Save to disk [HELP]
Hide/Show menus

By David H. Holtzman

The Seven Principles of Privacy

Protect Your Customers' Privacy Ethically, Not Legally

There are two kinds of privacy: what you expect for yourself and what you're willing to extend to others. An ethical approach to privacy attempts to converge the two.

Privacy is one of those simple sounding words that each of us thinks we can define, but couldn't agree on if the correct answer would cure cancer. I wrote my book, *Privacy Lost: How Technology is Endangering Your Privacy* to show why it's impossible for legislators to protect our privacy because information technology moves much faster than the legal system. This makes it tough for business executives who have to formulate privacy policies in a legal vacuum—what criteria do you use to decide how to handle confidential customer information, where a misstep could cause a public relations nightmare resulting in resignations (maybe yours) and a depressed stock price?

It's quite fashionable for business executives to treat privacy problems like fires and privacy officers like insurance agents, ignoring them until it's cleanup time.

If the law cannot protect privacy, then the last person who should be in charge of formulating privacy policy should be a lawyer; yet in most firms, guess who the Chief Privacy Officer is, in the unlikely event that there actually is one? If you guessed “a lawyer?” you’d be right almost every time. Usually privacy falls into the domain of the company’s General Counsel (GC), where it’s out of sight. It’s quite fashionable for business executives to treat privacy problems like fires and privacy officers like insurance agents, ignoring them until it’s cleanup time.

The typical corporate approach to privacy is twofold: a vacuous CYA memo protecting the company (often referred to as a privacy policy) and internal documents written by the resident “Dr. No” listing prohibitions on data handling, generally reflecting the legal environment of the areas in which the company does business. Neither document affords any real protection for customers beyond the minimum. As enlightened management, you might want to do more than this bare-bones approach and be proactive towards privacy. But what can you use for guidance? The best strategy is to resort to an old-fashioned business approach—ethics.

I propose seven ethical principles for handling corporate privacy, based on the “seven privacy sins” explained in detail in my book.

Principle No. 1—Don't spy on me just because you can

Protect your employee's privacy. Modern technology has made it all too easy to spy on anyone, not just using cameras and microphones but also transactionally; by surreptitiously monitoring electronic communications, financial dealings and social activities. Our offices have become electronic junkyards scattered with remnants of old communication; it's no accident that prosecutors of financial scandals have increasingly relied on electronic evidence to gain convictions. Not only is there too much information available in the workplace, but also there are virtually no strictures on using the data. When it comes to privacy, workers are the worst protected class of user in America. Legal protection for workplace privacy is so weak and the gap between what can be technically obtained and what is prohibited is so wide, that most companies have too much information on their employees lying around. This data cannot only be misused internally, but is available for subpoena by government investigators or as evidence in a lawsuit. For all these reasons, take a stand and prohibit routine spying on employee communications.

It's difficult to get workers to protect customer privacy when they have none of their own.

Principle No. 2—Thou shall erase my data

Data lasts forever, yet very few companies have data erasure policies. The trend has actually been in the opposite direction; the government has been toying with the idea of requiring service companies to retain customer information indefinitely. It's always cheaper to buy hard drives than pay for the labor to figure out what is safe to delete—thus ensuring that data centers will continue to fill up with old, unwanted, yet potentially dangerous information. I say "dangerous", because old information not only threatens your customers' privacy, but also becomes a target for litigious vultures, who for the cost of a routine subpoena, can pick at your electronic bones. Avoid future grief and put policies in place requiring complete data destruction of customer information at the earliest possible opportunity. Sure, it's tempting to hold onto customer information for marketing purposes, but if you have it, sooner or later you'll use it. Or worse it'll get subpoenaed—either by the government or by private attorneys.

Don't keep data any longer than you have to; you can't give up what you don't have.

Principle No. 3—Keep my information to thyself

Don’t give away consumer information to other business groups, either inside or outside the company. The ethical rule of thumb is to only use a customer’s personal data in the way that they had understood that it would be used when they volunteered the information in the first place. Many businesses split hairs by saying that they will only give information to “strategic partners” or “third party consultants”. This organizational distinction is completely irrelevant to the person who’s being spammed. Other companies use the artificial contrivance of corporate ownership to justify exchanging consumer information freely between different legal entities of a parent company. Lawyers are comfortable with this distinction, but users are not. It seems bizarre that a coupon submitted for free Kraft Macaroni & Cheese could somehow result in an offer for a carton of Marlboros, but it could happen because they’re owned by the same company. American businesses have been playing fast and loose with private information for decades now, using weasel–worded privacy policies to effectively create “opt–never” programs, where accounts information is traded around like fungus at a nudist colony.

Require customers to opt-in for each additional use of their information.

