The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers

Mark Hachman, Senior Editor, PCWorld , Oct 1, 2015

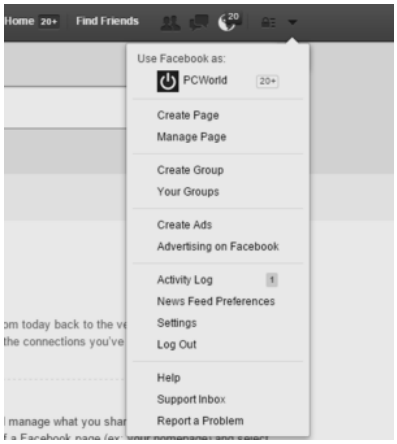
Here's what popular services like Apple, Google, Facebook, and Microsoft collect -- and what you can do about it.

Jumping from Windows 7 directly to Windows 10 has to be something like a farmer visiting Times Square. Live Tiles flash and move. A nice assistant named Cortana always hovers nearby. Click on the wrong spot and you could be whisked away elsewhere on the Web. And there are always people asking who you are, where you live, what you like...
Because the latest version of Windows is always asking for information in the guise of being helpful, it's easy to think that Microsoft's the poster child for the collective attack on your digital privacy. But it's not.
In fact, there are plenty of other companies who feel perfectly entitled to require you to hand over your personal info before they open their doors. On a day where Microsoft clarified what it does with your data to try and soothe your fears, a Bloomberg feature profiled Facebook's "unblockable" ads, while a new Google program revealed that advertisers can now tune ads to who you are just by knowing your email address.
This is the price of free: free email, free operating systems, free connecting with friends, free search. And while Microsoft has thrown itself on the ground, begging for forgiveness, you can make the argument that other companies are doing as much or more to mine your data. Let's take a look.

Facebook

"...Facebook trackers are just about everywhere on the Internet. But because most of Facebook's 1.49 billion users routinely access the service through an app, the ads cannot be hidden using one of the many blocker tools now topping the download charts on Apple's App Store." - Bloomberg

At this point, Facebook represents its own self-contained ecosystem. Want to share baby pictures? Ping a friend to meet up after work? Chances are that you're making those connections on Facebook—connections that Facebook knows and can exploit for its gain.



Track your own history with Facebook's Activity Log.

The latest? Facebook is now pitching a program by which advertisers can market their products across TV and Facebook as a unified whole, so that a trailer for the latest James Bond movie, for example, might run at halftime of "Monday Night Football"—or on news feeds of users who have "liked" a previous Bond flick. And if that's not enough, advertisers will also gain the power to poll you about what you thought of them.

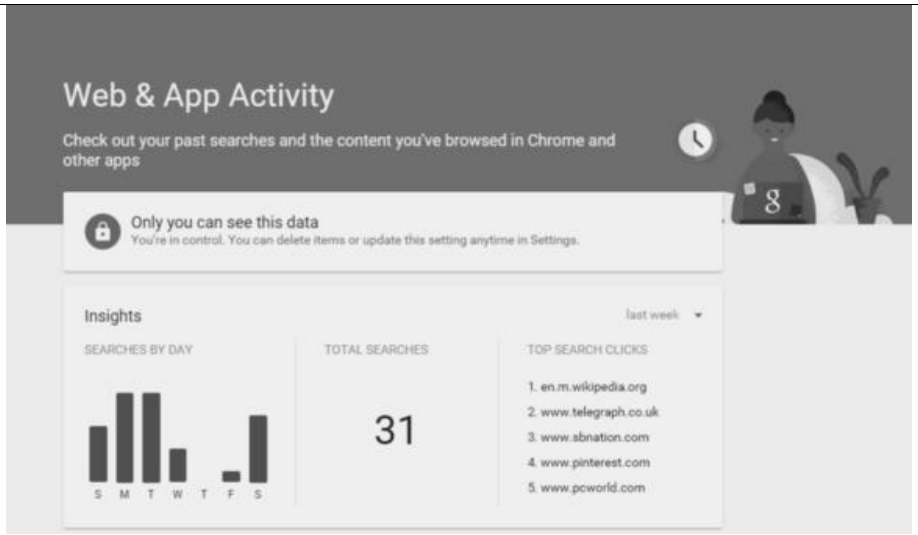
What information does Facebook collect? It's no secret that there's little "privacy" in Facebook's privacy policy. Here's a snippet:
"We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities."
Facebook knows your friends, what information you provide about them, what they say about you, what other sites you visit (if they include a Facebook "like" button, which most do), what you bought, what device you used to access Facebook, and much more.

What can I do about it? It's an amazing amount of information, although you can download it all right here, using Facebook's Download Your Information tool. You can also check your Activity Log to see exactly what you've done since you've joined the service. Note that the latter choice is far less complete than the Download Your Information tool. You can also delete your account, but Facebook reserves the right to keep information that others have shared about you. Because to Facebook, that information isn't yours.

