacy is thus the right of individuals to control the collection, use, and dissemination of personal information that is held by Web sites. In broader terms, Web privacy also means making sure that your Web site's handling of personally identifiable information complies with a wide range of applicable laws, industry standards, and business best practices. In short, if it is personally identifiable information, your Web site and your company need to "Handle With Care." Failure to do so could result in problems ranging from angry customers and lost business to fines and imprisonment (you can read a lot more about the negative consequences of privacy problems in Chapter 2).

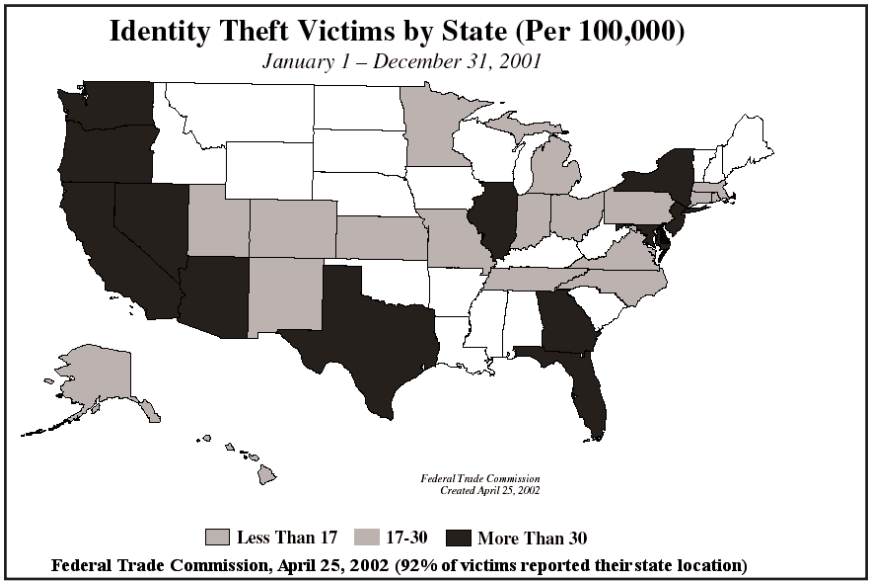


Figure 1-1: Identity theft is spreading fast

Data Ownership

When you are responsible for a business Web site it is natural to think in terms of *you* versus *them*—where *them* is anyone who tries

to compromise the confidentiality, integrity, or availability of *your* data. In fact, it is unlikely that all the data handled by your Web site actually belongs to you. The people who visit your site will generate or supply data, some of which can be said to belong to them and not you. This might be data that you actively request—for example, information needed to complete an online order form—but it could also be passive data, such as logs showing who visited the site and what pages they viewed.

Some of the people to whom this data relates may consider it private information—that is, they may think that they have a right to determine how it is used and by whom. Plus you may have a legal obligation to allow people to review and make changes to data pertaining to them that your Web site collects, stores, or processes. The Children's Online Privacy Protection Act contains such a provision, and a case settled in August of 2002 requires one of the Internet's largest ad companies, DoubleClick, to disclose to Web users the information it compiles on them in order to customize the selection of ads at some of the Web's largest commercial sites.

Non-public Web sites: Some Web sites may be exempt from privacy requirements because they are not freely accessible to the general public. Access to such sites typically is limited to a group of people, such as employees, who use the Web site for access to company information. A non-public Web site controls all access of any kind, effectively acting like an internal or intranet web site. Such sites may not be subject to some of the legal disclosure requirements that apply to public Web sites. When this distinction arises in later chapters, the terms **public Web site** and **non-public Web site** will be used in this way to make the distinction clear .

Common sense says you should use reasonable security measures to protect the confidentiality of any information relating to individuals that your Web site handles, but some privacy legislation has made such security mandatory. For example, if your company is involved in financial services you probably know that the Gramm-Leach-Bliley Act holds the board of directors responsible for information security (specifically, for "approving and overseeing the development, implementation, and maintenance of the institution's efforts to ensure the security and confidentiality of customer information and protect against any anticipated threats or hazards to the security or integrity of such information"). The board is also

responsible for protection against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Privacy Acronyms

Like any other subject, privacy has its own acronyms. As I mentioned in the Introduction, the acronym PII is commonly used for "Personally Identifiable Information." You may find the term defined differently in different places, but the following definition is not only typical, it is particularly relevant since it comes from a government ruling in a privacy case involving a business Web site: "PII is individually identifiable information from or about an individual consumer including, but not limited to:

(a) a first and last name;

(b) a home or other physical address, including street name and name of city or town;

(c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address;

(d) a telephone number;

(e) a social security number;

(f) an Internet Protocol (IP) address or host name that identifies an individual consumer;

(g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or

(h) any information that is combined with (a) through (g) above."

If this strikes you as a pretty broad definition, you probably need to expand your privacy horizon, because some privacy advocates will tell you this does not go far enough. In its Data Protection Directive, discussed in Chapter 5, the European Union highlights several other aspects of PII, including any identification number assigned to a person, or one or more factors specific to "physical, physiological, mental, economic, cultural or social identity."

To put this in perspective you need to realize that "personally identifiable information" is a relative concept. The context in which information appears can be critical. Consider this piece of information: jprz268@msn.com. This doesn't look very personal. You could say it reveals nothing, but connect it to other pieces of information and it can be both personal and revealing. What if it appears in a list of email addresses belonging to people who have expressed an interest in Viagra? If you happen to know who uses the email address jprz268@msn.com, that is immediately revealing. If jprz268@msn.com appears as the sender of an email message that contains illegal information, then law enforcement may well be able to find out who is using it, making it a very personally identifiable piece of information.

Another way to focus on the meaning of PII is to look at a group of people, such as "all people in the county." For most counties in most countries, this is not a piece of personally identifiable information. The statement that "ten percent of the residents of Cobb County use marijuana" is not revealing any PII. A list of how many people in each age group in Cobb County take antidepressants is probably not PII either. But what if there was only one person in one of the age groups? In that case a group definition would constitute PII. Improbable perhaps, but think about "all men in the county over ninety." In some counties this might be one person, who is thus identified without the use of his name. Adding a second and third factor, such as gender and age, can turn a broad category into a personal identifier. In fact, marketing experts and law enforcement alike have developed considerable skill at identifying specific individuals by overlaying several pieces of nonspecific data.

Such distinctions are far from academic, although some academics have a keen interest in them, particularly when the data is health-related. By analyzing large accumulations of health data, medical researchers can discover remarkable and potentially lifesaving facts. However, the privacy implications of giving researchers access to large amounts of health data are enormous. One strategy is to "de-identify" the data, that is, strip it of any information that could enable someone to identify the individuals to whom it refers. The rules for doing this must take into account the relative nature of PII. For example, there are guidelines for the de-identification of medical data in the rules implementing the Health Insurance

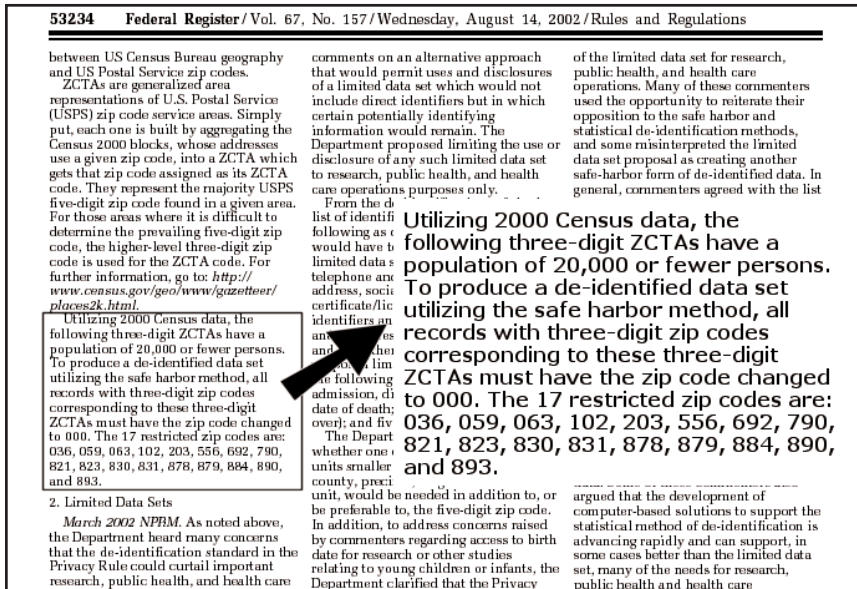
Portability and Accountability Act (known as HIPAA and discussed in detail in Chapter 4). If you read the ninety pages of densely-packed, three-column Federal Register text that constitute the final version of the HIPAA Privacy Rule, you will see that exceptions had to be made for certain ZIP codes when de-identifying data (see Figure 1-2). There are several variations on PII, notably PIMI, PMI, PHI, PMI and IIHI, all of which may be found in discussions of health information privacy and in legislation such as HIPAA. Here's what each one stands for:

PIMI: Personally Identifiable Medical Information

PMI: Personal Medical Information

PHI: Protected Health Information

IIHI: Individually Identifiable Health Information



53234 **Federal Register** / Vol. 67, No. 157 / Wednesday, August 14, 2002 / Rules and Regulations

between US Census Bureau geography and US Postal Service zip codes.

