;login:

THE MAGAZINE OF USENIX & SAGE

April 2002 • Volume 27 • Number 2

inside:

THE WORKPLACE

Data Privacy

BY JOHN NICHOLSON

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

data privacy

Life Just keeps Getting More Complicated

by John Nicholson

John Nicholson is an attorney in the Technology Group of the firm of Shaw Pittman in Washington, D.C. He focuses on technology outsourcing, application development and system implementation.

John.Nicholson@ShawPittman.com

Not too long ago, the public started worrying about "privacy" related to the Internet.[1] They weren't really sure what it meant, or how it differed from privacy in the real world, but they had an opinion, anyway.

Sensing an opportunity/need for regulation, governments started getting involved. The US government enacted laws like the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), and the European Union implemented its own Privacy Directive.

Over time, companies also put up "privacy policies" on their Web sites. Sometimes these policies were written by lawyers, sometimes by a marketing intern, and sometimes they were just copied from another Web site. Frequently, they were posted and ignored by the business itself. Surprisingly, however, a large number of companies do not yet have a privacy policy. The purpose of this article is to discuss what should be in a privacy policy and to discuss some of the recent developments in privacy regulation that will make your life more complicated.

Privacy Basics

The essence of data privacy involves four fundamental principles: notice, choice, access, and security. If your company doesn't already have a privacy policy, it should develop one that is accessible from your home page (preferably with a clear and easily identified link on your home page and also on each page where users can provide information to you). The purpose of this section is to provide examples of the type of language that should (and, occasionally, should not) be in your privacy policy.

Privacy Policy Part 1

Companies frequently like to include some type of introduction in their privacy policy, and this is the first place where you can get yourself into trouble. For example, one Web site opens its privacy policy with the following:

"We will ensure that our relationship is as exclusive as you want it to be."

This is a fairly sweeping statement and is the kind of language that marketing executives use to give their lawyers high blood pressure. From a legal perspective, "ensuring" something is a very high standard, especially when what you have promised to "ensure" is that you will comply with the potentially subjective and variable wishes of a consumer. Other privacy policies have promised to use "best efforts" to protect consumer information. When technical people say "best efforts," they mean that they will try to do something, and if they can do it – great. From a legal standpoint, that actually describes what are known as "reasonable efforts." On the other hand, in legal terms, "best efforts" means that you will use ALL efforts, regardless of cost. This type of distinction is one of the big reasons why your privacy policy should be reviewed by your legal department.

The introduction should also specify that your company's privacy policy can be modified at your discretion without prior notice to consumers, and that any changes to the policy will apply both to all information gathered after the change and retroactively to all information already in your company's possession. Although it has not been settled whether or not such language will be effective, having it at least provides notice to consumers that retroactivity is your policy.

An example of good introductory language is:

> [*Web site*] supports a general policy of openness about personal data collection and use. We have adopted and implemented this Privacy Policy as part of our commitment to protecting your personal information from misuse. Although this Privacy Policy is not intended as a contract or as creating any legal rights, it does represent [*Web site*'s] current policies with regard to personal data collection and use. We reserve the right to modify this policy at any time without notice, and any changes to this policy will apply to all information then in [*Web site*'s] possession or acquired after the date of such change.

PrivacyPolicy Part 2: Contents

The policy should explain your company's policies with regard to:

NOTICE: WHAT INFORMATION YOU COLLECT

Early in your privacy policy, you should tell users in a broad sense what information you collect. If you collect personally identifying information such as name, email address, mailing address, or even demographic data such as zip code, age, income, etc., you should notify the user.

If you use tracking technologies such as cookies or Web bugs, disclose it, but explain what they are and why they are used. The following text is an example:

> From time to time, we may use the standard 'cookie' feature of major browser applications that allows us to store data about your visit. Cookies help us learn which areas of our site are useful and which areas need improvement. We do not set any personally identifiable information in cookies, nor do we employ any data capture mechanisms on our Web site other than cookies. You may configure your Web browser to prevent cookies from being set on your computer.

Some Web sites even actually explain, at a very basic level, the difference between session cookies and persistent cookies in order to educate users.

Some Web sites even actually explain, at a very basic level, the difference between session cookies and persistent cookies in order to educate users.

Do not try to make these technologies sound more palatable to consumers by using euphemisms that may end up being technically inaccurate. For example, one Web site tells consumers that it uses "pixels," by which it means Web bugs, to track how consumers move through the site. This kind of technical inaccuracy could lead the Federal Trade Commission (FTC) to believe that the owner of that Web site was trying to mislead consumers. If you (or your marketing department) feel strongly about not using the term "Web bugs," then at least be accurate and call them "single pixel images" or "clear GIFs" and explain how they work.

