Data Privacy in an Online World

by Joshua Gold

As social and business networking sites have taken off, the privacy of data has become increasingly more vulnerable. With legions of online users uploading and posting huge volumes of both personal and business information, the demarcation between business and personal content is becoming more blurry with every passing day. The deployment of business-related information to these social networking sites has created a whole new set of issues regarding the use and privacy of information posted online, particularly on social networking sites.

For example, in a recent decision, a federal judge ruled on the legitimacy of subpoenas seeking online messages and user-posted information from four different networking sites in connection with a business dispute. While the judge ended up quashing the subpoenas in question and ruling that third party networking sites did not have to disclose private messages between their users, the decision did not resolve the issue of whether wall postings on such sites would have to be disclosed under the subpoenas. According to the ruling, such a decision would have to hinge upon the privacy settings opted for by the user.

Undoubtedly, many other issues remain, which means that businesses need to think carefully about the implications of their data appearing in an ever-expanding panoply of public and semi-public repositories. Last year, one social networking site angered many of its users by reserving its right to use member content after a user closes his or her account, while several other announcements regarding the use and availability of user information by networking sites has prompted calls for state and federal action and investigations.

The upshot of all this is that data privacy remains in a state of great flux. Since millions of individuals and businesses have likely had their personal or business information compromised either through hacking incidents or loose policies concerning the use of data uploaded or posted onto social networking sites, risk management and insurance issues will become increasingly more important for companies seeking to minimize the repercussions from major losses or misuse of online data.

Insurance Coverage and Risk Management

Many policyholders worry whether their business, employee and customer-related information can be inappropriately accessed no matter how many state-of-the-art safeguards they employ for online data. But when information does get wrongly accessed and misused, policyholders may have insurance coverage for breaches of online security. Many forms of liability insurance protect against invasion of privacy claims. Should a policyholder be confronted by such a claim, umbrella insurance, general liability insurance, errors and omissions policies and other stand-alone specialty insurance policies should be checked for potential coverage. More proactively, if an insurance portfolio review reveals that those provisions have been written out of the businesses' portfolio of insurance, the broker should be enlisted to get those increasingly important coverages back in. If these provisions cannot be written back into existing policies, then stand-alone insurance policies specifically designed to cover online risks should be explored with the insurance broker.

Historically, media and publishers' policies have also contained protection from online risk exposures. These policies, including media errors and omissions insurance coverage, may provide the insurance coverage framework for valuable protection to businesses of all types.

Beyond insurance, other risk management strategies can be effective in minimizing the risk of online data security breaches. While the risk cannot be eliminated, it may be ameliorated by employing a few common sense principles in an organized and systematic approach. It is almost axiomatic that up-to-date security software and firewalls should be employed to safeguard the business' computer system. Less obviously, a business protocol should be adopted that regulates the manner in which data is used both outside of and inside the office. Given the size of laptop computer hard drives, it is critical that information contained on laptops be protected as much as possible. Also, mobile devices should be password protected, given their ever-expanding capabilities and memory size. Information within the organization should be ranked in terms of sensitivity, and internal access limited based upon actual business needs. Lastly, for those businesses dabbling with or embracing social media sites as part of their business strategy, care should be taken as to the extent of the information posted or uploaded to those sites, as it could lead to information being exposed to many more eyes than originally intended.

While no data security plan or approach will ever be water-tight, a combination of smart data-handling procedures and quality insurance coverage can lessen the blow of unauthorized or unintended uses of business-related data.

Joshua Gold *is a shareholder in the New York office of the law firm of Anderson Kill & Olick, P.C. where he regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property insurance coverage issues.*