ZCTAs are generalized area representations of U.S. Postal Service (USPS) zip code service areas. Simply put, each one is built by aggregating the Census 2000 blocks, whose addresses use a given zip code, into a ZCTA which gets that zip code assigned as its ZCTA code. They represent the majority USPS five-digit zip code found in a given area. For those areas where it is difficult to determine the prevailing five-digit zip code, the higher-level three-digit zip code is used for the ZCTA code. For further information, go to: *http://www.census.gov/geo/www/gazetteer/places2k.html*.

Utilizing 2000 Census data, the following three-digit ZCTAs have a population of 20,000 or fewer persons. To produce a de-identified data set utilizing the safe harbor method, all records with three-digit zip codes corresponding to these three-digit ZCTAs must have the zip code changed to 000. The 17 restricted zip codes are: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.

2. Limited Data Sets

March 2002 NPRM. As noted above, the Department heard many concerns that the de-identification standard in the Privacy Rule could curtail important research, public health, and health care operations activities. Specific concerns

comments on an alternative approach that would permit uses and disclosures of a limited data set which would not include direct identifiers but in which certain potentially identifying information would remain. The Department proposed limiting the use or disclosure of any such limited data set to research, public health, and health care operations purposes only.

From the d
list of identifi
following as
would have t
limited data s
telephone an
address, soci
certificate/lic
identifiers an
an es
and the lim
ve following
admission, di
date of death;
over); and fiv

The Depart
whether one
units smaller
county, preci
unit, would be needed in addition to, or be preferable to, the five-digit zip code. In addition, to address concerns raised by commenters regarding access to birth date for research or other studies relating to young children or infants, the Department clarified that the Privacy Rule de-identification safe harbor allows

of the limited data set for research, public health, and health care operations. Many of these commenters used the opportunity to reiterate their opposition to the safe harbor and statistical de-identification methods, and some misinterpreted the limited data set proposal as creating another safe-harbor form of de-identified data. In general, commenters agreed with the list

Utilizing 2000 Census data, the following three-digit ZCTAs have a population of 20,000 or fewer persons. To produce a de-identified data set utilizing the safe harbor method, all records with three-digit zip codes corresponding to these three-digit ZCTAs must have the zip code changed to 000. The 17 restricted zip codes are: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.

argued that the development of computer-based solutions to support the statistical method of de-identification is advancing rapidly and can support, in some cases better than the limited data set, many of the needs for research, public health and health care operations. These commenters asserted

Figure 1-2 ZIP codes and HIPAA in the Federal Register

Why so many similar and overlapping privacy acronyms? Because data privacy is still an emerging topic, the language of

which is still evolving. Although PII, PHI, and IIHI are now fairly well-established in privacy circles, you can help avoid confusion and false assumptions if you explain privacy acronyms whenever you use them.

Legal Angles

Many countries have determined that the privacy of PII is important enough to merit legal protection. In some, that legal protection takes the form of broad privacy legislation which applies to almost all personal data in almost every situation. In other countries, notably the United States, the legislated protection of privacy is piecemeal, applying only to certain information in certain circumstances. For example, the privacy of your video rental records is specifically protected by the Video Privacy Protection Act (created in 1989, shortly after newspapers published a list of movies rented by Supreme Court nominee Robert Bork—presumably by politicians concerned that their movie choices might otherwise see the light of day).

Note that legislation is not the only way to provide legal protection for PII. A number of experts have argued that Americans enjoy extensive privacy protection under tort law. In other words, citizens have a right to sue for damages if they think they have suffered harm due to an invasion of their privacy. This position is extensively documented in a report prepared by Privacilla.org, a non-profit organization that describes itself as "Your source for privacy policy from a free-market, pro-technology perspective." Here is the conclusion of the report:

> "The privacy torts provide baseline privacy protections, below which no company or individual may go. They are not limited to any type of information or medium. They cover all information, including medical and financial information, and they apply equally to communications on or off the Internet."

A similar claim is articulated by the U.S. Department of Commerce in a paper titled "Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law." The paper was prepared in 2000, as part of the negotiations between the United States and the European Union over data protection and

something called Safe Harbor, a topic covered in more detail in Chapter 5. The goal of the negotiations was to assure Europeans that America can be a safe place for personal data despite the fact that the legal protections in America are not based on the broad legislated protection of data privacy to which Europeans have become accustomed. The paper asserts that:

> "The right to recover damages for invasion of personal privacy is well established under U.S. common law."

On the issue of damages, the paper concludes that invasions of privacy in the United States give injured parties the right to recover damages for any harm to their interest in privacy that results from the invasion, plus any mental distress proved to have been suffered, if it is of a kind that normally results from such an invasion. There may also be special damages of which the invasion is a legal cause (for an example of this, consider what happened when the *National Inquirer* breached the medical privacy of singer Tammy Wynette and reported that she needed a liver transplant—she suffered a loss of revenue due to cancelled bookings).

Privacy Promises: Recently, a completely different legal angle has been used to enforce what are being referred to as "privacy promises." If a company promises its customers that it will protect the privacy of their information and then fails to keep that promise, a charge of deceptive business practice maybe forthcoming, either from the Federal Trade Commission or any number of state business regulators. There is more about privacy cases of this type in Chapters 2 and 4.

While a detailed discussion of legal theory is beyond the scope of this book, knowing the lay of the land will help because privacy legislation and privacy litigation make a big difference to your company's responsibilities as a Web site operator or sender of email. Based on such parameters as intended audience, physical location, and type of content, your Web site may be subject to specific legislated privacy requirements. In addition, your company has underlying and much less specific legal obligations with respect to people's privacy, as well as other general legal obligations. Chapter 4 addresses U.S. legal requirements in more detail and Chapter 5 describes the privacy challenges that arise from the global nature of the World Wide Web.

Standard Legal Disclaimer: At point I should reiterate the standard legal disclaimer that says: "The information contained in this book is for general guidance only. The application and impact of laws can vary widely based on the specific facts involved. Accordingly, the information in this book is provided with the understanding that the author and publisher are not herein engaged in rendering legal, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional legal or other advisers."

Privacy Positives

Hopefully, most commercial Web site operators will regard the legal requirements of privacy as a baseline, a minimum standard that they will want to exceed in the interests of good business. Privacy as a positive business differentiator is certainly a theme you will find repeated throughout this book. While there will be a lot of talk about the potential for negative consequences from what is commonly referred to as a *privacy incident* or a *privacy breach*, privacy can also be defined in a positive way. For example, on the right of Figure 1-3 you can see a "privacy seal" displayed on a Web site.

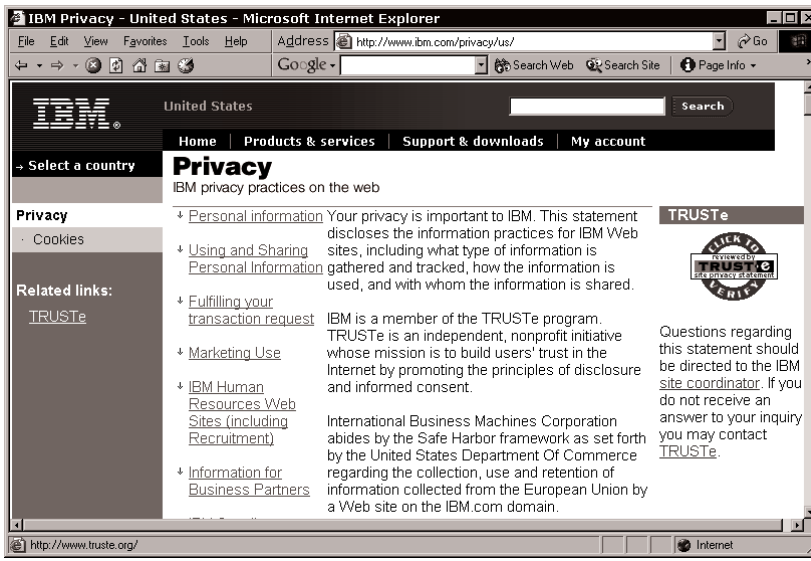


Figure 1-3: An example of a Web privacy seal

This seal represents a form of self-regulation among Web site operators—the seal can be displayed only by sites that meet or exceed a voluntary, self-imposed set of privacy standards. One powerful indicator of privacy's importance to Web users is the fact that within three years of its launch, the TRUSTe seal was the most clicked symbol on the Web, way ahead of second-place Microsoft and registering more impressions than Yahoo!, Amazon, and eBay combined. All major Web portals display the seal, and it can be found on 15 of the 20 most popular Web sites and on more than half of the top 100 sites.

