Privacy Policy

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. ... They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

—Louis Brandeis, dissenting, *Olmstead v. U.S.*

As soon as your site asks my name, I get suspicious. Then if you ask for my address, phone number, credit card number, bank names, account numbers, health history, or current job info, I worry about what you are going to do with that information, and I am likely to nudge legislators around the world to order you to protect my privacy.

If your site mines raw transaction data to identify me, to come up with new offers, to sell my name to eager merchandisers, or to run a more sinister scam, you are going to have to explain how you "share" that information within your own family of companies and outside, or else you will be hearing from the lawyers.

How can you avoid lawsuits and reassure your guests?

Go ahead, reassure me

Two thirds of Internet users are willing to accept a guarantee that you won't abuse their privacy. "We guarantee that we will not violate your privacy." Just the statement is enough—very few of these folks actually read privacy policies.

Of course, about a quarter of the Web population feel extremely nervous about the way their personal information might be used, and these folks are not likely to be placated with a simple statement.

For the rest of the Web world, though, assertions are often good enough. Put a link to your privacy policy on every page, and make a big deal out of going to your secure server when a customer makes that leap, and, whenever you ask someone to fill in a form, put your guarantee right up there.

Does this strategy make you feel a little anxious as a writer? You might want to make sure that your company really will protect the consumer's privacy before you scribble the announcement. An interesting way to probe your organization's honesty would be to volunteer to write an in-depth explanation of their privacy policy.

Your boss's reaction will tell you more than the policy does.

Reward me for exposing myself

If your firm really needs my personal information, give me a reason to take the risk—and the time. Almost two thirds of the folks out on the Internet have parted with their e-mail address and "real" name in order to get access to a site's content, special e-mail newsletters, affinity points on purchases (such as frequent flyer miles), or a chance to enter a sweepstakes. If you offer the opportunity to personalize the site, most say they will give you their real name for that convenience.

People swap info for benefits. So write up the benefits on the page on which you are asking folks to respond to a question, complete a form, or opt into an e-mail.

Let me out

All we ask is to be let alone.
—Jefferson Davis, Inaugural, 1861

Give me access to my personal profile or account, and let me delete myself. If you give people the opportunity to edit their information, oddly, they provide even more. Almost no one destroys his or her data.

So as soon as you display the personal information, write labels indicating how they can edit it and resubmit.

Since one of the biggest invasions of privacy is spam, make sure that you allow people to opt into your e-mail newsletter twice (once by clicking the checkbox and Submit button, again by responding to the e-mail notification that they can subscribe if they reply). **Double opt in** makes it more likely that people know what they are doing when they volunteer for the e-mail. But let them unsubscribe, and write clear directions for that in every issue. You really don't want to end up testifying in front of some group like the U.S. Federal Trade Commission on something they call UCE—"unsolicited commercial e-mail."

Write a privacy policy that people can understand

Unfortunately, most privacy policies are written by lawyers, with headlines inserted by marketing veeps. The tone is schizophrenic. The big type says, "We would never tell," and the fine print inserts

exceptions, excuses, and bland generalities that leave anyone wondering, "Are they sincere?"

Avoid the "We-we's." *We* do this, *we* do that, but what about the user? "We use advanced technology and well-defined employee practices to help ensure that customer data is processed promptly, accurately and completely," says American Express. Thank goodness. American Express feels much better now, but I don't. Those employee practices, in particular, give me an eerie feeling that something isn't being told; for instance, why aren't those practices actually spelled out here, if they are so well defined, and what difference do they actually make to me?

The free state offers what a police state denies—the privacy of the home, the dignity and peace of mind of the individual. That precious right to be let alone is violated once the police enter our conversation.

—William O. Douglas, Address, American Law Institute

Stop boasting. Politically, you may have a hard time getting rid of bogus phrases like:

- "Our policy is simple."
- "The security of your personal information is of the utmost importance to us."
- "We are in the forefront of the critical issue of privacy."

But make the effort. A ten-page legal document is not simple. Making money is probably more important than privacy. So don't make bogus claims, or you vitiate the whole purpose of the policy, which is to build trust.

Don't pontificate. Guests don't think of you as a philosophy professor, so edit the heck out of the boss's reflections on subjects like "consistent service quality." In fact, try not to sound like the boss. The managerial perspective seems alien to most customers, even when couched in "you" phrases. Take this sentence describing one of the "key values" of Bank One's privacy policy:

> Information must be shared to fulfill your requests, deliver products and services, administer and update accounts, reduce fraud and other risks, and to comply with laws and regulations.

True, but here we are looking at things with the eyes of an Information Technology Officer, or CIO, not a consumer.

