"HELLO, WE'RE FROM THE F.T.C. AND WE'RE HERE TO HELP." THE TOP 5 PRIVACY POLICY MISTAKES COMPANIES MAKE

By: Daniel A. Batterman, Esq.

While many companies have privacy policies posted on their websites, few realize the impact of policies that have not been carefully drafted or the consequences of not following them. Privacy policies have little value unless there are strong enforcement efforts. This is why the Federal Trade Commission ("FTC") and the Attorneys General from many states have been active in bringing suits against companies that have engaged in privacy practices which are regarded as "unfair" or "deceptive," a common legal standard in the consumer protection arena.

In addition to the unwelcome scrutiny that government enforcement actions bring, a company also risks negative publicity, loss of customer confidence, and lost revenue. And given the almost daily parade of privacy breaches in the media, the public is very aware of these issues. It's therefore a good idea to stay off of the government's radar, and the best way to do this is to make sure that your company's privacy policy and practices are carefully developed and implemented. Listed below are the most common mistakes I've found that companies make in this area. Make sure your company is avoiding these five big ones.

1. Pulling a Fast One. There's no quicker way to get into trouble with both federal and state authorities than promising to do one thing with people's data and then doing another. It's imperative that your company actually follow its own privacy policy. It doesn't matter whether users actually read it or not. The statements in the policy bind your company to do what it says it's going to do.

If your policy states that it will never sell, license, or disclose any personally identifiable information and you do it anyway, you're playing with fire. And you're fooling yourself if you think no one will find out. In March of 2006, the New York Attorney General sued Gratis Internet, a company which operates several marketing websites, for disseminating customers' personal data after promising that it would never do so. The case is pending (although Datran Media, which purchased this information with knowledge that it was disclosed in violation of Gratis's privacy policy, settled with the state for $1.1 million).

In March of 2005, the FTC settled a case against Vision I Properties, LLC. Vision I was a third party provider of shopping cart software to on-line merchants who had privacy policies which promised their customers that personal data wouldn't be disclosed. Vision I, which knew about the policies, "rented" the personal information of almost one million people, including their names, addresses, e-mails, and credit cards. The settlement (called a "consent decree") prohibited Vision I from using the information, barred misrepresentations about the collection and use of personal data, and required disgorgement of the money it made. The consent decree is in effect for 20 years, which is typical once the FTC becomes involved. Be prepared for long term involvement. And once any agency gets involved, others are never far behind.

2. "Oops, Did I Forget to Mention . . ." Failing to disclose all the ways your company collects data from users is another red flag. Information-gathering is generally grouped into two categories: Active and passive. Active techniques include asking for data in response to prompts, such as on a registration form. This is straightforward. A person knows exactly what information you're asking for and voluntarily provides it. If a person doesn't provide it, the site may not allow the user to access the site or all of its features.

Passive collection of information occurs when a user doesn't have to take any affirmative steps. In other words, it happens automatically, often without the user's knowledge. These include the use of Internet

Protocol ("IP") addresses, Globally Unique Identifiers ("GUID"), cookies, internet tags, or other methods. All of these should be disclosed in your company's privacy policy, especially if passive gathering techniques are combined with a user's personally identifiable information (but even if they're not). If you have nothing to hide, you might as well say so. You may not have much of a choice anyway as laws are passed requiring notice to users of passive data-gathering techniques.

If your policy also fails to inform users that software is being installed on their computers—like spyware, for example—then you will almost certainly be inviting close scrutiny from authorities, and possibly from law enforcement as well. Indeed, this practice is illegal in states such as Utah, California, and many others. It just isn't worth it. And people will find out. The media loves to expose companies which are engaging in questionable practices. Indeed, there are numerous watchdog groups which make it their mission to do so. Given the headlines that privacy is garnering these days, it's best to keep a low profile.

3. The Left and Right Hands. Do you know what's really contained in the many agreements that may be posted on your company's site? Depending upon the type of business your company is in, it's not the least bit unusual to have multiple agreements on your site, including user agreements, acceptable use statements, support policies, and privacy policies. These agreements commonly touch upon the subject matter of other agreements. But do they contradict each other?

Consistency is key. I've seen privacy policies which state one thing, but user policies which say another. Also, make sure that all other places on your site where applicable content appears doesn't contradict what's written elsewhere. For example, many companies also address privacy issues in the "FAQ" sections of their sites. Make sure answers to FAQs are reviewed carefully prior to posting. They should not deviate from what's written in the privacy policy or add any new information. Keep it simple.

Such inconsistencies could be unfair or deceptive. For example, if a site's user agreement allows for the sharing of personal information, but the privacy policy doesn't, this will get the FTC's attention. Inconsistencies like this are easy for it to pursue. In addition, any resulting settlement will likely require the company not to disseminate any information in violation of the privacy policy, even if other statements on the site provide otherwise. As far as the FTC is concerned, the company made representations that it would not disclose this information regardless of other contrary statements. When this type of ambiguity exists, it's construed against the drafter, which is the company.

Also, while we're on the subject, be sure to limit the scope of your policy to the on-line world. Policies which fail to do so could be deemed by the FTC to apply to all of the company's privacy practices, whether on-line or off. This can result in significant headaches for a company that is unprepared to take every piece of data about its customers (and even its employees) and subject all of it to rigorous privacy standards. Let users know that the policy applies to on-line information only and that data gathered elsewhere is excluded.

4. "Once upon a time . . . ." Marketing to children is big business nowadays. Whether it's soda, movies, video games, or clothing, children are now considered to be fair game. And given how computer-savvy kids are these days, companies can reach them whenever they sit in front of a computer—which is pretty much every day, several times a day.

