

Protecting Privacy, circa 2008: Our personal information now in the clouds?

By Randy V. Sabett – ISSA member, Northern Virginia, USA chapter



Several years ago, every business on the Internet worried about having a privacy policy, and many tried to make sure their privacy policy accurately captured the business' practices. For several companies that didn't worry enough, the FTC entered the picture and will remain in the picture for them over the next 20 years. The burning privacy question now centers on what happens as we move toward more computing in the cloud?

Privacy today (at least in the United States) might be best viewed as moving forward chaotically. At one extreme, we have state laws affirmatively requiring encryption of personal information and "red flag" rules addressing identity theft. At another extreme, we have numerous services that some view as heightening concerns over privacy. As only a partial list, things like software-as-a-service (SaaS), targeted advertising, Web 2.0, widgets, and computing-in-the-cloud all raise privacy issues. Almost as a third extreme, we have personal and sensitive information being provided to service providers at an unprecedented pace, both by consumers and by companies.

The notion of SaaS or computing-in-the-cloud (i.e., using applications hosted on remote third-party servers and storing data on those servers) dates back many years. Many companies during the Internet bubble tried to launch Web operating systems and Web applications, but only recently has the concept developed enough momentum to garner serious attention. The implications from a privacy perspective are significant. By using such applications and storing data "in the cloud," both users and data subjects lose some amount of control over their data.

For companies, some protection and comfort may be derived from the contractual arrangements with the supplier of those services. Those companies responsible for sensitive information may find, however, standard confidentiality clauses to be insufficient. Instead, stronger terms and conditions around the security of their data may be needed. Statutory requirements could further drive this issue. For example, at least two states now require that entities encrypt personal information. In addition, the federal "red flag" rules require companies to identify triggers related to potential identity theft. *The complexity of implementing such requirements increases as control over the data decreases.* Carefully constructing appropriate contractual provisions will become a necessity.

Another exemplary privacy concern involves widgets, those small, self-contained desktop or web-based pieces of software that can contain content ranging from text to images, audio, and video to applications. Widgets can be easily distributed (think viral and targeted advertising) and can be placed on any social networking site, blog, or start up page. No longer simply a desktop novelty, widgets can contain powerful and potentially dangerous functionality that is portable across platforms.

Some entities in the widget ecosystem have begun employing information collection practices that in some ways resemble some early web-based applications and services. Certain widget authors or entities that distribute widgets will collect personal information prior to sending the desired widget to the customer. The use of that personal information will depend on the privacy

practices of that author or distributor. The possibility also exists that a third-party widget could collect personal information as part of its functionality. The collection of that personal information could be under an unknown (or nonexistent) privacy policy. Thus, a visitor to a particular website of a first company might click on a widget written by a second company for a product of yet some other third company. That visitor, however, may never be presented with the privacy policy of either the company that wrote the software for the widget or the company whose product is being advertised.

So, is it safe to use these new constructs and, so to speak, venture into the cloud? Certainly, using SaaS, targeted advertising, widgets, and computing-in-the-cloud can help a business control costs and resources. Responsibility for many time-consuming issues (e.g., upgrades, patches, and similar configuration issues) will now lie with a third party. All of these are good things, but hard questions must also be confronted in dealing with the security and privacy implications. At the end of the day, hopefully there is a privacy-focused silver lining somewhere in that cloud.

About the Author

Randy V. Sabett, J.D., CISSP, is a Partner in the Internet, Communications, and Data Protection (ICDP) practice group at Sonnenschein Nath & Rosenthal LLP, an adjunct professor at George Washington University, and a member of the Commission on Cyber Security for the 44th Presidency. He may be reached at rsabett@sonnenschein.com.