Safe Space or Police State: How Far Should You Go in Monitoring Your Kids Online?
WSJ

By
Julie Jargon
June 4, 2019 5:30 a.m. ET

Tyler McDonough, 11, recently got his first phone. His mother checks it daily to make sure he's not texting or posting anything inappropriate. Photo: Benjamin Hoste for The Wall Street Journal

School is almost out and parents know what that means: no homework, later bedtimes and kids who want to bend the rules on screen time.

During those long summer days, parents worry about how to make sure kids aren't getting into trouble online. There are tools available that can monitor every picture, email and text message a kid sends or receives—even every Google doc a child creates—and alert parents at any sign of mischief. But at what point do you cross the line from parental duty to police state?

It's not always an easy call.

As soon as her 11-year-old son Tyler got his first phone in February, Jana McDonough made a habit of checking it daily. She also followed him on Instagram and Snapchat. A few weeks ago she came across a photo he posted on Instagram of a new gun he'd gotten in the videogame "Fortnite." She asked him to remove it.

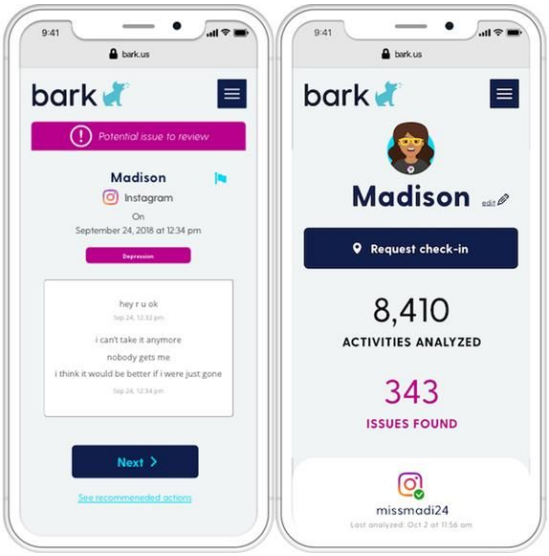
"He didn't understand why I didn't want him to post it. I know he did it innocently, but to me it felt inappropriate," she said. Tyler agreed to delete it.

The hands-on approach only lets you intercept so much. Kids can hide apps in folders on their phone, post to fake Instagram accounts or use burner phones to avoid detection.

Ms. McDonough, a publicist from Thornwood, N.Y., considered using Bark, an app that monitors everything from posts made on social media to texts sent to friends. For $9 a month, it scans for evidence of bullying, sexual content, drug use, violence, depression and predators.

Its sophisticated AI can detect not just key words but the nuance in messages kids send to each other. For example, if a kid tells a friend that he wants to take a "yellow school bus," Bark's AI understands that could be slang for taking a large Xanax pill.

In a one-week period in May alone, out of 737,000 alerts Bark said it sent to parents, 2,500 were about kids expressing feelings of severe depression and 38 were about comments involving imminent plans of self-harm. On average, parents receive three to four alerts a month per child. The alerts contain the worrisome portion of the child's message along with a timestamp and other details.



Bark is an app that allows parents to receive notifications if their child has said anything worrisome in texts or on social media. When Bark's AI finds something potentially troubling, such as a language that signals depression, it sends the parent an alert, along with a snapshot of the message or post and where it was stated. Photo: Bark.us

Since the app launched in the fall of 2015, Bark says it has detected 16 school-shooting threats that law-enforcement officials deemed credible. The app now has 3.5 million users.

"We don't give parents full, unfettered access to read all of their kids' messages. We enable a parent to get a higher level of awareness while preserving a level of privacy for the child," said Bark Technologies Inc. CEO Brian Bason.

There's a hitch: Bark requires parents to enter the passwords to their kids' social-media accounts.

Ms. McDonough's son Tyler claimed he couldn't remember any of his passwords. Plus, he balked at the idea.

"I found that my kid is more willing to let me look at his phone than to give me all his passwords, which he could change anyway," she said.

Besides, cybersecurity experts say handing over passwords to a company is concerning in an age of hacking, no matter how trustworthy you deem that company.

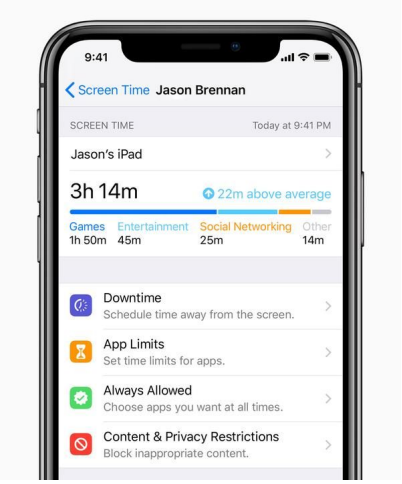
"I'm always nervous about any service provider that wants my password. That's fundamentally insecure," said Lorrie Cranor, a professor at Carnegie Mellon University and director of its CyLab Usable Privacy and Security Laboratory.