Obviously, there are costs associated with using such programs, but the risk of negative legal and business impacts arising from a privacy breach makes risk mitigation a worthwhile investment for many companies. Chapter 9 has more about Web site privacy seals as well as Web privacy tools and technologies that are being developed to aid in risk mitigation. In Chapter 10 the business case for Web privacy will be stated in more detail.

Privacy Paradoxes

Of all the tasks involved in making sure that your Web site and email communications are an asset to your organization and not a liability, privacy is probably the most mentally challenging. When you start to come to grips with privacy issues, you can quickly find yourself wondering why it seems to be such difficult work. Hopefully, this section will help you understand why Web privacy is so difficult, and it will give you a framework for dealing with some of the tough decisions that you, or someone in your organization, will have to make about privacy.

Privacy is a formidable challenge because nobody yet understands exactly what privacy means in today's highly interconnected, heavily computerized, data-dependent world. About the best we can say is that privacy in the information age is a work in progress. In the same way that environmental risks continue to emerge as the dark side of the industrial/technological age, emerging privacy risks have been cast as the dark side of the information age.

Whether or not you agree with that assessment, it is indisputable that many people see databases and computer networks as a

threat to their personal privacy. Thus, to the extent that your business depends on access to, or makes use of, personal information, you will want to provide reassurances to those who need them, regarding the handling and protection of their personal information.

On the other hand, a lot of people enjoy considerable commercial benefits from information technology, many of which depend upon the sharing of personal information. A widely cited example is consumer credit, rapid and widespread access to which has been made possible by the sharing of information about people's accounts and payment histories.

Other examples are personalized service, special offers, and loyalty programs. When I stay at my preferred hotel chain, for example, I automatically receive expedited check-in, a free room upgrade, and a bottle of wine. Naturally, I choose to stay at this hotel chain whenever I can. The same principles can be seen at work in frequent traveler mileage programs operated by airlines.

Such personalized brand loyalty programs are possible only when customers are willing to trust companies with private information, such as travel plans and personal preferences (typically through use of an assigned customer number). If my preferred company were to betray my trust—for example, by selling my preferences without my permission to a marketing company, which then used them to pester me with sales calls—chances are it would cease to be my preferred company.

Wherever consumers see their trust abused, or perceive a lack of trustworthiness in those to whom they entrust personal information, they usually show reluctance in sharing personal information. In the context of the Web, and email this is reflected in consumers' reluctance to provide credit card information to Web sites, which surveys have consistently linked to doubts about the ability of Web sites to keep such personal data secure. The first privacy paradox can thus be stated as *a reluctance to divulge personal information, despite a desire for personalized products and services*.

The second privacy paradox concerns the *ownership* of information. Consider your company's customer list, the names and addresses of people who have purchased your products or services. Traditionally, businesses consider such information to be the

property of the business. Indeed, customer data can be a valuable business asset, particularly if it includes purchase histories, buying habits, personal preferences, and similar information. You only have to imagine what a competitor could do with such data to understand that it merits the protection of strong security measures, such as access control and encryption. However, your company's ownership of this data is, in many ways, shared with the people to whom it relates—and some of this sharing is prescribed by law.

Privacy Target: Do not underestimate how upset some visitors to your Web site can become if they think you have done, or have even thought about doing, anything that might amount to an invasion of their privacy. Many Web site defacement and Denial of Service (DoS) attacks are motivated by an attacker's feelings of righteous indignation. While such attacks can never be justified, taking steps to avoid becoming a target makes sense, particularly when those steps, such as posting and abiding by a comprehensive privacy statement, already make sense from a business perspective.

Consider your bank: it has both a right and a duty to know how much money you have in your account, but a number of laws limit how, and with whom, the bank can share this information. On the one hand, your bank is prohibited from sharing the information with you, unless it takes reasonable steps to assure that you are, in fact, you—a challenge that operators of banking Web sites will recognize.

On the other hand, the bank can tell anyone it likes how much money you have in your account, if that data is either aggregated or "de-identified" (stripped of identifying data). Your bank can share detailed and fully identified information about you with another company, such as a stock brokerage or insurance affiliate *if* it has your permission to do so.

Yet your permission is not required for the bank to reveal certain information about your account to the government (some deposits and withdrawals must be reported under various laws relating to money laundering, tax evasion, and terrorism). The bank is also required to tell you what information it maintains about you and give you an opportunity to correct any errors within that information.

So the second privacy paradox is this: *a company's ownership of information about people, such as its customers, may not preclude their ownership of certain aspects or pieces of that information*. And the third privacy paradox is that *ownership of information about people may create an obligation to share some of that information, for example with government agencies or individuals identified by the data*.

The Europeans Have a Word for It: Instead of saying "the individual identified by the data" or "the person to whom the data refers," the Europeans use the term "data subject," which I find very convenient. You will find it used in this sense throughout the book.

The Privacy Landscape

Something else that will help you deal with privacy issues pertaining to your business use of the Internet is a clear picture of the *privacy landscape*. In the United States the privacy landscape is shaped by two main forces: marketers and privacy advocates.

The marketers want to use information about data subjects to sell more products—for example, to target data subjects with a specific message: "Dear Jane: We know you enjoy up-market shopping and staying in fine hotels, so you'll be happy to know that rates at our MegaMall Resort are 50 percent off this month." Use of data for marketing purposes can also mean analyzing large amounts of information to discover trends (urban couples with new babies tend to dine at home, so send them offers from restaurants that deliver—and send offers from more upscale eateries to certain zip codes, based on property values and median incomes).

Privacy advocates want greater legal restrictions on what companies can do with information about individuals. Many privacy advocates in the United States would like to establish a clear and general legal right of data privacy where none currently exists, so that individuals can know they have some control over how information about them is used, regardless of whatever new ways of using such information may be developed. A representative statement of this position can be found in the book *Database Nation*, by Simson Garfinkel:

> "In these chapters, I've argued that the most effective solution for preventing the unwanted collection and disclosure of personal information is sweeping legislation designed to restore our right to privacy in this age of computers."

As you might expect, marketers and privacy advocates disagree a lot. For example, here is the conclusion drawn by Sonia Arrison in the study "Consumer Privacy: A Free Choice Approach," published by the Pacific Research Institute for Public Policy:

> "New laws governing the collection of consumer information are not needed....Instead, new information restrictions would usurp consumer choice, drive up prices for consumers, and strangle business, especially small business, with red tape."

That people disagree about privacy is to be expected. The debate over what to do about privacy is intellectually challenging and you may find yourself drawn into it on a personal level. What you need to know from a business perspective is that the debate is far from academic.

Privacy advocates today act as unofficial privacy watchdogs. Their role in several landmark cases, cited in different chapters, has been significant. Major corporations have faced serious regulatory action involving Web site privacy issues, due in no small part to the advocacy of groups like the ACLU and EPIC (respectively, the American Civil Liberties Union and the Electronic Privacy Information Center). If the folks in your marketing department are the driving force behind your company Web site or email communications, take note: You may need to balance their perspective with the near certainty that any flagrant violation of what privacy advocates consider to be "fair information practices" will come to their attention, with potentially costly consequences.

As was noted at the beginning of this chapter, every major business and computer publication has run at least one cover story about privacy in the last two years. This means you will not be able deflect privacy-related criticism of simply by saying "I didn't know it was *that* important."

Privacy Policies and Statements

The widespread media coverage of privacy helps explains why, when you visit any Web site belonging to a well-known company, there's a good chance you will see a link on the home page that contains the word *privacy* (there is an example from IBM's Web site in Figure 1-4).

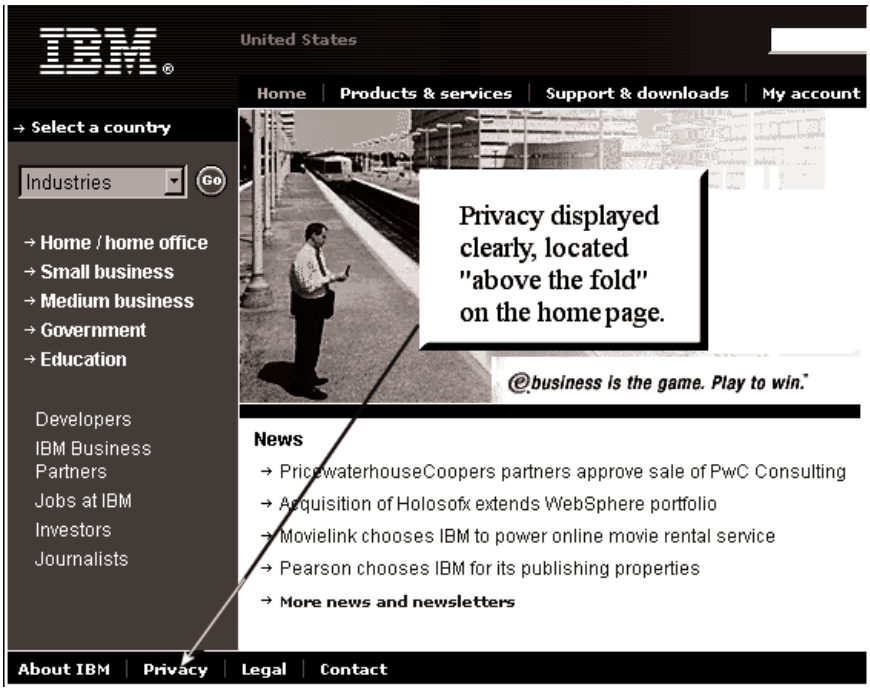


Figure 1-4 Corporate Web site privacy link (from ibm.com)

Such links invariably lead to a page stating the company's Web site privacy policies. There was an example of this earlier from IBM's Web site (Figure 1-3). The first task for a company getting to grips with Web site privacy is to make sure that all of the main pages on the company Web site have a link to a page about privacy.

