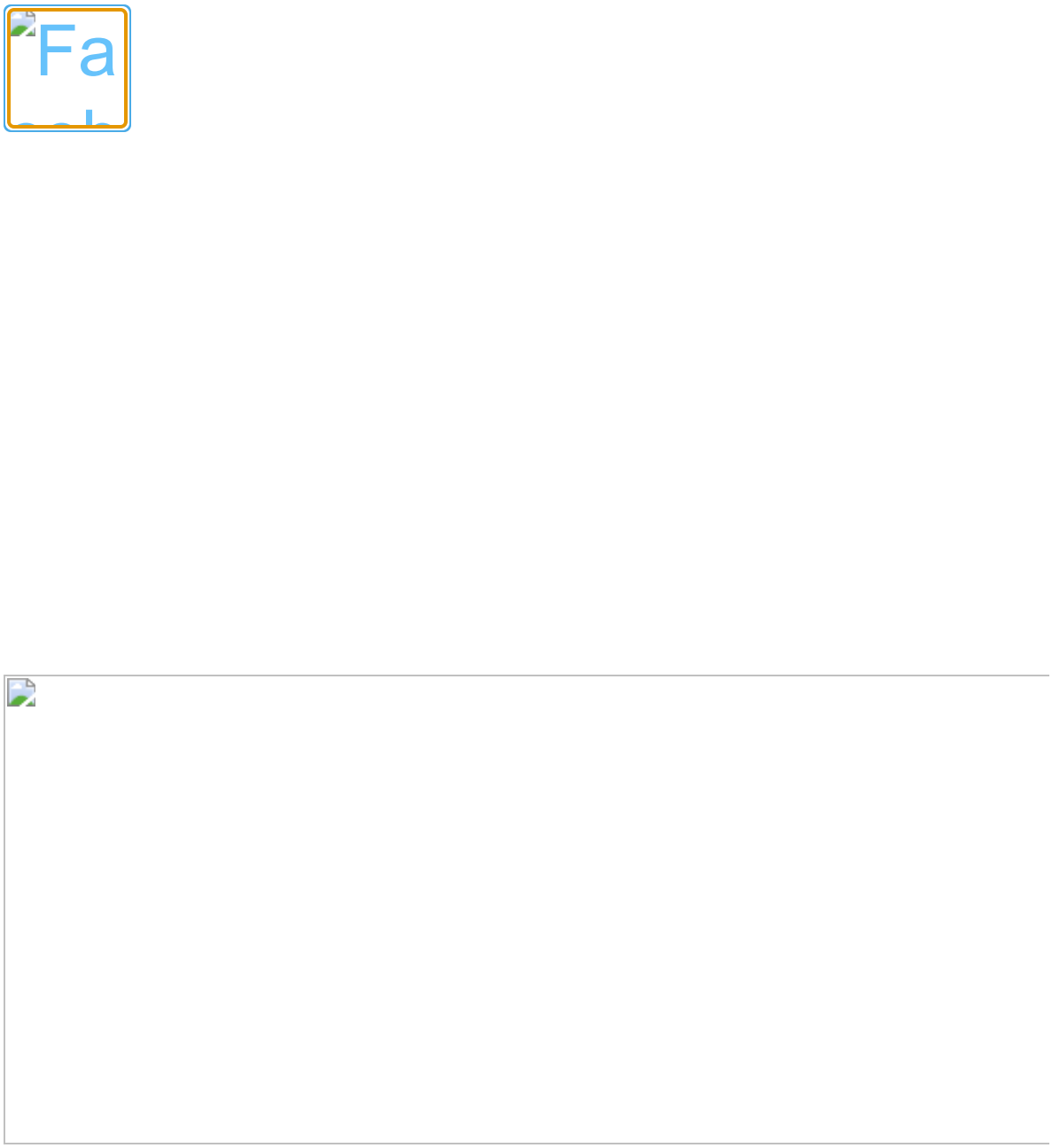
How you're tracked online and what you can do about it

