



New Regulatory Definitions May Change the Business You Thought You Were In

Author: Jon Garon, Dean, Hamline University Law school

Until recently, the United States government has played a relatively non-intrusive role in regulating Internet privacy and security matters. Although a few regulations predate the World Wide Web, it is only this year that the first statutes and regulations drafted on Internet privacy have gone into effect.

The Federal Trade Commission (FTC) has identified privacy concerns as one of the significant inhibitors to Internet business growth. The FTC warned that "consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information."

Congress has responded to the public concerns for privacy and security in the limited areas of children, banking and health care. Yet despite the seemingly discrete areas of regulation, emerging federal rules will have a much broader impact on the Internet community and e-commerce activities.

The only federal law drafted to cover all Internet Web sites is the Children's Online Privacy Protection Act (COPPA), which limits access to children under 13 years of age. According to the FTC "(if) you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children or if you operate a general audience Web site and have actual knowledge that it collects personal information from children, you must comply with the (COPPA)."

Organizations that offer children chat rooms, e-mail or hobby information that may result in collecting the child's personal data, such as name and address or e-mail, must comply with the FTC regulations.

COPPA requires that any party that collects personal information from children must first receive parental consent. The obligations for consent are more detailed if the data is shared with third parties. The goal of the regulations is to eliminate the collection of data on children in all situations other than those in which the child has been enrolled in a program by the parent.

From a planning perspective, nothing in the regulations suggest that the FTC will remain limited by Congress to enforcing regulations for only those under 13 years of age. Business should not be surprised to see the FTC jurisdiction expand over time. Because the types of activities covered by COPPA are reasonably clear, however, there has been

little objection to the privacy requirements or to the implicit goal of reducing commercially available information about our children.

Unlike the privacy of minors, commercial access to an adult's personal financial information is big business. Credit reporting agencies, banks, insurance companies, and many other providers buy and sell financial data as the first step to sell the public credit cards, mortgages and insurance. Access to this private information is a valuable commodity.

In a comprehensive update of federal banking and insurance law, Congress expanded the piecemeal regulation of online privacy and security. Under the Gramm-Leach-Bliley Act (GLBA), a financial institution must allow a customer to opt out of having non-public personal information sold to non-affiliated third parties. The Securities Exchange Commission has adopted complementary regulations for the financial services firms subject to its regulation. The financial institution must provide the disclosure at the time of the initial transaction and at least annually thereafter.

Despite a wide variety of loopholes in GLBA, the statute will have a long reach. The definition of financial institution is very broad. It ranges from traditional banks and finance companies to include some travel agencies, credit counselors and any business offering credit cards.

For companies covered by the GLBA, non-public information cannot be shared with unaffiliated third parties. The law exempts transfers of private information for the purpose of carrying on the business activity "in the ordinary course of business." This allows Web site design companies, check printers, data storage facilities and other ancillary service providers to access personal information, but only to the extent necessary to conduct the business of the financial institution.

Any company with access to non-public personal information is then bound by the banking regulations. As security and privacy requirements are implemented for the banking industry, these same requirements will be applied to the software, data storage, ISP and other service providers that support the banking industry. Depending on the data services a company provides, it may find itself suddenly being regulated as a financial services company.

The best illustration of this approach comes from the regulation of health care information. In 1996, Congress adopted the Health Insurance Portability and Accountability Act (HIPAA) to promote the ability of the public to transfer health care and insurance coverage from one provider to another. Under HIPAA, health care providers must provide substantial privacy and security measures to protect an individual from improper disclosure of health care information.

HIPAA regulations apply to the data itself -- wherever housed -- as well as the authors of the data. The Department of Health and Human Services (HHS), the regulator for HIPAA, has been the first federal agency to recognize that privacy and security issues are directly related. Privacy cannot be guaranteed unless confidentiality and security are fully maintained.

Under proposed HIPAA regulations, any company -- Web site design, data storage, computer backup or business consultant -- that has access to private health care information must meet all the security and privacy obligations under the HIPAA security requirements. These security regulations have not yet been finalized. No present legal obligation exists, but the draft proposals have been quite detailed.

The HIPAA regulations reflect an exacting, comprehensive standard of security that may surprise the industry. HHS has explained that the goal of the security regulations is to protect the confidentiality of private data from both "the risk of improper access to electronically stored information" and "the risk of interception during electronic transmission of the information." The regulation combines administrative procedures, physical safeguards, technical security services and technical mechanisms into a unified security standard. If successful, these regulations will serve as the model for many other federally regulated industries.

Even a company that provides no health care services must be prepared to enter into agreements that allow a health care provider to protect the integrity and security of the data from a wide variety of risks. Each company with access to data must be able to certify that the data is secure from internal risks (such as access by unauthorized personnel) and external risks (destruction by hackers, interception).

To the extent data is shared, transmitted, or stored with other companies, a "Chain of Trust Partner Agreement" must reflect the agreed-upon steps necessary to protect the data from any type of disaster (fire, hackers, defective storage medium, etc.).

The Chain of Trust Partner Agreement contemplated by the regulations is a very intrusive document, requiring that the health care company be able to monitor the activities of its partners' security conduct, personnel hiring, training and management. The proposed rules contemplate that the Chain of Trust Partner Agreement will state that both parties will protect the data, monitor compliance with the agreement, report all security failures and take steps necessary to cure any breaches of the agreement.

The agreement must assure that private information is limited to the greatest extent possible so that individuals do not use the information for any improper purpose or accidentally release the information to any third parties. It must also provide comprehensive employment policies that provide for ongoing training, supervision, as well as concrete security measures regarding personnel termination.

In addition, for each of these steps, the process must be formal, with documented instructions and auditing of compliance. For many companies, the task of documenting the necessary practices may be more onerous than complying with the required practices themselves. Nonetheless, both the documentation and the conduct must be in compliance.

A few companies are actively developing the procedures to comply with the HIPAA privacy and security regulations. Many others are now being asked to do so.

Those companies that meet the health care standards will have a distinct advantage for providing services in the banking industry as well, because the security requirements will become quite similar.

The governmental regulation of health care and banking will set new industry standards for security and privacy that will directly reach a much broader segment of the e-commerce community, and by example, change the privacy rules for much of the e-commerce in the United States. The quiet, piecemeal approach Congress has taken in regulating privacy may have already set new standards for years to come.

Although your business may not be in health care today, tomorrow it may be a bank. The era of federal regulation has arrived.