The privacy page may be called a Privacy Statement or Privacy Notice. Some sites use the term Privacy Policy although, as I explain in Chapter 6, that might not be the best term to use in this context.

The Better Business Bureau, or BBB, is another well-known organization that provides a privacy seal. The BBB describes a good privacy notice as:

> "easy to find, easy to read, and comprehensively explains all your online information practices."

In other words, a privacy notice or statement should be an integral part of your site's design. The creation of a privacy statement is covered in Chapter 6.

Note that a privacy notice should be posted even if your Web site does not collect or maintain any PII. For a start, visitors to your site don't know you are not collecting information about them unless you tell them. A privacy notice for such a site may not have a whole lot to say, but the fact that you have gone to the trouble of saying it may win you praise and deflect potential criticism. Furthermore, if you later decide to do things with your site that require the collection of information, having a privacy notice in place already will make it easier. You simply expand the existing notice—the necessary links are already in place.

Posting a privacy notice on your Web site is not just a matter of looking professional. Evidence from consumer surveys shows that people look for such statements when browsing at new sites, and people pay particular attention to them when shopping on the Web.

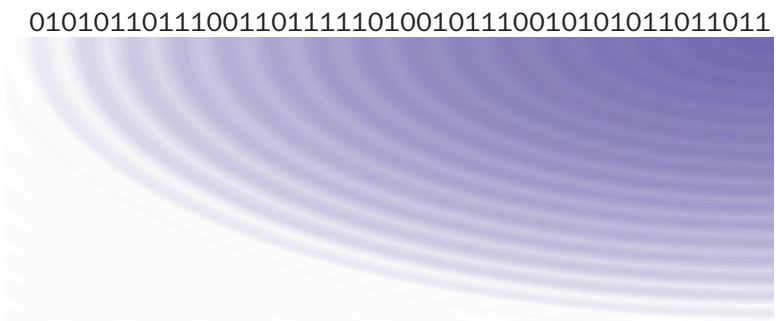
You may have seen some surveys suggesting that few consumers read privacy statements. This may well be true, but it does not mean they don't notice when a site doesn't have one. If the experience of sites that display a privacy seal is any indication, this extra attention to privacy is well rewarded. Surveys indicate that nine out of ten Web users actually mistrust privacy statements *unless* the site uses a third-party oversight program such as TRUSTe. (See Chapter 9 for more on how to get one for your Web site.)

What's Next?

Now that I have laid the basic groundwork, I want to give you a closer look at privacy problems that can arise from company Web sites and email operations. Chapter 2 describes privacy incidents that have shaped the privacy landscape for businesses, and the costs that incidents of this type can incur. Beginning in Chapter 3, I start to assemble the building blocks of business privacy solutions, starting with basic privacy principles. Chapter 4 examines how those principles are embodied in privacy laws, and what those laws imply for business Web sites and email. Because WWW stands for *World Wide* Web, Chapter 5 examines the international aspects of privacy for business. In Chapter 6, the task of creating privacy policy is described. The need for an overall business strategy with respect to privacy is addressed in Chapter 7, which also describes strategies for responding to privacy incidents. Chapter 8 focuses on privacy and email, while Chapter 9 looks at tools that are available to help with privacy tasks. In the final chapter, Chapter 10, there is a summing up, together with some of my thoughts about what all of this means for businesses and why good privacy practices are good for business.

Chapter Two

Privacy Incidents and Their Costs



"Online retail sales would be approximately 24 percent higher in 2006 if consumers' fears about privacy and security were addressed effectively. With poor online privacy practices, many companies will experience negative effects not only on their online sales over the next several years, but also on off-line sales that shift to more privacy-sensitive competitors. Jupiter forecasts that as much as $24.5 billion in online sales will be lost by 2006, up from $5.5 billion in 2001." —*Online Privacy: Managing Complexity to Realize Marketing Benefits*, Jupiter Media Metrix (www.jmm.com).

2: Privacy Incidents and Their Costs

In this chapter I describe the kind of Web privacy problems you want to avoid and the costs can incur if you don't. Some are real cases, others are hypothetical. I want to give you an idea of the range of problems that can arise and the seriousness of their potential impacts on the business. The goal is to help you identify potential problems at your company and encourage you to take the appropriate steps to deal with them. This chapter should also prove helpful if you are trying to raise privacy awareness within your organization. Showing people real examples of what can go wrong is a proven strategy for encouraging them to trying harder to get things right.

Defining "Privacy Incident"

The first step to understanding privacy incidents is defining what they are. Consider this definition: a privacy-related event with potentially negative consequences. In fact, articles and presentations about privacy often use "privacy incident" as shorthand for "damaging privacy incident." Examples of such events include: hackers gaining unauthorized access to your Web site and stealing personal information about your customers; an employee using her authorized access to customer records to find sensitive information to sell to the press; your marketing department emailing sales literature to customers who asked not to receive such email; upper management deciding to make changes to the company's Web site privacy policy that result in widespread public criticism of the company.

Not all privacy incidents result from lapses in security. Some are violations of policy while others result from poor judgment. To define "privacy incident" in plain English: it has to do with privacy, and it's not good. In the specific context of Web privacy you might

say: something's happened, it has to do with privacy and the Web site, and it's not good. This is undoubtedly what some employees at pharmaceutical giant Eli Lilly thought in June of 2001 when they found out that the email addresses of people who had registered on the company's prozac.com Web site —"Your Guide to Evaluating and Recovering from Depression"—had been publicly revealed due to an error in an email program written by the company's IT department.

You will find the Prozac Email Incident widely reported and discussed in privacy journals, but not because anyone wants to make an example out of this particular company. The simple fact is that the Prozac Email Incident was the first of its kind and so it has become the defining Web-related privacy incident: a programming error led to a privacy breach which drew public criticism and triggered a regulatory response. In many ways it was the privacy nightmare scenario, but that also means much can be learned from it, hopefully preventing future incidents of this type.

The Costs of a Privacy Incident

A privacy incident can cost a business in many different ways, from the number of person hours diverted to deal with the incident, to the loss of customers and brand value. This section discusses different types of cost, illustrating them with some real world examples.

Scrutiny and Glare

There may be a few people for whom there is some truth in the saying "There's no such thing as bad publicity," but don't try telling that to your CEO right before she has to take a call from a Washington Post reporter who wants to know why your company's Web site revealed the credit card numbers of several thousand customers. For businesses, there definitely *is* such a thing as bad publicity. Consumers tend to vote with their wallets and unless your company happens to have a monopoly, the media glare associated with bad news can rapidly impact the bottom line as customers switch to other suppliers.

Bad news can also have a cumulative effect. For example, less than six months after Eli Lilly reached a settlement with the Federal Trade Commission (FTC) regarding the aforementioned prozac.com privacy problem, the company was accused of another Prozac-related privacy violation. This second case involved samples of Prozac which were mailed to people in Florida, through a marketing deal involving—allegedly—the recipient's physician, the recipient's pharmacist, and Eli Lilly sales reps. The incident did not involve the Internet or the company Web site, but you can bet that reporters writing about this latest incident took the opportunity to remind people of the company's troubles with the FTC over the earlier Prozac-related privacy incident.

CNET tech sites: Price comparisons | Product reviews

c|net NEWS.COM TECH NEWS FIRST

Front Page | Enterprise | E-Business | Communications | Media

FTC to settle Eli Lilly privacy probe

REUTERS

By Reuters
January 11, 2002, 2:55 PM PT

update WASHINGTON--Pharmaceutical giant Eli Lilly is close to a settlement with the U.S. government for releasing an e-mail list last summer of patients who used its anti-depressant drug Prozac, according to sources familiar with the matter.

The Federal Trade Commission is investigating whether Lilly engaged in unfair or deceptive trade practices when it mistakenly revealed the e-mail addresses of more than 700 Prozac users, the sources said.

The FTC could announce a settlement as soon as next week, sources said.

It would be the first settlement with a major U.S. company for privacy violations since the FTC announced last fall that it was stepping up efforts to protect consumer privacy.