Facebook Employees in an Uproar Over Executives Leaked Memo (nytimes.com)

submitted 1.1 days ago by One-Way_Bus to **news** (**+5**|**-0**)

3 comments



The Associated PressFILE - In this Wednesday, Nov. 27, 2013, file photo, a passenger looks at his smartphone while waiting in the security line at Hartsfield-Jackson Atlanta International Airport, in Atlanta. Though Facebook gets all the attention, the social media service isn't the only company to collect massive amounts of data on you to help marketers sell their goods and services. Google, for one, also does extensive tracking to power its advertising engines. There are ways to block or minimize such tracking, but they come with trade-offs. (AP Photo/David Goldman, File)

Though Facebook gets the attention because of a recent

privacy gaffe, the social network is far from alone in collecting massive amounts of data on you to help marketers sell you stuff.

Google, for one, also does extensive tracking to power its advertising engines. And many other websites and apps run ads sold by Facebook and Google and exchange data with them. Beyond that, plenty of services including Uber and Amazon keep detailed histories on you.

Here are some of the ways to block or minimize such tracking — but they come with trade-offs.

TRACKING IDs

Websites have long used unique IDs in "cookies" — data files stored in your browser — to know it's you when you return a week later. Cookies also let advertising networks run by the likes of Facebook and Google connect you as you visit multiple websites. Phones and tablets have a device advertising ID that apps can use to track you.

> Combatting this: You can reset the cookie ID by clearing cookies periodically. Most browsers also have a private mode to limit tracking through cookies, though it's not foolproof. Companies can still link you if you've signed in, for instance. As for the device ID, you can reset that or tell advertisers not to target ads through the phone's settings.

Many browsers also let you install add-ons that block ad trackers. Notable add-ons include Ghostery or the Electronic

Frontier Foundation's Privacy Badger.

The trade-offs: You'll still get ads, just not targeted ones. And clearing cookies makes your browser forget who you are, so you'll have to sign back into any site that was saving your login. Tracker blockers can sometimes prevent websites from displaying or working properly.

LOCATION SERVICES

Many apps need your location to work. Mapping apps, for instance, can't tell you when to turn without knowing where you are. Video services typically have rights only in certain countries and need to verify your location. But location can be used for much more. Google, for instance, keeps a fairly detailed account of your whereabouts through a feature called Timeline.

Combatting this: You can turn off location services in the phone's settings, though for apps to work property, it's better to turn them off for specific services that don't really need them. As for Timeline, you can pause or delete location history in Google settings.

The trade-offs: Some apps won't work without your location. Others, such as weather apps, will require you enter your location manually. And you might miss out on recommendations such as better commuting routes via apps like Waze.

SIGNING IN

Signing into an online account gives services a sure-fire way of tracking you. Facebook won't work at all without an account; Google merely works better with one. And you'll generally need an account with any service that charges you, although sometimes you can sign in with your Facebook or Google ID instead.

> Combatting this: Resist creating an account or signing whenever you can — such as when you're merely browsing rather than buying. Avoid using Facebook or Google IDs whenever possible, as those companies could then track you. You can also use a different email address for each account to frustrate efforts to connect you across services, although it can be a major pain.
>
> The trade-offs: Some services require signing in, and creating accounts on each service means more passwords to remember (though you might consider using a password manager). Whatever you do, don't reuse the same passwords across service; that makes them easy to hack.

IP ADDRESS

The Internet Protocol address lists where your phone or computer lives on the internet; it's how you get messages and load websites. But IP addresses can also help companies remember who you are and link the various devices you use,

since most homes use a single IP address for the whole network. Databases can also map IP addresses to physical locations.

> Combatting this: You can mask your IP address by using a secure intermediary. VPN services, common in corporate settings, will route your traffic through a separate IP address; a secure web browser called Tor automatically sends traffic through multiple third parties. You still need to avoid signing in.
>
> The trade-offs: Tor can slow down performance, particularly with high-data tasks such as video. And with VPNs, you need to trust the VPN operator, whether that's your boss or a private service.