Interacting with Your On-line Web Visitors Can Create Privacy Concerns

By Craig Foster, Thompson Hine LLP

Columbus Business First, (April 14, 2017) – If your organization is getting ready to launch a new website, most likely it's brimming with features that provide a more interactive and user-friendly online experience for the visitor. But if you are collecting personal data of any kind from users, the implementation and disclosure of privacy practices must be part of the planning process before you launch your new site.

Websites and operators often collect, use, share and dispose of personal information in many different ways. Those practices can trigger different legal requirements under many different laws and jurisdictions, depending upon the type of information being gathered and from whom it is collected. In today's regulatory environment, there is a potential for noncompliance simply due to the sheer number of potential requirements that may apply.

Whether you are asking users to create a profile or provide personal information to apply for a job, a number of federal laws may apply including the Federal Trade Commission (FTC) Act, Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), as well as state consumer protection and privacy acts. And those just scratch the surface because foreign laws may apply as well.

Collect only what you need: Consider carefully what personal information is actually required to provide your service. Collect only what you need, and dispose of it securely when you no longer need it.

Keep it simple: An effective website privacy policy should meet certain minimum standards. It should be easy to locate on your website, easy to read, describe what information the site collects, and explain how such information is processed, protected and disposed. And, most critically, ensure that your policy is accurate. Outside of violating legal requirements, failure to follow promises made in privacy policies has been one of the principal reasons for regulatory enforcement actions.

Consider current legislation: To effectively develop a privacy policy for your organization, ensure that you consider the current statutory and regulatory climate affecting the industry and organization, and seek legal help if you need. What personal information will be collected? Is it sensitive data, such as health or financial information? From whom is it being collected (such as children or foreign nationals)? Where is it being sent (U.S. or internationally)? How

will you dispose of the information? Are there any self-regulatory initiatives with which the website policies and practices must comply, such as industry or trade organization affiliations? Legal and regulatory considerations such as these are critical when designing and implementing an effective privacy policy.

When sharing is bad: The policy also should explain how information will be used and whether it will be shared with other parties. Beware of statements such as "we will not share your information ever" or statements that appear to offer consumers a choice regarding sharing practices unless you have the means for processing those choices. Privacy policies with terms that your firm cannot easily comply with are easy targets for regulatory agencies.

Coming to terms: A companion to a website privacy policy is a site's Terms of Use agreement. Does the website require affirmative acceptance of the terms of use, such as a click-through agreement? Do they set forth prohibited uses, limitations of liability and disclaimer of warranties designed to protect your organization?

Stay vigilant: Ongoing maintenance and review of the site is equally important. Owners should identify areas of law and enforcement actions that may affect the site in the future based on anticipated changes in law or business practices. And, as the site changes, you will need to consider if changes in content, features or information sharing practices require notification, disclosure, addition of disclaimers, restriction of certain access or modification of operations. Establish a point person who will review all changes and monitor industry best practices.

Because most organizations have websites, inevitably there is a risk. The scope of privacy-related laws and regulations that may apply are enormous. With this in mind, it is critical that those overseeing your website are doing what they are required to do and what they promise to do. Failure could result in hefty fines, significant administrative burden and damage to your reputation. Building the cost of assessment and thoughtful design into the planning process is a lot less costly than the cost of noncompliance.

For more information on ensuring your organization is meeting critical privacy laws and regulations, contact Thompson Hine's Information Security & Privacy group.

About Thompson Hine LLP. *Thompson Hine LLP, a full-service business law firm with approximately 400 lawyers in 7 offices, is ranked number 1 in the category "Most innovative North American law firms: New working models" by The Financial Times. For 4 straight years, Thompson Hine has distinguished itself in all areas of Service Delivery Innovation and is one of only 7 firms noted in the BTI Brand Elite for "making changes to improve the client experience." The firm's commitment to innovation is embodied in Thompson Hine SmartPaTH® – a smarter way to work – predictable, efficient and aligned with client goals. For more information, please visit ThompsonHine.com and ThompsonHine.com/SmartPaTH.*

Craig Foster is a member of Thompson Hine's information security and privacy group. He advises clients on state, federal and international privacy and information security matters and he carries the Certified Information Privacy Professional/U.S. (CIPP/U.S.) credential. Craig.Foster@thompsonhine.com; 614.469.3280

Reprinted with permission of *Columbus Business First*