Also, watch out for grandiose phrases reflecting defensiveness (why we are forced to collect information about you), self-pity

(the darn law makes us tell you these things), or just managerial duplicity (we reserve the right to sell your information anytime we feel like it, but we can't admit that). Lying, of course, is the biggest stylistic problem in privacy policies, and one reason so many people distrust these otherwise bland and boring documents. As a mere writer you can only do so much to force your organization to be honest with consumers. But give it a shot. And if you get a lot of jive talk back, maybe you should pull out your resume for a little update.

Lead up to the jargon, or ax it. Too often the authors of privacy policies assume that the readers know acronyms like SSL, understand the subtle differences between internal and external sharing and selling, and enjoy hearing about encryption standards. Using industry or in-house jargon without explanation simply makes readers suspect that you are trying to pull the wool over their eyes. Sure, you may have to talk about your security precautions, but walk people through these safeguards in plain English before you mention IP addresses. Remember, a lot of people still think cookies are a great snack.

Phrase the policy as a FAQ. People are used to this organization on the Web, and it breaks the information up into digestible chunks, in the give and take of a virtual conversation. Answer questions like these:

- Why do you want to know my name and e-mail address?
- Why do you want to know my credit card number and street address?
- What other information do you track about me?
- Do you collect information from children?
- How do you verify parental consent for information about their children?
- How do you make sure nobody steals my credit card information?
- How do you use this information?
- Do you share my information with other parts of your company?
- Do you share my information with other companies?
- Do you sell my information to anyone?
- What do you do if one of your employees violates my privacy?

- Can I see and change the information you have about me, personally? Can I review information you have about my child?
- How can I start or stop receiving e-mail from you?
- How do you protect the privacy of my e-mails to your customer support team?
- Where can I learn more about my right to privacy?
- Who can I talk to if I have a question about my privacy?

If you can answer most of these questions in a paragraph or two of plain English, you will surprise and please most consumers, even if your legal team has a fit. If you must defend yourself against your own firm's lawyers, do some user testing to show what people understand, and what they don't, in their prose and yours. Then make the case that the document claims to be addressed to the general public, not just lawyers, and so the norms, conventions, and standards of ordinary people are what the text must be judged by—not the stricter, but slippery language that is legally correct.

Explain security before and during the transaction

Don't just dash off a little paean to security in your general FAQ. Explain what makes your server secure, and why that matters to me, as a consumer—before I have to enter my credit card number, and inside any forms I have to fill out to complete the buy.

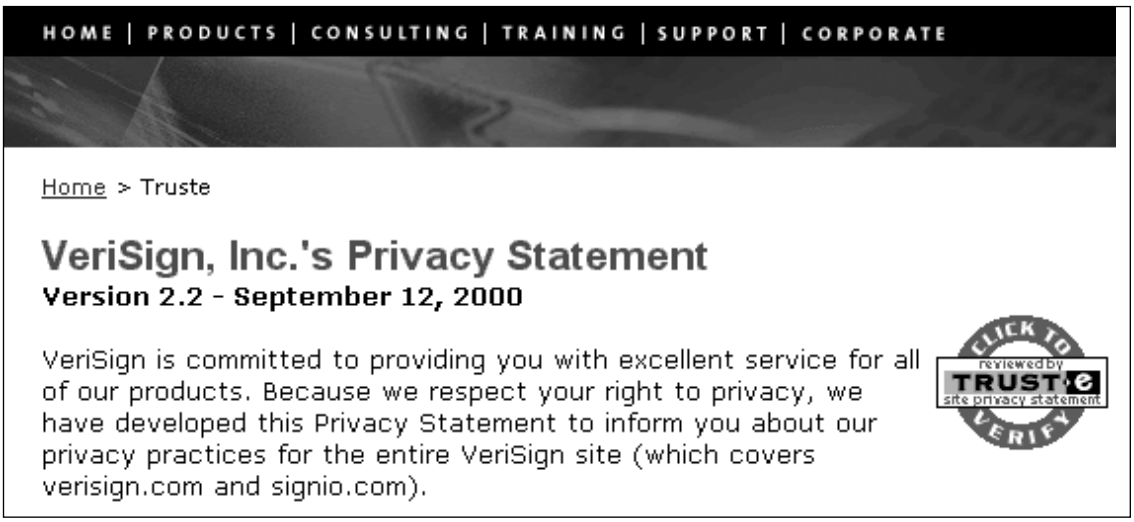
Point out how your consumers can tell if they are really on a secure server (the change in the URL, the icons that show up on the status bar). In other words, tell people what you take for granted, as obvious, about security. Say more than you think is really needed, and folks will be grateful.