Figure 2-1 Lilly CNET

To understand the costs of a privacy incident in general, and the costs of scrutiny in particular, it might help to think of a rock thrown into a pond. First, there is a large initial splash at the point of entry. In the Prozac Email Incident, this was the message hitting

the in-baskets of the hundreds of recipients, each of whom could see the email address of the other people who got the same revealing message. From the initial splash, waves emanate in concentric circles, the first wave being a call to the American Civil Liberties Union (ACLU). This was followed by the ACLU taking the matter to the FTC, then the press coverage of the incident and the ACLU's involvement. When the FTC decided to pursue the matter there was more press.

Eventually the waves spread out across the entire pond and start rippling back. This is the deployment of Eli Lilly resources to respond, first to internal personnel, then to the press, then to the FTC. Employees had to be interviewed to find out what happened. Documents had to be assembled ready to submit to the FTC investigators. Decisions had to be made about how to respond, what documents to submit and which to hold back. Legal counsel had to be consulted at all stages of the response process. Probably there were several rounds of document requests from the FTC as it framed its complaint (published on the FTC web site, and quoted later in this chapter). Eventually, a settlement is negotiated, which brings more headlines (see Figure 2-1).

Settlement Costs

Depending on the relative size of the rock and the pond into which it is pitched, the waves can keep going for some time. The original Prozac Email Incident occurred at the end of June, 2001. In January of 2002, Eli Lilly agreed to settle the FTC charges. In doing so, the company did not have to admit any violations of the law, but it did have to accept a series of requirements set out by the FTC, including close oversight of certain internal and external activities. Some of the requirements extend twenty years into the future and failure to meet them could result in fines, further actions, and an extension of the period of compliance beyond twenty years. The Sources section at the end of the book has more about what the FTC required, but the following is a short summary:

- Create and maintain an information security program that identifies, and defends against, all internal and external security risks to personal information from or about consumers, including any risks due to lack of training.

- Complete a written review of the security program within 90 days of the agreement, and every year after that.
- Make available to the FTC all reports, studies, reviews, audits, training materials, and plans relating to compliance with the information security program.
- Make available to the FTC every print, broadcast, cable, or Internet advertisement, promotion, form, Web page, email message, or other document that says anything about the collection, use, and security of personal information from or about consumers.
- Make sure all current and future company officers, directors, managers, employees, and contractors who have anything to do with personal consumer information are shown a copy of the agreement.
- Submit a report on compliance with the agreement within six months of the agreement and at any other time the FTC asks for one.
- Avoid any further misrepresentation of the level of privacy protection Lilly provides for consumers' personally identifiable information.

This last item is significant because the order lasts twenty years from the date it is issued, or twenty years from the last date that the FTC or other agency files a complaint alleging any violation of the order. In other words, if there is anything like a repeat of the original incident, the company could find itself in several kinds of trouble (which could be the case if Florida's Attorney General acts against the company under that state's Deceptive and Unfair Trade Practices Act in the aforementioned Prozac postal case). Violations of an FTC consent order can result in further sanctions, including civil penalties up to $11,000 per violation.

The cost of fixing the problem and complying with the terms of any settlement you may reach comes on top of any fines that may be involved. For example, fines may be levied to pay for the cost of the investigation. After the FTC settlement, several states sought payment from Eli Lilly for the legal costs they incurred in their own investigations of the incident (paying $160,000 to 8 states). Some observers have suggested that what Eli Lilly agreed to do in response to the Prozac Email Incident was no more than any company

should be doing anyway with respect to information protection. However, there is a big—and potentially expensive—difference between carrying out such a program on your own terms and doing it under the watchful eye of others, in this case the FTC *and* privacy watchdogs (the ACLU has already filed requests for copies of all compliance documentation).

Coping Costs

So what would something like the Prozac Email Incident cost your company? Apart from the intangible costs that come from having your brand name tarnished, there are some very tangible costs, starting with the legal bills. If you are facing legal action from either the Federal government or state regulators you will probably want to retain expert external counsel to bolster in-house legal resources. Such experts do not come cheap. You can also bet on there being an overtime bulge in your public relations department.

In March of 2001, Forrester Research issued a landmark analysis of privacy for business titled *Surviving the Privacy Issue*. In this report Forrester quantified the cost of a privacy "blowout." The numbers, shown in Table 2-1, make very interesting reading. The categories into which the costs are broken down are a useful checklist if you want to perform a similar analysis for your company.

Cost of a Privacy Blowout	**Small Dot Com**		**Big Company**	
Category	Time (hours)	Cost ($)	Time (hours)	Cost ($)
CEO/president time	86	$ 7,100	48	$ 8,100
Management time	95	$ 5,544	620	$ 38,889
PR Meetings and calls	40	$ 1,067	800	$ 21,333
Management press calls	26	$ 1,778	76	$ 5,456
Management review of privacy practices	15	$ 833	250	$ 13,889
Customer service calls and emails	88	$ 1,944	18,750	$ 416,667
Employee communications and training	1	$ 1,333	18,770	$ 335,889
External consultants		$ 22,500		$ 181,250
Travel		$ 2,000		$ 16,500
		$ 44,099		**$ 1,037,973**

Table 2-1: Cost of Privacy "Blowout" as estimated by Forrester Research in the 2001 report *Surviving the Privacy Issue*.

As you can see, Forrester performed the same analysis for both a large and a small company. While there is a big difference in the raw numbers, the total costs are probably about the same if you

figure them as a percentage of income or revenue or capitalization. In other words, a privacy incident can have a significant impact on the bottom line, whether your company is a small one or a large one.

Note that the costs in Table 2-1 do not include either loss of business or fines imposed by regulators. What they do include is worth a closer look just to be clear on where the impact of the incident will be felt.

- CEO/president time
- Management time
- PR meetings and calls
- Management press calls
- Management review of privacy practices
- Customer service calls and emails
- Employee communications and training
- External consultants
- Travel

Opportunity Costs

Another way to look at the costs of a privacy incident is what it does to the company's stock price. Eli Lilly was trading close to $80 per share right before the incident occurred. Over the next ten days it dropped to $74. However, it soon started to recover and within two months of the incident it was over $80 again. So you could argue that the overall effect of the incident was insignificant, especially when compared with other factors at work that summer, such as the expiration of the patent for Prozac which generated revenues of more than $20 billion in less than a decade, more than a quarter of the company's total revenues. Nevertheless, there is a strong case for saying that any time a company incurs unexpected and avoidable costs it is bad news.

In assessing the impact of this or any other incident there can be no avoiding what economists call "opportunity cost." Simply put, this is what you could have done with the time and money that the

incident expended. Suppose that on the first day of the first quarter of the year, a glitch on your Web site reveals the names, phone numbers, and email addresses of several thousand men who have registered for a newsletter about impotence. Some of them are very upset and talk to a lawyer. The press gets hold of the story. You open up your Privacy Incident Response Plan and activate your Privacy Incident Response Team (you will read how to create a PIRP and deploy a PIRT in Chapter 7). Through a combination of Herculean technical, legal, managerial and PR efforts you fix the glitch and diffuse the situation. By the end of the quarter the whole thing is history.

At first, this sounds like success. Suppose that by getting more work out of some people, by shifting some resources around and cutting back on some other expenditures, you accomplished the above with no apparent impact on the bottom line. On several levels this would be considered an amazing accomplishment. Unfortunately, what the law of opportunity cost tells you is that the incident was still bad news for the company. Why? Because if all these efforts had been directed at something else besides recovering from a privacy incident, the bottom line would almost certainly have looked a lot better than it did.

This can be a hard pill to swallow, so to speak, especially if you and your staff are patting yourselves on the back for the great work everyone did to minimize the damage from an incident. But think about the resources the damage control required: public relations, technical, management, legal. With those same resources a new marketing campaign could have been designed, implemented on the web site, and launched in the press. Revenue could have been boosted. That is opportunity cost and that is why it is best to make a concerted effort to avoid such incidents in the first place.

Cost Limits and Gaps

Why would the recommendation be "make a concerted effort to avoid such incidents in the first place" as opposed to "defend against a privacy breach at all costs"? Once again the answer is economics, specifically opportunity costs and diminishing returns, both of which must be factored in when deciding how much to spend to mitigate privacy risks. Such calculations will be familiar to

those involved with information security management. Suppose it will cost $1.7 million to install software to protect the confidentiality of your data with powerful 128-bit encryption, but only $1.2 million if you use a weaker option, say 64-bit encryption. Is the $500,000 extra for stronger encryption a worthwhile investment? How likely is it that someone with the resources to break the weaker encryption, but not the stronger encryption, will target your data?

In other words, there comes a point of diminishing returns in any risk reduction plan. In terms of privacy, you probably do need to spend money to beef up your privacy awareness among employees, to perform a privacy audit of your Web site and to participate in a Web privacy seal program. But you can't just keep spending on privacy programs. Their cost must be weighed against other needs within the company.