In a strong showing of solidarity, the government passed the Children's On-Line Privacy Protection Act ("COPPA"). This is a federal law which regulates the collection of personal information from children under the age of 13 by operators of commercial websites. COPPA imposes a number of requirements on websites, including the posting of clear and comprehensive privacy policies, obtaining "verifiable parental consent" before collecting data, and providing parental access to children's personal information. Failure to comply with COPPA could expose your company to close FTC scrutiny and significant financial liability.

Even if your company doesn't direct its marketing efforts to children, don't assume that COPPA doesn't apply. There could be many hidden issues that require you to "childproof" your site. If, for example,

you use on-line forms to gather information and ask for ages or birth dates, does your site then prevent further collection of personal data if the user responds that he/she is younger than 13? If not, then under COPPA this qualifies your company as having "actual knowledge" that it's collecting information from children and could expose you to liability. Even if you don't ask for this, asking for a school, grade level, or other data that could be used to easily ascertain a person's age could also be problematic. Keep in mind that your company doesn't have to do anything with this information to be liable. It only has to collect it.

The type of content posted on your site can also raise concerns. Even if your company doesn't target children, the subject matter, language, layout, and graphics on the site may attract them anyway. For example, liberal use of animated characters, bright colors, and child-like fonts may be appealing to kids. In addition, if your company sells advertising on its site to other businesses that actively target children (such as toy companies), this can be another factor that the FTC takes into consideration when deciding if COPPA has been violated. Remember, the FTC has broad discretion when making these decisions.

5. <u>Promising the World.</u> Far too many privacy policies make sweeping and unrealistic pronouncements about how users' data will be treated. These policies have to be worded carefully and must take into consideration a company's actual business model, the industry it's in (which may be regulated), and the public relations issues that arise from gathering personal information.

If you haven't thought through these considerations carefully, it's easy to make statements about how your company will never sell, license, or disseminate its customers' information to anyone else for any reason. Indeed, you may never want to disclose data that may end up in a competitor's hands. But there's also a possibility that this information could be valuable to other companies which are willing to pay a great deal for it. Whether your company does this is a business decision. If, however, your privacy policy prohibits it, it's a moot point anyway, as self-imposed restrictions create binding obligations.

Consider the sweeping language taken from an actual policy found on a Massachusetts state website. It provides an excellent example of what <u>not</u> to do in any context, whether commercial or not:

> *<u>A Privacy Partnership</u>. Your privacy with respect to the use of the Mass.Gov Portal results from a partnership between the Commonwealth and you, the user. At this Web site, we attempt to protect your privacy to the maximum extent possible. However, because some of the information that we receive through this Web site is subject to [public disclosure laws], we cannot ensure absolute privacy. . . .*

Besides being poorly worded, language like this can get a company into trouble. First, consider the word, "partnership." This is a word I avoid except where an actual partnership exists. Partners have "fiduciary duties" to each other, which means that they must act with the utmost honesty in their dealings. Duties such as these are easy to breach. While I'm not suggesting that a court may find such a relationship here, why even invite the inquiry? Companies don't "partner" with their customers—they sell to them. Don't make the relationship more than it is. It's best to avoid terminology that in the hands of a tenacious lawyer may end up imposing far greater obligations on the company than was ever intended.

Much more problematic is the language: "At this web site, we attempt to protect your privacy to the maximum extent possible." This can be very problematic. What does the "maximum extent possible" mean? It means that your company isn't just taking "reasonable efforts" (a common legal standard), but that it's making efforts beyond what's customary. If your company is encrypting data, is it using the most secure encryption commercially available? Using encryption that could be easily compromised by a bored 16 year old would not be meeting this standard. Neither would allowing most employees access to customer information. The point is this: Watch these sorts of sweeping statements. The scrutiny that could follow may very well uncover major shortcomings in your privacy practices.

In another portion of the policy, it reads: "Your privacy is one of our top priorities." This could be problematic as well. What does it mean to make privacy a "top priority?" Spending a great deal of money on it? Constantly upgrading security? Hiring a Chief Privacy Officer? Who knows? It certainly implies,

however, going above and beyond what another organization may be doing that doesn't regard privacy as its "top priority." From the FTC's perspective, it could be unfair or deceptive to tell your customers that their privacy is a "top priority" when the company is making only minimal efforts to protect it.

Petco Animal Supplies, Inc. learned this lesson firsthand. It settled charges with the FTC after it made claims on its website such as: "At PETCO.com, protecting your information is our number one priority, and your personal information is strictly shielded from unauthorized access." The FTC alleged that Petco's site was vulnerable to common web-based attacks (*i.e.*, SQL injection attacks) which disclosed customers' personal data. The case settled. In short, the words in your policy mean something and may have a much broader effect than intended. Make sure they mean what you want them to. At least the Massachusetts site is clear about not ensuring "absolute privacy." This would be foolish to do, especially when the government and other authorized parties can obtain this information anyway.

As the Mass.gov site is run by the state, it's not on the FTC's radar. However, I've seen many companies put together their privacy policies by "cutting and pasting" language from policies like the Mass.gov one. While this may save money initially, these savings will mean little if the government ever targets your business. The FTC may be there to help, but it's not there to help you. Its job is to protect the public. And once the government becomes involved, be prepared for the joy of dealing with determined bureaucrats in a cumbersome administrative process. Or better yet: Litigation. But that's a different article.

The Law Offices of Daniel A. Batterman
Old City Hall
45 School Street, 3rd Floor
Boston, MA 02108
617.259.1600
DBatterman@BattermanLaw.com