Not too techie, please. Take a shot at explaining encryption, and the Secure Sockets Layer, if you dare. But concentrate on the benefits to the consumer. Most online transactions are safer than a trip to the local dry cleaner (where they keep a paper copy of your information), and a lot safer than e-mail. But trying to explain this fact can be a challenge, particularly when you are really just writing a label on a form.

Sure, you can link to a fuller explanation in the FAQ or Privacy Policy, but make a solid effort to capture the gist of those ideas at the moment of action, so most people don't have to leave the page to learn what is going on.

See: Agre and Rotenberg (1997), American Civil Liberties Union (2000), American Express (2001), Bank One (2001), Davies (2001), Federal Trade Commission (1999), Gilbert (2001), Givens (2000), MasterCard (2001), Porter (1987), Price and Price (1999), Rotenberg (2000), Visa (2001).

Case Study: Privacy Policy at VeriSign



VeriSign, a company that issues and manages certificates of authenticity for software, Web sites, and even individual documents, is in the business of trust, so they have developed an elaborate privacy statement, following the guidelines of another organization, Truste Privacy Program, which places its seal on sites that agree to follow its rules (and pay a licensing fee). So the VeriSign privacy policy sounds a lot like the policies on other TRUSTe-endorsed sites, but the VeriSign lawyers have added their own special edits. Printed out, the statement takes up eight pages, with seven major headings, and 13 subheads—and 37 very long paragraphs in between.

The team of lawyers start out with an impassioned appeal:

> Because we respect your right to privacy, we have developed this Privacy Statement to inform you about our privacy practices for the entire VeriSign site (which covers verisign.com and signio.com).

The parenthetical comment adds a lawyerly touch. This page exists on the VeriSign site, and its URL begins www.verisign.com. I have never heard of this other site devoted to signio.com. The editorial insertion (in the interests of complete accuracy and legal precision) dilutes the force of the original sentence.

And that's the way a lot of the text goes. Earnest beginnings trail off into legal or technical jargon. Repetitions, acronyms, passive verbs, and weasel words make the prose seem to frown like a judge:

> With respect to VeriSign's Public Certification Services, the VeriSign Certification Practice Statement ("CPS") presents the practices that VeriSign and our affiliates, subscribers, customers, and relying parties follow in issuing, managing, and using certificates and in maintaining a certificate-based public key infrastructure and related trust services. The CPS is intended to legally bind and to provide notice to all parties that create and use certificates within the context of VeriSign's Public Certification Services.

Surely, this kind of talk is aimed at lawyers, not consumers. And, sure enough, in another tangled paragraph, the writers admit that this privacy statement only covers "non-Public Certification Services" for "our site visitors and subscribers." Of course, ordinary visitors like us have no idea what the difference might be. We saw their certification on a public site, so is that covered by this other document, the famous CPS? Who knows? The lawyers forgot to tell us outsiders. But we can tell they have definitely covered their ass.

Getting past the lyric outbursts ("Privacy is of great concern to most users of the Internet and is a critical part of an enjoyable and satisfactory user experience,") and wading through the legalisms, we do discover a few phrases that sound like one person talking to another, albeit a little coldly:

> "...we do not collect personal information from you unless you provide it to us."

> "We use links throughout our site to provide you with the opportunity to contact us via e-mail to ask questions, request information and materials, or provide comments and suggestions."
>
> "When you visit our site, our computers may automatically collect statistics on your visit."

The tendency to cover the waterfront (like telling us all the reasons we might ask them to e-mail us) stems from the merging of the legal and the technical mind—both of which hate half thoughts, incomplete statements, and partial truths. So this document is thorough enough to intimidate anyone who might just wonder whether VeriSign was passing along personal information to its licensees. (The answer is yes, but the third parties must sign a confidentiality agreement.) The sentences go long, the lines extend far across the page, and the paragraphs extend to a dozen or more lines. The phrases that answer key questions lie deep within those nests, almost inaccessible to the average reader.

Fortunately, the statement includes the street address, if you care to use snail mail. Ironically, the only e-mail address I could find is for customer support for people who have already purchased something called a Digital ID. The rest of us will just have to put our questions on paper, rummage up a stamp and envelope, put the address on there, and carry our little letter out to the mailbox. Hey, we should hear back within a month or two.

The company seems reliable, even valuable, but the privacy statement is written by and for lawyers and engineers, not the "visitors and subscribers" they claim to be committed to. I get the feeling this statement will work well in court. And, if the aim is to baffle ordinary consumers, keeping the real practices a commercial secret, the statement succeeds. It keeps the policy private.