NOTICE: WHAT YOU DO WITH THE INFORMATION

You should clearly explain what you are going to do with the information. If you plan to share the information with third parties or other partners, say so. If you plan to use the information for marketing purposes, say so and say how. Just as importantly, if you may use or disclose the information, do not say you won't. Failure to comply with a

The user should have the option to decide whether the information will be used or shared.

published privacy policy is exactly the kind of action that would attract the FTC's interest.

Here is a sample of some language used by one Web site that only collects automatic traffic data:

> In general, our site automatically gathers certain usage information like the numbers and frequency of visitors to [*Web site*] and its areas. We only use such data in the aggregate. This aggregate data helps us determine how much our customers use parts of the site, so we can improve our site to ensure that it is as appealing as we can make it for as many of you as possible. We also may provide statistical 'ratings' information, but never information about you personally, to our partners about how our members, collectively, use [*Web site*].

Children under 13

You should confirm with your lawyers that your Web site is in compliance with the regulations related to the Children's Online Privacy Protection Act of 1998 (COPPA).[2] If any portion of your Web site is directed toward children under 13, including providing products or services directed to children under 13, then you need to comply with the COPPA regulations. On the other hand, if your Web site is not intended for children under 13, the following is an example of the type of language you could include:

> [*Web site*] respects the sensitive nature of children's privacy online. We are a general audience site and do not direct any of our content specifically at children under thirteen (13) years of age. We have implemented procedures so that if we obtain actual knowledge of a child's personal information, we will take steps to delete that information. In addition, if [*Web site*] knows that a user is under age 13, we will NOT:
>
> 1. deliberately collect online contact information from that user without prior parental consent, except where used to respond directly to the child's request;
> 2. deliberately collect personally identifiable offline contact information from that user without prior parental consent;
> 3. deliberately give that user the ability to publicly post or otherwise distribute personally identifiable information without prior parental consent;
> 4. distribute to third parties any personally identifiable information of that user without prior parental consent;
> 5. entice that user, by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in the activity.

Be sure, however, that if you use this type of language you comply with it. Failure to comply with provisions like this when posted on your Web site could lead to unwanted attention from the FTC. So far, the FTC has taken action and levied fines against several Web sites that have violated COPPA and/or their own privacy policies:[3] the fines have ranged from $30,000[4] to $100,000.[5]

CHOICE

The user should have the option to decide whether the information will be used or shared.

You should include directions for how users can prevent you from providing their information to a third party, to remove their information from your database, or to stop receiving communications from you. You can set up an email address, URL or other contact method. The following is an example of language you can use related to opting out:

> Opting Out
>
> [*Web site*] gives you the following options for contacting us to (i) prevent your information from being shared with third parties; (ii) stop receiving communications from us; (iii) remove your information from our database (which may prevent you from receiving our service); or (iv) stop receiving our service:
>
> 1. Send email to [opt out email address]
> 2. Visit [opt out URL]
> 3. Send postal mail to [opt out address]
> 4. Call [opt out phone number]

The user should have the ability to see what information you have collected and to correct it, if necessary.

ACCESS

The user should have the ability to see what information you have collected and to correct it, if necessary.

You should include directions for users to review and modify information from your database. You can set up an email address, URL, or other contact method. The following is an example of language you can use related to users accessing and modifying information:

> Updating Your Information
>
> [*Web site*] gives you the following options for changing and modifying information previously provided:
>
> 1. Email [*corrections email address*]
> 2. Visit [*corrections URL*]
> 3. Send postal mail to [*corrections address*]
> 4. Call [*corrections phone number*]

Finally, you should refer any questions related to the privacy policy to a contact person:

> Contacting [*Web site*]
>
> If you have any questions about this privacy statement, the practices of this site, or your dealings with [*Web site*], please feel free to contact: [*contact information*].

SECURITY

You should have in place protections appropriate to the nature of the information collected; for example, health care or financial information would be expected to be better protected than an address list.[6]

Your Web site should specify that you have taken “reasonably appropriate security measures” to protect information in your possession and should generally describe the technologies you use for security (e.g., SSL). You are not required to (and should not) discuss in detail the security practices on your Web site. You should recognize, however, that in the event of a use or disclosure by an unauthorized person of information stored by you, your security policies and practices could come under scrutiny. Even if your practices are reasonable by current industry standards, in the event of a security breach, you could be criticized for not doing enough to protect your information.

So far, dealing with privacy in the US has been complicated and expensive.

Security and incident response are areas where you should have a team of technology, legal, operations, and marketing personnel developing policies and procedures. Unless your operations and marketing people understand the implications of security, including potential legal/regulatory issues, and unless those same people believe that you understand their concerns about the impact of security on operations and customers, they will not cooperate with you, and your security efforts may be circumvented.

