

Privacy Rights and Policies Evolve

Many businesses collect personal information on their websites, ranging from name and email to home phone and address; often to employer data and job title; and sometimes to income level and credit card information.

Recently, however, attention has focused on privacy practices after repeated reports of unintended releases or thefts of credit card information and other personal data. For example, within the last year it was reported that hackers had stolen over 4000 credit card numbers from the official Rhode Island website and that at least 23 Senators were using cookies to track visits to their web site, despite pledging not to do so.

Thus, a critical issue for businesses is: what should their Internet privacy policies say, and what does the law require? The following highlights legal and practical concerns.

U.S. Privacy Law

U.S. privacy law is a patchwork of interlocking rules and regulations. In general, except for a handful of areas where specific laws govern — financial institutions collecting financial data (subject to Gramm-Leach-Bliley), healthcare entities and their business associates collecting personal medical information (subject to HIPAA), and sites targeted to or knowingly obtaining information from children under 13 (subject to COPPA) — the governing principle is twofold: accuracy in describing how personal data will be used, shared and safeguarded, and compliance, or following your own policy in practice.

Indeed, the FTC has sued and settled with several companies for misrepresenting what they do under §5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices. Thus, for example, in January the FTC announced that Choice-

Does your business:

- ✓ Collect personal information from visitors to your website?
- ✓ Post a privacy policy on your website explaining how you protect, use and share information?
- ✓ Collect personal data from California or Europe?

Then, read on...

Point had agreed to pay \$15 Million to settle FTC charges that its procedures for handling data violated consumers' privacy rights, after data pirates infiltrated ChoicePoint's database and stole personal information of over 145,000 people ... which incident ChoicePoint had allegedly failed to disclose for 4 months.

State Activities

The landscape in the U.S. changed significantly when in July 2004 California became the first state to require, by law, that web operators post their privacy policies on their home page (or make them accessible from the home page in a defined manner) and that these policies identify the types of personal information collected, the classes of third parties with whom this might be shared, the process for consumers to review and change their data, and the process by which operators notify consumers of material changes to their privacy policies. California's Online Privacy Protection Act applies to all businesses that have a commercial web site that reaches California consumers and is enforceable by fines and injunctions.

It was reported recently that over two dozen states are considering legislation to empower consumers over the use of their personal data.

European Union: Privacy Directive

The Europeans are far ahead in protecting personal information, by virtue of the 1998 Privacy Directive, which requires member states to enact strict laws that protect personal data. Indeed, as originally passed these laws would require the application of the same strict rules to foreign (including American) businesses that collect data from the EU. However, in 2000 the U.S. reached an agreement with the EU whereby American businesses can comply with EU law by satisfying certain "Safe Harbor" conditions.

These Safe Harbor principles permit U.S. businesses that collect personal information to transfer that information to third parties, provided they comply with certain basic principals concerning notice (individuals must be told how their personal data will be used), opt-out (individuals must have the right to choose whether their data can be transferred to third parties), opt-in (sensitive data cannot be transferred or used in a new way without express consent) and onward transfer (to receive collected data, third parties must provide the same level of protec-



The law firm built for business.SM

tion), as well as access, security, integrity and enforcement.

Breach of Security

To add a final complication, following the example set by California, over 20 states and one locality have laws that require notification in the event of certain breaches of security. So now, on top of adhering to privacy rules that govern the collection and use of personal information, companies may have additional duties under the laws of relevant states to notify people when their information is stolen.

Recommended Actions

If you operate a business that collects personal information over the Internet (or otherwise), be sure to do the following:

- ✓ Consider whether your business is subject to specific privacy or security rules, for example, because it is the type of financial or medical business that is subject to Gramm-Leach-Bliley or HIPAA.
- ✓ Post a Privacy Policy on your website that *accurately* and *completely* describes how you protect, use and share personally identifiable information; *don't over-promise*.
- ✓ Check these policies periodically against your actual practices to be sure you do what you say you do, that your policies allow for actual *and predictable* uses of collected data, and that your security features are up-to-date and effective. *Have procedures to prevent security breaches.*
- ✓ Be sure your policy allows you to transfer collected data to successors or acquirers of your business, to cooperate with law enforcement, and to ensure the safety of members and the public.
- ✓ Offer subscribers a way to update or remove their personal information.
- ✓ Consider including in your Privacy Policy or Terms of Use (you have those, right?) specific limitations on your liability for security breaches and for misuse or disclosure of confidential data.
- ✓ Determine if security or privacy violations would be covered by your insurance, or if such insurance is available to you.
- ✓ Ensure that all personnel with access to personal information are familiar with — and required to comply with — your security and privacy rules.
- ✓ If you do business within the EU, consider whether EU rules apply and how to respond, including privacy self-certification and Safe Harbor compliance.
- ✓ If you sustain a breach of security, consider whether your privacy policy, applicable state laws, or just good business practices require that you notify consumers or take other actions.
- ✓ Finally, keep abreast of changes in the law, including state legislation that could apply to you ... and be sure your advisors do, as well.

The Morse, Barnes-Brown & Pendleton, PC, **Technology Licensing & Intellectual Property Practice** counsels businesses of all sizes on creating, protecting and transferring IP assets, including advice on trademark, copyright, advertising, Internet and technology law.

Peter N. Barnes-Brown -
pbarnes-brown@mbbp.com

Howard G. Zaharoff - hzaharoff@mbbp.com

Jeffrey P. Steele - jsteele@mbbp.com

Shannon S. Zollo - szollo@mbbp.com

Thomas F. Dunn - tdunn@mbbp.com

Michael J. Cavaretta - mcavaretta@mbbp.com

Morse, Barnes-Brown & Pendleton, PC
Reservoir Place, 1601 Trapelo Road
Waltham, MA 02451
781-622-5930

 **MORSE
BARNES-BROWN
PENDLETON** PC
The law firm built for business.SM

IP News is intended as an information source for clients and friends of MBBP. It should not be construed as legal advice, and readers should not act upon information in this article without professional counsel.

© 2006 Morse, Barnes-Brown & Pendleton, P.C.