How to Protect Your Online Privacy

There are ways you can protect your privacy online and limit the "behavioral surplus data" collected about you.

Robert Epstein, senior research psychologist for the American Institute of Behavioral Research and Technology, recommends taking the following steps to protect your privacy:

1. Use a virtual private network (VPN) such as Nord, which is only about $3 per month and can be used on up to six devices. In my view, this is a must if you seek to preserve your privacy. Epstein explains:

"When you use your mobile phone, laptop or desktop in the usual way, your identity is very easy for Google and other companies to see. They can see it via your IP address, but more and more, there are much more sophisticated ways now that they know it's you. One is called browser fingerprinting. This is something that is so disturbing. Basically, the kind of browser you have and the way you use your browser is like a fingerprint. You use your browser in a unique way, and just by the way you type, companies now can instantly identify you. Brave has some protection against a browser fingerprinting, but you really need to be using a VPN. What a VPN does is it routes whatever you're doing through some other computer somewhere else. It can be anywhere in the world, and there are hundreds of companies offering VPN services The one I like the right now is called Nord VPN. You download the software, install it, just like you install any software. It's incredibly easy to use. You do not have to be a techie to use Nord, and it shows you a map of the world and you basically just click on a country. The VPN basically makes it appear as though your computer is not your computer. It basically creates a kind of fake identity for you, and that's a good thing. Now, very often I will go through Nord's computers in the United States. Sometimes you have to do that, or you can't get certain things done. PayPal like you to be in a foreign country for example."

Nord, when used on your cellphone, will also mask your identity when using apps like Google Maps.

Do not use Gmail, as every email you write is permanently stored. It becomes part of your profile and is used to build models of you, which allows them to make predictions about your line of thinking and every want and desire.

Many other older email systems such as AOL and Yahoo are also being used as surveillance platforms the same way as Gmail. ProtonMail.com, which uses end-to-end encryption, is a great alternative. The basic account is free.
Don't use Google's Chrome browser, as everything you do on there is surveilled, including keystrokes and every webpage you've ever visited. Brave is a great alternative that takes privacy seriously.

Brave is also faster than Chrome, and suppresses ads. It's based on Chromium, the same software infrastructure that Chrome is based on, so you can easily transfer your extensions, favorites and bookmarks.

Don't use Google as your search engine, or any extension of Google, such as Bing or Yahoo, both of which draw search results from Google. The same goes for the iPhone's personal assistant Siri, which draws all of its answers from Google.

Alternative search engines suggested by Epstein include SwissCows and Qwant. He recommends avoiding StartPage, as it was recently bought by an aggressive online marketing company, which, like Google, depends on surveillance.

Don't use an Android cellphone, for all the reasons discussed earlier. Epstein uses a BlackBerry, which is more secure than Android phones or the iPhone. BlackBerry's upcoming model, the Key3, will be one of the most secure cellphones in the world, he says.

Don't use Google Home devices in your house or apartment — These devices record everything that occurs in your home, both speech and sounds such as brushing your teeth and boiling water, even when they appear to be inactive, and send that information back to Google. Android phones are also always listening and recording, as are Google's home thermostat Nest, and Amazon's Alexa.

Clear your cache and cookies — As Epstein explains in his article:

"Companies and hackers of all sorts are constantly installing invasive computer code on your computers and mobile devices, mainly to keep an eye on you but sometimes for more nefarious purposes. On a mobile device, you can clear out most of this garbage by going to the settings menu of your browser, selecting the 'privacy and security' option and then clicking on the icon that clears your cache and cookies. With most laptop and desktop browsers, holding down three keys simultaneously — CTRL, SHIFT and DEL — takes you directly to the relevant menu; I use this technique multiple times a day without even thinking about it. You can also configure the Brave and Firefox browsers to erase your cache and cookies automatically every time you close your browser."

Don't use Fitbit, as it was recently purchased by Google and will provide them with all your physiological information and activity levels, in addition to everything else that Google already has on you.