One way to look at this is "closing-the-gap analysis." This is different from a plain ordinary "gap analysis," which you may have heard mentioned in the context of privacy compliance. Ordinary gap analysis is simply looking at where your organization stands today, relative to some standard with which it needs to comply. This standard may be legislated, as in the case of the Children's Online Privacy Protection Act (COPPA). Or it might be a voluntary standard, such as industry best practices, or an ISO standard. Such gap analysis often precedes and serves as a roadmap for a compliance effort. The purpose of closing-the-gap analysis is to determine at what point your investment in risk reduction measures, ceases to make a meaningful difference.

Consider the chart in Figure 2-2 on the next page. The Y-axis of the chart is the probability of a privacy incident occurring at an organization. The X-axis across the bottom is the number of privacy programs the organization has implemented. Privacy programs is a broadly defined category in this context, encompassing any measures which enhance privacy posture, such as privacy awareness campaigns, privacy training for key employees, privacy audits, and so on.

At first there are no privacy programs and the probability of a privacy incident is high, almost a certainty (where a certainty equals 1.0). Employees are either unaware of the importance of protecting personally identifiable information or not terribly serious about

actually protecting it. The effect of the first privacy program is thus considerable, as indicated in the chart. The probability of a privacy incident occurring has been moved closer to zero . The probability is further reduced by the second program, but the effect is less dramatic— the gap between current probability and zero closes by a smaller amount this time, and each time thereafter.

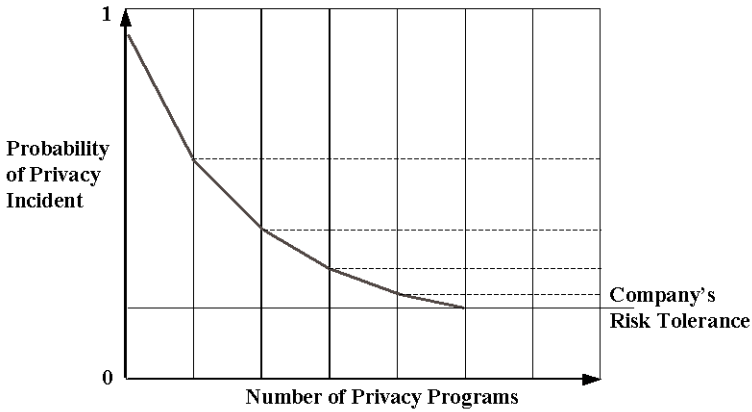


Figure 2-2: Closing-the-gap analysis

How close to zero can, or should, you bring the probability of a privacy incident? That depends upon several factors, including the incremental cost of privacy programs and your company's "risk tolerance." Think of risk tolerance as how comfortable management is with taking a chance that things will go well, given an accurate description of both the risks faced and the mitigation efforts in place to reduce those risks.

As you might expect, different companies, at different stages in different industries, have different risk tolerances. Consider a small startup company creating game software that is licensed to larger companies. The company does not deal directly with the public, has very little contact with personally identifiable information, and is accustomed to living on the edge; risk tolerance is probably high. Take the same company a few years later, when its name has become a household word and its core business has evolved into direct sales of online games that appeal to children, played over the Internet. Risk tolerance is probably a lot lower.

An extensive discussion of risk management theory is clearly beyond the scope of this text. What you need to be thinking about at this point is the balance between your desire to protect the company from damaging privacy incidents and all the other things to which the company needs to pay attention; then allocate resources in order to fulfill its mission. Or to put it another way, it is great that you are concerned about privacy because privacy is very important, but don't lose perspective.

Fines and Other Costs

The cost of a privacy incident can be the fines your company has to pay for breaking certain laws. This was hinted at earlier in relation to Eli Lilly and the Prozac Email Incident, which was investigated under the Federal Trade Commission Act (FTCA). Although Lilly did not pay a federal fine, it did enter into a consent decree, future violations of which can incur fines; and Lilly did pay fines to eight states. The total paid was $160,000 which might sound like a lot if you are a small company, but the Indianapolis-based pharmaceutical giant is not—the fines represented less than $5 per employee, or about half of one percent of what the company CEO earned in 1999.

Numerous companies have paid fines for violating the Children's Online Privacy Protection Act (COPPA), a law discussed in more detail in Chapter 4. In fact, the FTC marked the first anniversary of the effective date of COPPA by announcing settlements with operators of three Web sites: www.girlslife.com; www.bigmailbox.com; and www.insidetheweb.com. These companies were all charged with illegally collecting personally identifying information from children under 13 years of age without parental consent. They paid a total of $100,000 in civil penalties (they also had to delete all personally identifying information collected from children online at any time since the legislation went into effect).

There is more privacy legislation in the pipeline, with more potential for fines, but Web site privacy problems can have less obvious impacts. One is the lost deal or opportunity. Quite often in business, two or more companies come together for some kind of deal, such as a merger, acquisition, strategic alliance, partnership or capital investment. Normal business practice is for the companies involved to perform due diligence, business-speak for "check them

out." Due diligence means asking a lot of questions, such as: Who are these people? How is their credit? What is their reputation? During the last decade a new category of question emerged: How good is their data security? In fact, security consulting companies like the one I used to own were hired to assess information security at companies that were the target of a merger or acquisition.

Now, there is a new category in due diligence, which goes to the heart of Web site privacy practices by asking the question: how "clean" is the PII that a company has collected? The word "clean" can have several meanings in the context of data, for example, there are companies who specialize in cleaning up databases by eliminating duplicate records and correcting some mistakes (such as the wrong state/zip code).

In this context clean means compliant with privacy policies. Suppose that a company which is about to be acquired says, "we have a list of 300,000 people who have given permission for us to send them sales literature." Privacy due diligence requires that assertion be verified. Further suppose that, upon examination of the company's Web site, it appears that all customer email addresses are added to this list, regardless of whether or not they check the box marked:

"Please tell me about new product developments."

The list is thus deemed "dirty," and it will either need to be cleaned up, or its value discounted (lists that are purely opt-in are more valuable than those that are not). Such discrepancies, between list description and list reality, are particularly significant if they are associated with a Web site that has a privacy statement which is specific about how PII will be used, such as a strong statement like "we will NEVER send you offers if you ask us not to." Tempting as it might be, in the heat of a deal, to violate such a pledge, it may not be worth the risk of a privacy incident.

The same temptation arises when a company wants to cash in on data it has collected, not an uncommon business strategy these days. In an article in *Business 2.0* magazine in July, 2001, Warren Packard, managing director for Draper Fisher Jurvetson, a venture capital firm in Redwood City, California, said he was seeing more companies in financial trouble selling off consumer data, and noted:

> "It is a concern when someone's business model is not working and they are looking for alternative sources of revenue. The more granular the data you sell, the more you can get for it and some companies are going to get so desperate that they are going to sell their data outside with personally identifiable information."

Note that, in the same article, Packard was asked if he could think of any functioning company that has been punished by the market for conducting a data fire sale. He could not, but that misses the point. If the company that gets into trouble selling its data is already on its way out of business, it is somewhat immune to criticism. However, the buyer of the data needs to be sure they are not paying too much. For example, if a large number of people on the list object to the new owner contacting them, the costs, in terms of complaint calls alone, could cancel out any gain.

Types of Privacy Incident

The following sections discuss the main types of privacy incident. You will be better prepared to develop appropriate responses if you have thought about the different ways in which privacy could become a problem for your company. Bear in mind that the categorization of incidents presented here should not be considered exhaustive. You may think of something specific to your company that does not fall into these categories. If so, be sure to document it for when you get to Chapter 7 and start to prepare your privacy incident response plan.

Security Breach

When a Web site is attacked and security mechanisms fail, the potential clearly exists for a privacy incident. This was the case at the University of Washington Medical Center in March of 2000 when a hacker downloaded medical records, health information and social security numbers of more than 5,000 patients—data which is clearly personally identifiable information or PII. Later that year, Western Union's Web site was hacked and the credit card numbers of 15,700 customers were exposed. More recently, Qwest Communications acknowledged in May of 2002 that its Web-based

paperless billing system had stopped checking passwords, allowing anyone who entered a valid username to access that subscriber's billing record, including a complete copy of their most recent phone bill and, if they paid by credit card, the card number and expiration date. Web site security breaches with privacy consequences are typically the result of one or more of the following factors:

- External Attack: someone with no prior internal knowledge of the company attacks the Web site, or systems containing Web-derived data, thereby compromising PII.
- Internal Attack: someone inside the company or with inside knowledge of the company systems, attacks the Web site or internal systems containing Web-derived data, thereby compromising PII (note that many attacks which appear to be external actually involved an internal component).
- Configuration Error: errors in the configuration of systems that process Web-derived data, or security measures put in place to protect such systems, allow PII to be compromised.

A Security Breach Example

While it is never fun to be the victim of a Web site hack, the consequences can vary a great deal according to the type of attack. If the site is simply defaced you can restore it fairly quickly from backups. If PII is compromised, that is, exposed to persons who do not have permission to access it, there is potential for a privacy incident. This was the case in the UWMC and Western Union examples, and a host of other incidents.

