TIP SHEET

PROTECTING YOUR PRIVACY ON COMMERCIAL APPS AND WEBSITES

Almost all of kids' favourite apps and websites make money from *targeted advertising*, which uses their personal information to choose which ads to show them. Many of them also sell the data they collect to data *brokers*, which use information from many sources to make detailed profiles of users. Some also share it with other apps that are owned by the same company, such as Google and YouTube or Instagram and Facebook.

HOW CAN WE HELP KIDS PROTECT THEIR PRIVACY ONLINE?

As William Budington of the Electronic Frontier Foundation says, "There are things you can do to protect your privacy by 85, 90, 95 per cent that will not add much friction to your life." Here are a few key ones:

- As early as possible, model good privacy behaviours by asking your kids before you post anything about them. Tell them what audiences you think might see what you post and explain what you'll do to limit who else can see it.
- Install privacy-protecting plugins such as **Privacy Badger** on laptops and desktops and apps such as **DuckDuckGo** or **Do Not Track Kids** on mobile devices.
- Review what information different apps are collecting on mobile devices. Teach kids how to do this themselves too.
- Teach young people to review and customize **privacy settings**. These settings are primarily used to control social privacy, but they increasingly offer options to limit data collection (or the use of users' data for things like targeted advertising) as well – though these tools are often accessed in different places than the standard privacy settings.

  For instance, here's how you can turn off tracking and targeted ads on:

  - Google and YouTube: https://myaccount.google.com/data-and-privacy
  - Facebook, Whatsapp and Instagram: https://www.facebook.com/privacy/checkup/
  - TikTok: https://support.tiktok.com/en/account-and-privacy/ personalized-ads-and-data
- Make sure to regularly review the **default** privacy settings, which may change with little notice, and watch for communications from the platform about changes to them.
- Teach kids not to sign in to any apps or websites using their social network logins. You can also show them how to create secure and disposable email addresses using **Protonmail** or **Sharklasers** if they want to register for something without giving away their regular email address.
- Learn together how to limit apps' permission to access a device's camera, microphone and location.
- If your kids use iOS devices such as iPhones or iPads, teach them to refuse data collection when installing new apps. If they use Android devices, install the DuckDuckGo app and turn on App Tracking Protection.

- Teach kids to accept only the minimum required level of data collection on websites – first, by never clicking "Accept All," and then by looking for phrases like "Reject All" or "Only Necessary."

Learn how to skim privacy policies for the most important information, and **teach older kids to do this as well**. To find the most important information, look or search for section titles like:

- **"Personal information we collect"** or **"How we collect your personal data."**
- "**Geolocation**" or "**geotargeting**": If an app wants to access your location for reasons that don't make sense to you, you may need to turn off GPS on your device.
- "**How we use your personal information**": Look for vague phrases like "**business activities**" or "**business purposes**."
- "**Personalize**," "**enhance**," "**improve your services**" or "**interest-based advertising**": If the policy contains any language like this, find out if you can turn off algorithmic sorting (such as by switching from the "For you" to the "Following" feed) and targeted advertising.
- "**Your rights**" or "**your choices**": This will usually lay out what options they have to give you under the laws where you live.
- You can also visit the website **Terms of Service – Didn't Read**, which rates and reviews different apps and websites' privacy policies. **Common Sense Media** also evaluates apps' privacy practices and **Mozilla** has privacy reviews of mental health apps, toys and games, entertainment devices like e-readers and smart devices.

Teach kids to watch out for ***dark patterns*** in an app's design or interface that nudge you to give away more privacy like:

- **obstructing** ways of protecting your privacy, like by making "Accept All" a single button but making you reject different kinds of data collection one-by-one;
- **obfuscating** privacy protections by making them harder to find or being unclear about what they do; and
- **pressuring** you to accept data collection or making you feel bad about protecting your privacy,

TO SPY OR NOT TO SPY?

Parents often feel pressure to use surveillance tools on their kids in the name of keeping them safe. But to model respect for privacy, **we should only directly surveil our kids if there is a clear and present reason to do so** – if they have done something that shows they need close supervision, for instance. Even in this case, however, parents **should be open about the surveillance and clear about the reasons** why we are doing so.

Not surveilling kids, however, **does not mean not supervising them**. With younger kids, that may be as simple as making sure that all connected devices are used in public parts of the house and walking by every now and then to check in. During the tween years, making shared social network accounts can be a form of "training wheels" that also allow them to use their real age when they do create their own account at 13 or older. At all ages, having a conversation about their media lives, clearly communicating your values and expectations through household rules, and modeling the kind of behaviour you want to see are essential.