Principle No. 4—Don't judge me

Don't rely too much on smart software that automagically categorizes your customers. One of the most useful, yet insidious artifacts of the Information Age is data profiling. These artificial intelligence systems can sift through huge piles of transactions, spotting patterns and trends using rules-based reasoning. These systems are a cheap and efficient way to process a lot of electronic information, but if not handled properly, can become the mindless voice of authority in a company. An AI-driven software approach can create a customer service nightmare where employees mindlessly defer to the automated opinions, ignoring their own common sense. Even worse, it's easy to forget that profiling systems are only as good as their rules. Bad programming yields stupid, incorrect and damaging conclusions, which can become a permanent part of an account file. Usually these are descriptive labels, often useful for segmentation, but sometimes they can be pejorative or unflattering. For instance, it would be simple for a grocery store to analyze information gleaned from the store's checkout courtesy card and create a customer category called fatty, referring to people that buy an excessive amount of sweets. Yet doing so would brand those people in an unflattering way, possibly even reaching beyond the store if the information was ever sold or shared with another firm.

Never create a profiling system that labels your customers in a way that you'd have trouble justifying if they ever saw their file, because some day they probably will.

Principle No. 5—Protect my data like it were thine own

Most consumer privacy problems aren't caused by deliberate misuse but from neglectful handling. Electronic privacy is inherently dependent on computer security. Corporate America uses computers in every possible way, yet new data processing capabilities don't come with better ways to protect the information. If anything, it's the opposite: business environments are so saturated with sensitive data, that the information is often handled cavalierly, often negligently. A single DVD can hold the credit card information for all 300 million Americans, yet the disk looks innocent enough that it's left casually lying around. There have been too many cases lately of government workers taking home computers loaded with sensitive information—data that could negatively affect millions of people. It's a good idea to annually reevaluate your data handling policy assuming the worst case—laptops will be lost, networks will be penetrated, computers will be hacked and backup tapes will be misplaced. Good customer relation management needs good privacy policies. Good privacy procedures require great computer security. Every row in a marketing database is a potentially irritated customer in the event of a data breach. Of course, it could be worse because conventional wisdom says that every dissatisfied customer tells six more. It could even be a lot worse if there's a class action lawsuit. PR damage control and legal defense is always more expensive than good computer security.

Provide the best computer security that you can afford.

Principle No. 6—I am who I say I am

Accept pseudonymous identities whenever possible. The online world is developing its own rules of behavior including customs, protocols, etiquettes and morality. Many businesses are trying to insinuate their products into cyberspace because they want to sell to the lucrative 18–35 year old male who spends a lot of time there. If you're planning on selling into that demographic, respect the culture. One concept that most conventional marketing people haven't gotten yet is that identity on the Internet is not an absolute, but relative to the environment. Most Net denizens maintain multiple identities, sometimes because they had to pick an unused logon id, or they wanted some distance from their real–world profession or just because they wanted to. If you are dealing with an online community that uses aliases like this, respect their pseudonymity. Unless you need to take credit card information, don't attempt to find out their real name and information, but accept what they give you. A less intuitive rule is to use whatever demographic information that a respondent gives you, even if you think it's wrong. For instance, a 55 year old white male that identifies himself as a 25 year old Asian female is not lying, because he's planning on acting that way and will almost certainly spend his money that way. So why do you care what he "really" is?

Let your customers pick their own demographics.

Principle No. 7—Don't humiliate me

The most important privacy consideration is often the most neglected—preservation of human dignity. All the marketing hype about "customer intimacy" and building "online communities" is just lip service when customer relationship management is a kind of software system, not a management strategy. The more that you lose sight of the person behind the data record, the more likely it is that you will cause embarrassment through inappropriate usage of information. For instance, several years ago, Eli Lilly inadvertently cross-copied 700 people on a Prozac mailing list, exposing their true identities to each other. More recently AOL posted three months of search log information from their user base. Even though they "anonymized" the data, it was relatively simple to identify several people by clues contained in the searches. The idea that hundreds of thousands of their members might have been embarrassed should have raised the bar on internal data handling—sensitive customer information (which includes web searches) should always be treated like gold.

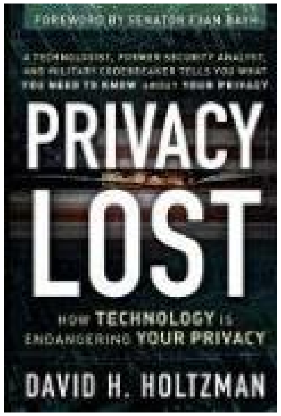
Avoid embarrassing your customers by mishandling their data.

Laws make poor privacy guidelines. Business people need better directions when navigating their customer relationships than simply to be told to steer around legal roadblocks. Boardroom discussions should be less about what is permissible and prohibited and more about what is positive and proactive—in short, what is ethical. The question should not be "Can we do this?" but "Should we do this?" "What's the right thing to do?" If your company handles the electronic representation of the customer the way that they'd deal with them if they were standing face-to-face, you'll do fine. Create an environment where your employees have the flexibility to treat your customers well, unhampered by either the dogma of the lawyers or the tyranny of computers.