At Western Union the incident was particularly embarrassing because the company has built its reputation on safely delivering money, yet here it was, in September of 2000, calling thousands of customers—such as myself—to advise them to cancel the credit cards they had used at the Western Union web site. This was not good news for customers, who had to deal with the hassles of canceling a credit card and the worrying thought that an unethical stranger might have their personal details (see "Consumer Costs" section later in this chapter for more on this topic).

The news was not good for Western Union investors either. Within two days of the story breaking in the press the stock had lost

ten percent of its value. Fortunately for Western Union, it is just one part of a large company, First Data, which happens to be the largest processor of credit card transactions in the U.S. The stock price recovered quite quickly as bargain hunters stepped in, but you can wager that being an executive of Western Union during that time was not fun.

Security or Privacy?

The Western Union incident, like many others over the last ten years, was reported in the media as a security breach. This is technically correct, since what happened was a failure of security. In this case, according to some reports, Western Union had turned off some security mechanisms while they were doing maintenance on the site and a hacker who was probing the site at the time noticed. The hacker gained access and captured the credit card information as proof of this "accomplishment."

A Word to the Wise: If you ever find exposed data, you need to be very careful how you report it. Some people do not take kindly to being told their system is misconfigured, or insecure, or otherwise below par. One way for such persons to mitigate embarrassment and deflect blame is to attack the messenger. A particularly devious strategy on the part of a system owner or manager is to characterize the person reporting the problem as a hacker, a skilled and somehow dubious attacker. Casting matters in this light minimizes the system owner's culpability and may even elicit sympathy; it doesn't do anything good for the messenger.

A few months ago I found, quite by accident, thousands of unprotected personal records on a Web server that was hosting sites for a wide range of professional organizations. No hacking skills were required to get to this data, but I did not want to find myself having to explain this to people less versed in the topic than me (like a judge and/or jury). So I asked a third party to pass along a suggestion to one of the associations: ask your Web hosting company to move PII off the Web server or tighten permissions on the directories in which it is stored. That was enough to prompt the company to improve the security of all of the sites it hosts.

According to the three factors listed earlier, this was a combination of External Attack and Configuration Error. The latter is surprisingly common but very few cases are actually made public. When they are, it is often by individuals who could hardly be

described as hackers. In the Qwest example it appears that some customers were annoyed that Qwest was not moving quickly enough to fix the problem once it had been reported.

As a Web site operator you need to make sure you have a way of tracking such reports. The problem with data compromise is that, without strong evidence to the contrary, you have to assume it is absolute. In other words, even when it is caused by an honest mistake and is reported by an honest person, you have to assume the worst, unless you can prove that nobody actually saw the data during the time it was visible (something that is very hard to achieve).

According to several accounts, the hacker in the Western Union case was not seeking to profit from the credit card data that was exposed, but that hardly fits the definition of a reliable assumption. The only assumption the company could make was the one it did, the worst one—hence the advice to customers to cancel the cards that had been exposed.

Whilst some people might find the details of such incidents fascinating, most consumers are not interested in the finer points of a security violation. These incidents are, from the consumer perspective, privacy incidents. This is not because consumers cannot think in terms of data security. Many consumers actually implement security concepts such as data classification and access control (in simple terms, for example, there are some things you don't tell certain people). The point is, the data that consumers protect is personal, private data. When that data is exposed, it is perceived as a violation of privacy, not security.

Businesses that operate Web sites should note that the press is increasingly likely to report incidents like the Western Union hack as privacy breaches. The press has picked up on the consumer perspective, partly because the press are also consumers. Most know that if a credit card is compromised they won't have to pay for fraudulent charges, but they will have to go through a lot of effort and aggravation to replace the card. Sadly, there is an increasing probably that they will also know, personally or through a friend or relative, the much greater pain of identity theft (for more on this topic, see the section "Identity Theft" later in this chapter).

Policy Violation

When someone violates your company's Web site privacy policy this can lead to a privacy incident. Suppose there is a form on your Web site where people can request information about your products via email. There is another form where people who need technical support can report a problem and provide an email address for follow up. The Web site privacy notice states that information collected for support purposes will not be used for marketing without permission. If someone emails product marketing information to people who supplied their email addresses for support only, you have a policy violation.

Policy Violation Example

An example of Web site privacy policy violation is the Toysmart case. In July of 2000, Toysmart agreed to settle charges the company violated Section 5 of the FTC Act by misrepresenting to consumers that personal information would *never* be shared with third parties and then disclosing, selling, or offering that information for sale in violation of the company's own privacy statement. The agreement forbids the sale of this customer information except under very limited circumstances. Basically, Toysmart was in financial trouble and sought to sell its mailing lists and customer data. Since the company had promised, in its policy statement, not to do that, the FTC blocked the sale. One lesson here is that companies which seek to acquire PII, as part of a business deal for example, must make sure that the entity selling the data has the right to do so.

As was observed earlier with respect to Eli Lilly, the FTC is apt to see failure to live up to the assurances provided in a privacy policy as a violation of that policy. In other words, you do not have to do anything as flagrant as try to sell PII when you promised you wouldn't for a violation to be called. Consider the Microsoft Passport case, settled by the FTC in the summer of 2002.

Microsoft's privacy policies for Passport, an Internet service that allowed users to sign in at any participating Web site with a single name and password, included statements such as, "Passport achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information" and "Your Passport is protected by powerful online

security and a strict privacy policy." According to the FTC's complaint, Microsoft falsely represented that:

> It employs reasonable and appropriate measures under the circumstances to maintain and protect the privacy and confidentiality of consumers' personal information collected through its *Passport* and *Passport Wallet* services, including credit card numbers and billing information stored in Passport Wallet;
>
> Purchases made with Passport Wallet are generally safer or more secure than purchases made at the same site without Passport Wallet when, in fact, most consumers received identical security at those sites regardless of whether they used Passport Wallet to complete their transactions;
>
> Passport did not collect any personally identifiable information other than that described in its privacy policy when, in fact, Passport collected and held, for a limited time, a personally identifiable sign-in history for each user; and
>
> The Kids Passport program provided parents control over what information participating Web sites could collect from their children.

As a result, Microsoft found itself in a similar position to Eli Lilly, having to undertake a series of reforms, all with extensive government oversight. Microsoft has since altered the Passport product substantially and, if you visit Microsoft Web sites today, notably those at its Internet service, MSN, you will see a strong emphasis on privacy. In other words, Microsoft's response to the criticism was to accept it and learn from it, resolving to make privacy a priority rather than a liability.

Privacy Policy Catch-22

As you consider the impact of privacy policy violations, and the more fundamental question of what your privacy policies will be, you do need to be aware of a potential Catch-22: If you post a privacy statement on your Web site to demonstrate your commitment to privacy, you must stick to it, otherwise you could be facing legal problems that would not arise if you did not post such a statement. So making an effort to do the right thing could lead to

more trouble than not making an effort. Of course, if you don't post a privacy statement on your Web site you might find people are reluctant to use the site.

What sort of legal trouble are we talking about? In Chapter 4 you will read about a number of laws that are specific to privacy and Web sites. However, several major companies have endured embarrassing Web-related privacy incidents due to a law that is not privacy or Web specific: the Federal Trade Commission Act of 1914. Under section 5(a) of the FTCA: "unfair or deceptive acts or practices in or affecting commerce are declared unlawful." So here is what FTC Chairman Timothy Muris said at the news conference in Washington in August of 2002 announcing the agency's settlement with Microsoft over the Passport charges:

> "Companies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It is not only good business, it's the law. Even absent known security breaches, we will not wait to act."

Taken together with the FTC's action in the Prozac Email Incident described earlier, this is a clear signal that privacy statements must be adhered to, by law. This is a topic that will be revisited in Chapter 6. For now, ponder the words of Computerworld's Patrick Thibodeau:

> "In its enforcement action against Microsoft Corp. this week, the U.S. Federal Trade Commission demonstrated its ability, once again, to hang companies with their own words."

Policy Change

If there is one thing that companies can learn from the wild business cycles of the last few years it is that things change, sometimes very rapidly. Markets shift, business models change, technology advances. Not surprisingly, it can be hard for the company Web site to keep pace. Most companies recognize this when they craft a privacy statement for their Web site, typically including language that will allow for future changes to privacy policy. Here are two examples:

> "Sears.com may update this policy from time to time. Please check our policy periodically for changes."

> "The Lycos Network will update this policy from time to time so please check back periodically. When such changes occur, you will see the word "Updated" next to the Privacy Policy link on the front page of each site on the Lycos Network. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will prominently post such changes prior to implementing them."

Unfortunately, some companies have failed to warn people that the privacy policy may change. Others have made changes that exceed what some people consider acceptable. In other words, even if you tell people the policy may change, you cannot expect to escape criticism if you make a major change in the direction of less privacy protection.

Policy Change Example

To find out what sort of problems companies have encountered with privacy policy changes, simply go to google.com and use the following search phrase: privacy policy change uproar. At the top of the search results you will probably find a story about Yahoo. In March of 2002, this major Web portal changed the "marketing preferences" page by which users give, or decline, permission for Yahoo to send them promotional email. In so doing, the company reset the default preferences for all members, requiring them to manually request blocking of future messages, even if, in the past, they had declined to accept such email.

