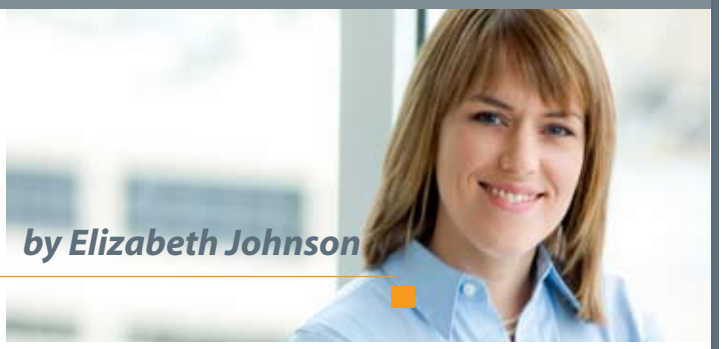
JULY 2010

PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

Are Facebook's Woes a Preview of Things to Come for Amazon?

Reprinted from TechJournal South, July 28, 2010



by Elizabeth Johnson

Most of you are familiar with the controversy over Facebook's revision of its privacy settings, with the default settings generally causing users to share more information about themselves with more people and, in some cases, with everyone on the Internet.

Around the same time, another controversy arose involving Facebook that received less attention: The social media site's sharing of individual user information with advertisers in apparent violation of its privacy policy.

Facebook's Legal Troubles...

Now, to be fair, other social media sites like MySpace are alleged to have engaged in the same behavior and the disclosure was potentially inadvertent. Although there are variations, the disclosure typically proceeds down a similar path. First, a social media user logs into their page and, while there, gets interested in an ad on the page.

The user clicks on the ad. That click automatically results in the social media site (in this case, Facebook) sending to the ad provider a stream of information. In the case of most websites, that stream of information ordinarily does not include anything about the user at an individual level. For example, the stream includes the website URL the user visited at the time he clicked the ad.

But, in the case of social media sites, a user's profile page often includes their username within the URL so, if the user clicks on the ad from his profile page, the stream of information sent to the advertiser will include his username. If the username is the user's actual name, then the advertiser now has his name as well.

In either case, the allegation is that the advertiser can now identify the individual user who clicked on the ad and may go back to his profile page on the social media site and view other information about him. And, in Facebook's case, since the site recently reset default privacy settings to make ever-greater personal information available to a larger audience, that advertiser will find more personal information now than it might have in the past.

Facebook faces lawsuit

As a result of these disclosures, Facebook faces a user's lawsuit claiming breach of contract due to its actions. The theory goes like this: Facebook promised users in its website privacy policy that it would never share their personal information with advertisers unless the user first consented. In spite of that promise, Facebook sent personal information to advertisers without consent in the manner described above.

The plaintiff is claiming that violation of Facebook's privacy policy is a breach of contract. Similar disparities between what a website privacy policy says as compared to what the website provider actually does have formed the basis for similar private actions and also government enforcement, particularly "deceptive trade practice" claims by the FTC.

In the FTC cases, providers often settle the FTC's claims by agreeing to FTC review of all proposed consumer privacy notices, disgorge any moneys earned from the alleged deceptive practices, and retain for the FTC's inspection copies of any invoices, records or communications related to any disclosure of information to a third party. As a result, violating your own privacy notice, even inadvertently, can be an expensive proposition.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Another case: Amazon vs. North Carolina

Now let's consider these developments in the context of another recent privacy-related case: Amazon's dispute with the state of North Carolina over the state's requested release of customer records. Presumably, the state would like to know the individual identities of Amazon's customers in North Carolina so that the state can review whether those shoppers paid sales tax in connection with their purchase of goods.

The controversy over whether such purchases are subject to state sales tax has a fairly long and contentious history, with Amazon closing its North Carolina affiliates in June 2009 to bolster its argument that it has no obligation to charge North Carolina sales taxes.

In the current case, Amazon is fighting the state's request for customer records, in part by claiming that there are privacy concerns with releasing customer information to the state. While some may judge this assertion by Amazon as nothing more than a smokescreen to fight what is really its staunch aversion to charging state sales tax, this view is too cursory.

As discussed above, a website operator can face real liability when its disclosures of information are contrary to the promises it makes to users in its website privacy policy. So what does Amazon's privacy policy say to users about whether it will disclose information to the government? The most relevant promise seems to be, "We release account and other personal information when we believe release is appropriate to comply with the law . . . ."

Court order ramifications

If Amazon had simply handed over the information because North Carolina asked nicely, it would be a little difficult to say that it had lived up to the promises in its privacy policy (and, yes, these statements often are enforced as promises in legal disputes) because the disclosure would arguably not have been "appropriate to comply with the law."

But what if Amazon, as it is doing here, fights the request in court but, despite its arguments against disclosure, is ordered by the court to hand over the information? In that case the disclosure is more clearly necessary to comply with law and, among other things, provides Amazon with a clearer defense to any customer-filed complaint alleging it violated its privacy policy by disclosing the information.

What are the chances of an Amazon customer filing a privacy-related claim against it in connection with disclosures of information to state government? Hard to say, but it usually depends on how annoyed the customer is by the objectionable disclosure and what level of harm he actually suffered.

In Facebook's case, its user filed a lawsuit over a seemingly inadvertent disclosure of demographic information to advertisers that would, at worst, result in the user receiving unwanted ads.

Amazon's Quandry

If that behavior is enough to prompt a lawsuit, imagine the ire of Amazon customers who find themselves outted by the company to state tax auditors who will, as a result of that disclosure, potentially demand that those customers pay past due sales taxes and subsequent penalties.

Now consider the scale of Amazon's quandary. If North Carolina succeeds in its request, can other states be far behind, particularly now that state coffers are running on empty?

So what's the lesson here for any organization with a website? Be careful with your website privacy policy. In most cases, websites are required to post one in order to comply with law. So, when producing yours, you need to carefully consider your current uses and disclosures of information collected via the site and, ideally, anticipate future uses and disclosures.

All should be disclosed clearly but at an appropriately general level so that users are informed of your practices but you maintain reasonable flexibility.

It's very helpful to be apprised of current case law in this area so that you understand the types of statements that proved problematic for other organizations. And, of course, know which laws apply to your provision of privacy policies to consumers and make sure all the legally-mandated contents are included.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.