It's hard to expect senior management to do this on their initiative. Most P&L bosses are held to such tight financial metrics that it would be naïve to not expect them to opt for any decision that is lucrative, even if ethically dubious. This situation is what causes marketing groups to wring every drop of privacy out of consumer information, by upselling and cross-selling, and if all else fails, selling the whole customer to another company.

Privacy policies should read like mission statements, empowering employees to do reasonable things with sensitive customer information and holding them and their supervisors accountable when they don't. As the world becomes a truly global economy, ethically sound privacy policies are a universally correct way to achieve the necessary managerial balance between legitimate marketing and customer protection.

info


FOREWORD BY SENATOR EVAN BAYH
A TECHNOLOGIST, FORMER SECURITY ANALYST, AND MILITARY CODEBREAKER TELLS YOU WHAT YOU NEED TO KNOW ABOUT YOUR PRIVACY
PRIVACY
LOST
HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY
DAVID H. HOLTZMAN

BUY THE BOOK
For more details or to buy a copy of David H. Holtzman's, *Privacy Lost: How Technology is Endangering Your Privacy* click here.

ABOUT THE AUTHOR
During the dot com boom of the late 1990s, David Holtzman ran one of the most critical networks in the world—the domain name system. As Chief Technology Officer of Network Solutions and the manager of the Internet's master root server, he oversaw the growth of the commercial Internet from five hundred thousand to over twenty million domain names. Mr. Holtzman has designed and built numerous information-based software systems and is the author of several major patents. He has consulted on marketing strategy for several large corporations, including Amazon.com. He has been a security consultant for several organizations, private and public, including Wesley Clark's 2004 presidential campaign. He has been an advisor to over a dozen high-tech companies throughout North America.

In addition to being the author of the recently released *Privacy Lost: How Technology is Endangering Your Privacy* (Jossey-Bass, 2006) and consulting, Mr. Holtzman is currently the president of GlobalPOV, a firm he founded to explore significant technology issues and their effects on society. He has been interviewed by major news media including the New York Times, CNN, and USA Today. Holtzman wrote a monthly ethics and privacy column called "Flashpoint" for *CSO* [Chief Security Officer] *Magazine,* and his essays have been published in *BusinessWeek, Wired Magazine, CNET,* and *ZDNet.* Holtzman publishes daily on topics such as privacy, intellectual property, business, and pop culture on his blog, www.globalpov.com.

Holtzman has a B.S. in Computer Science from the University of Maryland and a B.A. in Philosophy from the University of Pittsburgh. He is the father of five children, whom he raised as a single parent. He likes to sail, watch Shakespearean plays, and cook.

LAST PAGE READ | MORE →

info

DOWNLOAD THIS

This manifesto is available from http://changethis.com/28.02.PrinciplesPrivacy

SEND THIS

Click here to pass along a copy of this manifesto to others.
http://changethis.com/28.02.PrinciplesPrivacy/email

SUBSCRIBE

Learn about our latest manifestos as soon as they are available. Sign up for our free newsletter and be notified by email. http://changethis.com/subscribe

LAST PAGE READ | MORE →

info

WHAT YOU CAN DO

You are given the unlimited right to print this manifesto and to distribute it electronically (via email, your website, or any other means). You can print out pages and put them in your favorite coffee shop's windows or your doctor's waiting room. You can transcribe the author's words onto the sidewalk, or you can hand out copies to everyone you meet. You may not alter this manifesto in any way, though, and you may not charge for it.

NAVIGATION & USER TIPS

Move around this manifesto by using your keyboard arrow keys or click on the right arrow (→) for the next page and the left arrow (←). To send this by email, just click on. ✉

HAVING PROBLEMS SAVING TO DISK?

First, make sure you have the latest version of Acrobat Reader 6 which you can download from http://www.adobe.com/products/acrobat/readstep2.html. If problems persist, it may be due to your Acrobat Reader settings. To correct the problem (for Windows), a reader, J. Hansen, suggests going to your Acrobat Reader Preferences > Options > Web browser Options. Check the "Display PDF in Browser" option. Then click on Save to Disk. 💾

KEYBOARD SHORTCUTS	PC	MAC
Zoom in (Larger view)	[ctl] [+]	[#] [+]
Zoom out	[ctl] [—]	[#] [—]
Full screen/Normal screen view	[ctl] [L]	[#] [L]

↶ LAST PAGE READ | MORE →

info

BORN ON DATE

This document was created on November 6, 2006 and is based on the best information available at that time. To check for updates, please click here to visit http://changethis.com/28.02.PrinciplesPrivacy.

COPYRIGHT INFO

Cover image from www.istockphoto.com

ABOUT CHANGETHIS

ChangeThis is a vehicle, not a publisher. We make it easy for big ideas to spread. While the authors we work with are responsible for their own work, they don't necessarily agree with everything available in ChangeThis format. But you knew that already.

ChangeThis is supported by the love and tender care of 800-CEO-READ. Visit us at our main site www.800ceoread.com or at our daily blog http://800ceoread.com/blog/.

LAST PAGE READ