This action was roundly criticized by many Yahoo users and privacy advocates added their voices to the clamor. Whether Yahoo actually suffered any loss of business directly attributable to this incident is hard to tell. The effect was more likely a tarnishing of the brand. A lot of people who experienced this incident lost a measure of respect for the company, which may affect their future choices about Web services.

Note that Yahoo had planned to notify everyone who would be affected by the change, but word of the change got out before everyone was notified. This only compounded the criticism since a lot of users found out about the change in the press, before they

were told by Yahoo. Also note that Yahoo is by no means the only big name Web site to be criticized for a change in policy.

Policy Criticism

Public criticism of your company's Web site privacy policy can come from several quarters. Such criticism can be triggered by a change, as discussed in the previous section, but it can also be triggered simply by someone deciding that the policy, as it is, has problems.

Policy Criticism Example

For an example of a company facing criticism of its privacy policy you need look no further than the Web's largest auction site, eBay.com. In March of 2002, eBay faced a huge wave of criticism and a call for the FTC to investigate changes to eBay's privacy policy for possible "unfair or deceptive trade practices." While this wave of criticism was triggered by a change in policy, the very vocal objections to the change caused more people to read the company's privacy statement and find fault with things that had been there for some time. Here is how Jason Catlett, President of junkbusters.com, described eBay's privacy policy:

> "a repulsive confection of excessively broad disclaimers of liability coated in marketing sugar that deceitfully attempts to disguise the awfulness of its position."

Criticism and Correction

As in other areas of business, there are several ways that a smart company can use an outbreak of criticism over privacy to make friends and influence people. One option is to accept the criticism. That is what eBay did in March of 2002 when it backed off the change that had generated so much negative reaction. Although this response was not enough to satisfy many privacy advocates, one suspects that the average eBay user was favorably impressed: the company certainly appeared to be sensitive to privacy concerns. There will be more about handling such situations in Chapter 7.

Of course, avoiding criticism in the first place is usually the least costly option. Consider the case of DoubleClick, one of the

largest Internet advertising companies. In June of 1999, the company announced that it would acquire Abacus, a company that had accumulated large amounts of non-Internet information about people, referred to as off-line data (in this case, some 80 million households, profiled from direct mail catalogue purchases). Privacy advocates immediately expressed concern about the possible combining of the Abacus data with the online data that DoubleClick had been accumulating by tracking Web surfers through online advertisements. Concern had already been expressed over DoubleClick's "secret" tracking of Web users through cookies.

As a result of what can be construed as a failure to anticipate privacy policy criticism, DoublecCick has faced class action lawsuits, FTC investigations, and action by the Attorneys General from ten states. In August of 2002, DoubleClick agreed to pay $450,000 to settle with those states, and dramatically alter the way it operates, beginning with major changes to its privacy policies and notices (the settlement document in this case actually provides an excellent description of how DoubleClick's complex cookie system worked, as well as the mesaures with which the company now has to comply—see www.oag.state.ny.us for details).

Sensitive Data: Each new privacy case seems to expand the privacy language. The DoubleClick settlement with the states defines a "sensitive data" category that will probably play a role in future privacy cases. Sensitive data "includes but is not limited to data related to an individual's health or medical condition, sexual behavior or orientation, or detailed personal finances, information that appears to relate to children under 13, racial or ethnic origin, political opinions, religious or philosophical opinions or beliefs and trade union membership; PII obtained from individuals who were children under the age of 13 at the time of data collection; and PII otherwise protected under federal law (for example, cable subscriber information or video rental records)."

Like Eli Lilly, DoubleClick will have to live with the compliance guidelines for a number of years. In addition, the company must now provide privacy education, not only to own its employees, but also to the companies who use its services (these include some of the biggest names on the Web, including washingtonpost.com and CNN.com). Furthermore, as a result of the $1.8 million class action settlement, DoubleClick must conduct a public information cam-

paign consisting of 300 million banner ads that educate consumers on Internet privacy. Moreover, the company must retain an independent accounting firm to conduct an annual review regarding compliance with the settlement. (Note that this settlement was not tough enough for some privacy advocates, who are still seeking to have it overturned).

Consumer Costs

Clearly, companies can pay quite a price for a privacy breach, but what price does the consumer pay? Several cases of compromised credit cards have been mention in this chapter and it was pointed out that most consumers are not liable for fraudulent charges on compromised credit cards. However, it may be a mistake to look at the cost of a privacy breach to the consumer strictly in terms of money.

Aggravation

Companies should not underestimate the consumer aggravation factor of something like a credit card being compromised. For a start, these days an individual may have five or six monthly bills automatically paid by credit card. If the card has to be cancelled, all of those companies need to be contacted and provided with an alternative card or means of payment. If that is not done in time, bills can bounce and services can be interrupted. Perhaps even trickier are the annual subscriptions a person has placed on their cancelled credit card. These are easy to overlook when you sit down to deal with a compromised card. You don't have to loose any money in fraudulent charges for a cancelled card to cost you a lot of wasted time on hold, trying to mitigate the damage.

Identity Theft

A growing fear among consumers is that any of their personal data which is compromised will be the starting point for a identity thief. As was noted in Chapter 1, identity theft is a very real concern for consumers because it can create very real suffering, as well as create serious problems that require a lot of time and money to correct. To understand the connection between your Web site and the crime of

identity theft you first need to understand what an identity thief does. Here is a description used by the Federal Trade Commission, the agency charged with taking the lead on this issue:

> "An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name."

The problem is certainly on the increase. In 1999, the FTC created something called the Identity Theft Data Clearinghouse to try and get a clearer picture of the nature and prevalence of identity theft. In 2000, the first full year of operation, the agency entered more than 31,000 consumer complaints into the database. In 2001, that number grew to 86,168. As of the end of May, 2002, only five months into the calendar year, 55,000 complaints have already been added to the database. Here are some of the ways imposters can get personal information and take over someone's identity.

How identity thieves get your personal information:

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.
- They complete a "change of address form" to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for — and a legal right to — the information.
- They get your business or personnel records at work.
- They find personal information in your home.
- They use personal information you share on the Internet.

- They buy your personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services or credit.

How identity thieves use your personal information:

- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.

Loss of Privacy

Finally, it has to be said that many consumers see the main cost of a privacy breach as something very intangible and hard to define, yet very real: loss of personal privacy. Putting a price on personal privacy is not easy. I suspect that we have not yet seen anything like the upper limit on what a jury might award in a privacy case. What we have seen is a significant shift in perception. Consider the case of Ziff Davis Media, which settled a case with Attorneys General from several states in the summer of 2002, over what was originally reported, when it happened in 2001, as a security breach, but was later characterized as a privacy incident.

The New York Attorney General's office got involved after it was discovered that about 12,000 subscription orders were easily

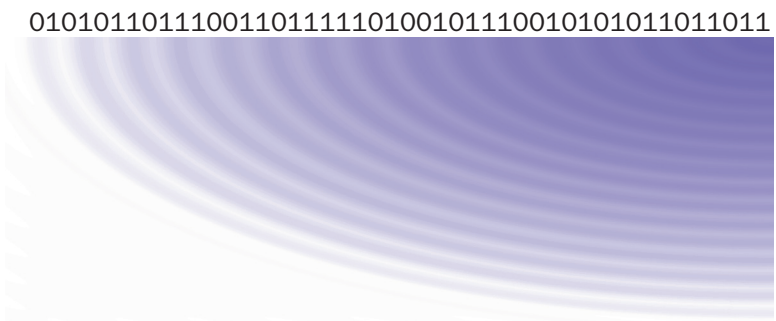
accessible on a Web site that the company used to accept orders for its magazines. For several days after a coding error was made, apparently during the execution of an internal marketing project, anyone on the Web who knew where to look was able to download a 1.3 megabyte text file of names, mailing addresses, email addresses and, in about fifty cases, credit card numbers. In the settlement, the company agreed to pay $500 to each of the approximately fifty U.S. consumers whose credit card data were exposed, regardless of whether they incurred fraudulent charges. The company also agree to implement new online privacy controls and pay the New York Department of Law $100,000 to be split among the states involved. New York's Attorney, General Eliot Spitzer, said the following in the settlement announcement:

> "The company's privacy policy promised reasonable security, but it was not effective in this case. With identity theft on the rise, consumers expect online businesses to recognize the sensitivity of personal contact and credit card information and to take reasonable measures to protect that information."

While the fines in this case might not sound like a lot of money, they establish a basis for further claims. When a company stipulates the facts in a settlement like this, even one in which they do not admit to breaking any laws, the groundwork is laid for other parties, such as someone whose identity was stolen as a result of the incident, to go to court.

Chapter Three

Web Privacy Principles



"The right to be left alone—the most comprehensive of rights, and the right most valued by a free people."

—Justice Louis Brandeis, Olmstead v. United States, 1928.