Life Gets More Complicated

So far, dealing with privacy in the US has been complicated and expensive. If your site caters to children, you have to deal with COPPA. If you are in the financial industry, you have to deal with the requirements of the GLBA.[7] If you are in the medical or heath insurance fields, you will be subject to the regulations being developed associated with HIPAA.[8] On top of these domestic laws, if you operate in or receive data from Europe, you may have to comply with the European Union Privacy Directive.[9]

So far, it is not clear how these various laws and regulations will evolve or interact. For example, what happens when US and EU privacy regulations conflict? Is a bank that provides outsourced billing for an HMO subject to HIPAA? What about credit card companies who process payments for medical services – do they have to determine whether a payment is medically related and treat that information differently from all other data? Should health insurance companies that provide financial services be subject to GLBA? The HIPAA regulations have not been finalized yet, so there may be even more surprises in store.

As if all that uncertainty weren't bad enough, dealing with privacy is getting worse. Other countries are beginning to pass privacy legislation similar to the EU Privacy Directive – notably Canada[10] and Australia.[11] In the US, furthermore, FTC Chairman Timothy Muris stated in a recent speech at the Privacy 2001 Conference in Cleveland, Ohio, that "privacy promises made offline should be held to the same standard as online privacy promises" and indicated that ensuring the security of sensitive information is fundamental to privacy, whether that information is collected online or offline.[12]

In a December 5, 2001, speech to the Promotional Marketing Association, the director of the FTC Bureau of Consumer Protection, Howard Beales, stated that a company's online privacy policy also applies to offline collection and the use of such offline information, unless the policy clearly limits its promise to the online realm. The FTC has begun looking more closely at whether companies are complying with their own privacy policies with regard to information collected online and offline, and whether companies are implementing security procedures that are sufficient to protect the information they collect.

It is not clear what the new FTC policy means for businesses, but it could make life very difficult – both operationally and in terms of technology. For example, you may need to create the ability to move all data collected offline into the area where your online-collected data is stored, so that consumers will be able to access that offline-collected data electronically. Your company may have data-sharing agreements in place regarding data collected offline, and those agreements may conflict with the privacy policy on your Web page. How will you make the people providing data offline aware of your privacy policy? Until the FTC's policy becomes clearer, your privacy policy on your Web page should clearly limit the application of the privacy policy to information gathered via the Web page.

Conclusion

Regardless of how some of the current issues in privacy law turn out, you should give a great deal of thought to how your company deals with information and data privacy. Your privacy policy is no longer something that you can just slap together (or poach from another Web site) and stick on your Web site. Your privacy policy needs to be carefully crafted, in cooperation with legal, operations, and marketing, to deal with your operations and your industry, and failure to pay attention could result in unwanted attention from the FTC, foreign regulators, and/or the media.

Your privacy policy is no longer something that you can just slap together.

Notes

[1] This article provides general information and represents the author's views. It does not constitute legal advice and should not be used or taken as legal advice relating to any specific situation.

[2] See Title XIII of PL 105-277, 15 USC 6501. See also, "Taming the Wild West: Laws and Regulations Governing the Technology Industry," *;login:*, vol. 25, no. 5, August 2000, pp. 43-49.

[3] *http://www.ftc.gov/privacy/index.html*.

[4] *http://www.ftc.gov/opa/2001/10/lisafrank.htm*.

[5] *http://www.ftc.gov/opa/2001/04/girlslife.htm*.

[6] HIPAA regulations, for example, include specific language and requirements related to the protection of health information.

[7] For a discussion of the requirements under the GLBA, see the FTC's Web page at *http://www.ftc.gov/privacy/glbact*.

[8] PL 104-191, Aug. 21, 1996.

[9] See Gary Rothenbaugh and John D. Woodward, "Fact Sheet on the European Union Privacy Directive," *http://www.dss.state.ct.us/digital/eupriv.html*, and the US Department of Commerce's page at *http://ww.export.gov/safeharbor*.

[10] Privacy Act 1980-81-82-83, c.111, Sch.Ii "1". See also, the Canadian Privacy Commissioner's Web site at *http://www.privcom.gc.ca/legislation/index_e.asp*.

[11] Privacy Amendment (Private Sector) Act 2000 (Act No. 155 of 2000). See also, the Australian Attorney General's Web page at *http://www.law.gov.au/privacy*.

[12] Timothy J. Muris, "Protecting Consumers' Privacy: 2002 and Beyond," October 4, 2001, *http://www.ftc.gov/speeches/muris/privisp1002.htm*.