Facebook Security Settings for Lawyers (and Their Families)

By Christopher Hopkins, Chair, Law Practice Technology Committee

At a recent bar seminar on Facebook marketing, the principle questions asked by lawyers were not about what to say – but how to secure their accounts. Without question, before you can promote yourself online, you need to protect your voice. Since many of us are parents as well as lawyers, it may be worthwhile to sit down, laptop to laptop, and compare Facebook settings with your family members to ensure that everyone from the firm to the family is protected. The steps below give you a hands-on opportunity to have a parent-child discussion about internet safety. Why would you pass that up?

We previously covered Facebook security settings in this column one year ago and, since then, Facebook has revamped its security measures twice (April 2010 and August 2011). The following ten steps will ensure proper security, custom-tailored to you and your family members. To begin, log into Facebook, hit the "Account" tab in the upper right corner. It will drop down a short list. In step 1, we will use "Account Settings." For steps 2-9, you will need to begin each step at the"Privacy Settings" page under the Account tab.

1. ***Don't Use Me in Your Ads***: Prevent Facebook and its partners from using your likeness. Under the Account tab, go to Account Settings. On the far left, find a list of options and select "Facebook Ads." In the center of the screen, it will give you two options to edit Third Party Ad Settings and Social Settings. Follow both links, setting them to "no one." Facebook will pop up a few screens begging you not to turn this off but hold your ground.
2. ***No Facial Recognition:*** Facebook has the ability to screen photos uploaded by users and identify if it is you. Convenient for other people… but the answer is no. On the Privacy Settings screen, select "Customize Settings" and find "Suggest Photos of Me to Friends." Select "disabled."
3. ***Who Can See Me?*** Under Account/Privacy Settings, select "Connecting on Facebook" at the top. For lawyers, consider setting each to "Everyone/Public" except Search for You, Friends List, and Activities which you will set to "Friends." For teenagers, consider "Friends" or "Friends of Friends" for most settings. In August 2011, there was a scare that Facebook was distributing user phone numbers. It is easy to solve: don't give Facebook your mobile number. Under the Account Tab, select Account Settings and, on the far left, select Mobile. If it is not already blank, delete your mobile number (as needed, uncheck the boxes).
4. ***Tagging in Photos:*** back on the Privacy Settings page, uncheck the box in the center of the screen which would otherwise allow non-Friends to tag (identify or link) you in photos floating around Facebook.
5. ***Existing Photos/Video on Facebook:*** on the Privacy Settings page, hit "Customize Settings." In the middle of that page, select, "Edit Privacy Settings for Existing Photo and Video." With the exception of your profile picture, lawyers should only allow Friends to see photos and video. For teenagers, consider also limiting the visibility of the Profile Picture to Friends of Friends.
6. ***Things I Share:*** return to the Privacy Settings page and hit "Customize Settings." For "Things I Share," lawyers should limit each setting to Friends except Bio and Website (which will be work-related); teenagers should limit everything to Friends.
7. ***Things Others Share:*** On the same Facebook page used in Step 6, consider whether you want people to publicly comment on your wall (I enabled it; if a problem post arises, just delete it). Photos and Videos, Permission to Comment, and Friends Can See Wall Posts should be set to Friends. As mentioned in Step 2, disable Suggest Photos of Me.
8. ***Facebook Places:*** Rumored to be discontinued this Fall, Places allows you to "check in" at various locations in real life. But Facebook also permits other people to check you in (i.e., publicly announce you are at a specific location, which may or may not be true). In short, it might be great for me to visibly "check in" and let everyone know that I am at the Palm Beach County Courthouse but I do not want a mischievous friend checking me in at an exotic dance club. Keep the control to yourself. Starting at the same page from Step 6, uncheck "Include Me in People Here Now" and disable "Friends Can Check Me Into Places."
9. ***Third Party Apps – Worst Offenders:*** Unless you already fiercely guard your settings, this step may reveal problems with your current Facebook security regimen. On the Privacy Settings page, select Apps and Websites on the bottom left. If you are a frequent Facebook user, you might find six or more "Apps You Use." Edit the settings and delete the apps which you do not use. Meanwhile, do not let your friends' apps share info either: Info Accessible Through Friends should be bio/website only (or whatever you chose for Step 5). Skip "Games and Apps" until Step 10. We disabled Instant Personalization in Step 2, above. Public search should be comparable, if not tighter, than your settings from Step 5.
10. ***Keep Your Gaming Habits Quiet:*** Too many Facebook users allow apps to publicize the growth of vegetables or number of mafia hits. Do not publicize your gaming nor pester your friends. On the Privacy Settings page, again select Apps and Websites. Disable Game and App Activity.

Christopher B. Hopkins might be able to subtly ignore a Facebook friend request but he cannot resist emails from lawyers (and their family members) at christopher.hopkins@akerman.com.