PROSKAUER ROSE LLP

# A Moment of Privacy

A newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose

December 2008

Edited by

Kristen J. Mathews

Welcome to "A Moment of Privacy," a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

"A Moment of Privacy" addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

## And now for this month's question:

Q: My company's marketing department wants to launch a campaign with a partner that will involve obtaining a user's address book contacts from his Web-based e-mail account and sending marketing messages to those contacts. What should I watch out for in connection with this campaign?

*A:* More and more clients have been asking about these sorts of "address book scraping" campaigns, in which a user is asked to import his contacts (i.e., the e-mail addresses he has stored in his e-mail account address book) into his social networking Web site or other online service so that a message can be sent to those contacts inviting them to join the social network or to participate in a joint offering of the client and its partner. In some cases, the user is asked to provide the username and password for his e-mail account so that the import can be done transparently.

There are a number of things to look out for in connection with these campaigns:

- ***Transparency***. Some of these programs have not made it clear enough to users that when they import their contacts, messages will be sent to those contacts. In some cases, this explanation has been buried within terms and conditions that are not actually read by the user. In one case, social network reunion.com suffered bad publicity (http://www.latimes.com/business/la-fi-lazarus16apr16,1,4041604,full.column) in connection with this sort of campaign.

- ***Unsolicited, Deceptive E-mail***. The recipients of marketing e-mails may also object to being targeted through these means. In a suit against reunion.com

(http://www.scribd.com/doc/8325973/HoangVReunion100308?secret_password=1c5gbxcez8tn7afd0gvd), a recipient of a marketing e-mail that was sent using an e-mail address that was taken from a user's address book alleged that the e-mail she received was deceptive because it purported to be from her friend when, she alleged, it was really from the social network service, and sent without her friend's informed consent. (Although the plaintiff's initial pleadings have been dismissed on federal pre-emption grounds, the plaintiff has been given leave to amend her pleadings.)

- ***Deceptive Sales Tactics***. In a similar case, another social networking service, classmates.com, was recently sued in a class action alleging that the service deceptively enticed users to pay for a "Gold Membership" with the promise that the users' friends were trying to connect with them. http://www.docstoc.com/search/classmates-class-action-suit/.

What should you look out for when assessing this type of campaign?

- Make sure that the user will be conspicuously informed that his address book contacts will be uploaded into his social networking account and that messages may be sent to those contacts.
- Be wary of programs that solicit users to provide the username and password for their e-mail accounts – a heightened standard of consent may be warranted.
- Make sure that the user provides informed consent for messages to be sent to the e-mail addresses in his address book.
- Make sure that the e-mail messages that are sent comply with the Federal CAN-SPAM Act and are not fraudulent or deceptive.

Your agreement with your social networking partner should establish these points, and should provide a strong indemnification in the event that the program goes awry. Of course, even an indemnification provision would not shield your company from the negative publicity that would result from a poorly administered campaign.

**Have a question? E-mail Kristen J. Mathews at kmathews@proskauer.com.**

## Privacy and Data Security Practice

Our Privacy and Data Security Practice is an outgrowth of our Internet, intellectual property, technology media & communications, labor and employment, health law, First Amendment, international law and litigation practices. Indicative of our experience and reputation in this relatively new field of law is the fact that the venerable Practising Law Institute (PLI) asked our Firm to create its first-ever treatise on the subject of privacy and data security law, called “Proskauer on Privacy,” which was published in late 2006.

Privacy and Data Security Practice Group Partners:

Christopher Wolf, Chair
202.416.6818 – cwolf@proskauer.com

Tanya L. Forsheit
310.284.4508 – tforsheit@proskauer.com

Grégoire Goussu
33.1.53.05.60.11 – ggoussu@proskauer.com

Kristen J. Mathews
212.969.3265 – kmathews@proskauer.com

Jeffrey D. Neuburger
212.969.3075 – jneuburger@proskauer.com