FAMILY TIP SHEET

Privacy, Surveillance, and Self-Disclosure

Online privacy is tricky. The information that we put in digital form can now be readily accessed by unintended viewers, whether because of an oversight in selecting privacy settings, the vulnerability of "secure" online data, sharing passwords that grant others access to personal accounts, or simply because a friend's eyes wander to read personal text messages. Work together with your kids to be vigilant about keeping private information private.

- **Underscore that any digital information has the potential to go public.**

  Information posted online or shared digitally (a picture, a status update, a text message) is searchable, easily copied, and often permanent. Even if your kids set strict privacy settings, there is the chance that a friend could copy/paste, take a screenshot, save, or forward something your kid didn't want to get widely shared. Or, a curious onlooker may simply steal a glimpse at their screens and read private messages. Password sharing with friends, while often done causally, leads to serious privacy issues and should be avoided. Make sure your kids know that it is their responsibility to set privacy settings thoughtfully and to keep passwords private - but also remind them that anything shared digitally might be seen by unintended audiences.

- **Together, set privacy settings on all social media accounts.**

  On a daily basis, you and your children probably use different apps and sites. Together, explore how varied privacy settings and privacy policies are. Discuss how companies use their members' personal information, and urge your children to be responsible and use "friends only" privacy settings. Many social media platforms default to mostly "public" settings — requiring users to set privacy controls. And many sites frequently require updates, which reset all settings back to the default. Not only will these opportunities help safeguard you and your children, but you will get insight into how and why your child participates in the digital world.

- **Be patient and take the time to understand all the features.**

  While companies don't always make it easy to understand their privacy settings and privacy policies, take the time to dig in. Be wary of "social sign-in" (like using your Facebook or Twitter login to sign onto other sites), because that entitles third parties to collect data from your accounts. Set privacy settings for each and every type of content — profile information, posts, comments, and photos. And learn what individual features do, like tagging and blocking, to help you and your children manage and control your presence online. If your kid's school provides devices, it may have the right — and responsibility — to monitor all content on the machines. Make sure your children know that they can't assume their digital life is private from you or from anyone else.