"We use the most stringent layers of security," said Bark's marketing chief Titania Jordan. "Nothing is 100%, but the risk of a child encountering something problematic online is way higher than the risk of their data being hacked."

Other apps that monitor kids' texting or browsing history include SaferKid and FamiSafe, yet few offer the same breadth or granularity of monitoring as Bark.

Many parents feel that level of monitoring goes too far. Some parents simply don't want to know all the details of their kids' personal lives. Prof. Cranor, a mother of three teenagers, doesn't use any monitoring or control tools. She'll occasionally look over her

kids' shoulders to see what they're doing and she keeps an eye on her phone bill to see who they're texting.
"I'm sure they look at things I'd prefer them not to, but my instinct tells me most things aren't extremely terrible," she said.
So what can parents do to make sure kids are safe and behaving appropriately online? Have ongoing conversations about technology, says Liz Repking, founder of Cyber Safety Consulting.
"I have clients who want me to set up their house with controls and I tell them, 'This is parenting, you can't outsource it.' If parents want to use parental-control tools, they have to understand that they're not foolproof," she said.



Some cybersafety experts say Apple's Screen Time feature, introduced in iOS 12, is a good way for parents to start monitoring their kids' online activity because it allows them to restrict the apps kids can download, limit the amount of time kids can spend on apps and shut off the phone itself at night. Photo: Apple
Ms. Repking said Apple's Screen Time feature, introduced in iOS 12, is a good starting point because it allows parents to restrict the apps kids can download, limit the amount of time kids can spend on apps and shut off the phone itself at night. Parents whose children use Android devices or Chromebooks can also set controls and screen time limits.
Rebecca Woan keeps tabs on the apps her 14-year-old son, Cameron, downloads. He'd burned through $125 in iTunes gift cards from Christmas on videogame in-app purchases. "We felt that was a waste of money," Ms. Woan said.
Ms. Woan, who owns an insurance agency in Chicago, used to use Circle, a parental-control device and app. It limited the amount of time her son and daughter, now 18, could spend on their iPads when they were younger. But her son would just unplug it.
"I was offended that she felt she had to turn off the Wi-Fi for me and my sister instead of just asking us politely," Cameron said. He remembers going into the app on her phone and changing the settings to allow for unlimited Wi-Fi access.
Circle Media Labs Inc. in April came out with the upgraded $129 Circle Home Plus that notifies parents when the device is unplugged and switches to battery. (There's also a $10 monthly fee after a year.) Still, enterprising children can always find workarounds.

Circle Media Labs Inc. in April came out with Circle Home Plus, an upgraded version of its parental control device that notifies parents when the device is unplugged and switches to battery. Photo: Circle Media

“We can’t solve everything,” said Gwen Smith, vice president of marketing at Circle, adding that parents should be talking to their children about tech use and not just relying on the device.

Ms. Woan now checks her son’s iPhone every morning and glances at his texts. Since her daughter is now in college, she no longer monitors her online activity.

Cameron said his parents have every right to check his phone. “It’s always in the back of my head to make sure I stay clean on my phone because my parents can see what I do,” he said.

For Ms. Woan, the checks are her way of protecting Cameron. “My hope is to create an environment that allows him to make some mistakes, but to avoid serious mistakes from which he can never recover.”

The Dos and Don’ts of Monitoring Your Kids Online

Don’t view the task of monitoring your children online as a tech issue.

Do view it as a parenting issue. Experts advise parents to approach their children’s online activity as they would any other concern, such as underage drinking. “Do you go to every party and watch them? You don’t. You educate them about how to get out of a tough situation and what the consequences are,” said Ms. Repking of Cyber Safety Consulting.

Don’t use the word “trust” when explaining why you’re monitoring their online activity. “A lot of parents talk about trust and privacy and those are dangerous words with kids because they use those as weapons. They’ll say, ‘Mom, you don’t trust me’ and you want to respond immediately with ‘Of course I trust you,’” Ms. Repking said.

Do use the word “independence” when explaining that you are monitoring them until they gain more independence in their digital lives.

Don’t wait until something bad happens online to begin monitoring your child because

suddenly the child will feel like he's under house arrest, Ms. Repking said.

Do start out with some basic monitoring as soon as your children get a phone so that they understand from the get-go that they don't have complete freedom online. "It's much easier to do it when they have nothing to hide. Don't wait until they're a sophomore in high school," Ms. Repking said.

Don't sneak around and monitor your children without their knowledge.

Do have ongoing conversations with your children about appropriate technology use, starting before they get their first phones. Once you begin monitoring their activity, be transparent about it.

Write to Julie Jargon at julie.jargon@wsj.com