Google

Google has become the de facto name in search (although I've since switched to Bing) and Gmail, Google Maps, and its other services now rank among the leaders in those categories. But all that "free" adds up to a huge amount of your personal information being traded away to create personalized, targeted ad experiences.

The latest? Google has launched a program by which your profile is now keyed to your email address. Dubbed Customer Match, the program ensures that an advertiser's "brand is right there, with the right message, at the moment your customer is most receptive," Google promises. So if you've previously asked a travel site to send information to your Gmail address, that site can sign up for Customer Match. Then when you're watching YouTube, that site "can show ads that inspire them to plan their next trip."



Google buries information about what you do on the Web all over this place, including your Search History. But does anyone ever bother digging it up?

Earlier this month, Google added native Gmail ads for all of its AdWords customers, meaning that you'll end up with interest-based advertising in your inbox unless you opt out.

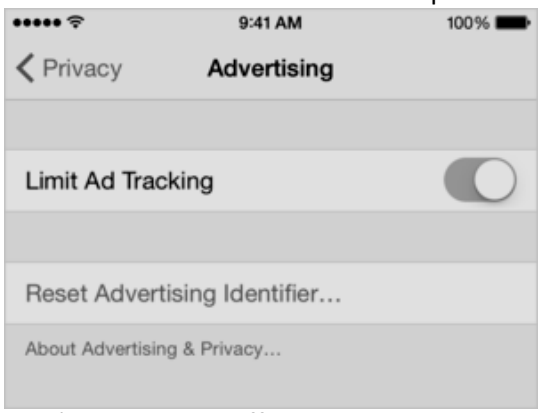
What information does Google collect? As with Facebook, there's a ton: name, email address, telephone number, credit card (if you enter it), details on how you use Google's services, how you interact with other websites that use AdWords and other Google technologies, your device, search queries—the list goes on and on. Google will also store information in your browser via local browser storage—that goes beyond the snippets of code commonly referred to as "cookies". And if your information is "public," it's fair game. "If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo," the policy states.

If there's one thing that I don't see in Google's privacy policy, it's a portion that's specific to Android.

What can I do about it? Google actually allows quite a bit of freedom to tailor what information you provide to it—although it's betting that just a tiny fraction of you will ever access it, let alone limit that information. But it's all here in the Google privacy policy: tweaks to allow you to turn off location tracking, voice searches, and other features; viewing and editing your preferences; adjusting your public profile; and much more. And you can download Google's data hoard, too.

Apple

Apple may have said that it's making it very clear how it's using your data, but you'll probably agree the way it does so is far more obtuse than the other companies we've listed here.



Here's how to turn off ad tracking in iOS9...

The latest? The news surrounding Apple isn't so much how it's using your data, but how it's preventing content companies from having the same access. Its controversial ad blocking technology built into the latest version of iOS 9 has roiled the advertising and media world alike. Part of this, of course, is that Apple makes the majority of its sales on hardware and app sales—not advertising—so it can take the high road.

What information does Apple collect? Apple's "privacy policy" can be summed up in three words: "We're for it." The policy doesn't do a great job explicitly listing what information it collects, most of it goes into more detail into what it doesn't collect. In all fairness, Apple appears to do a good job linking your preferences to an intermediary, anonymous series of ID numbers (sometimes linked to the Siri digital assistant) rather than "knowing" it is you.

...and in iTunes.

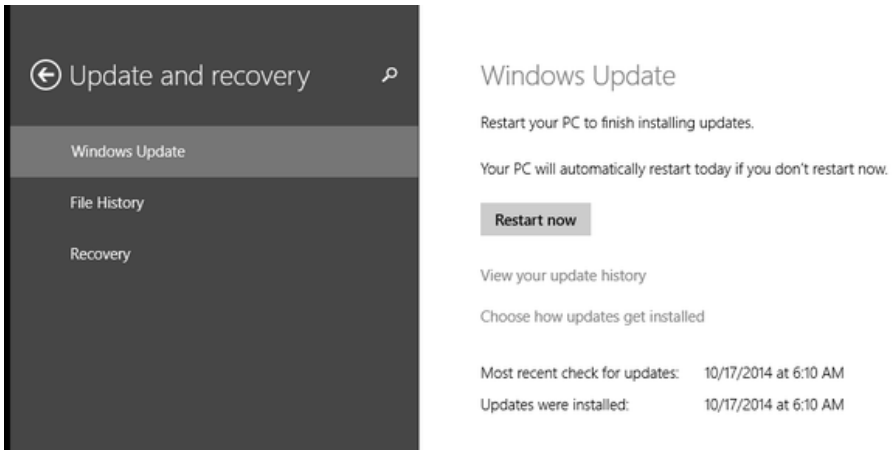
Apple does say, however, that it will collect certain information such as your name, contacts, and songs in your music library, and send them to Apple servers using encrypted protocols.—including your location, if that service is turned on. And your iPhone sends your anonymized location and calendar information, so it can predict when you'll have to leave to make your next appointment. Apple Music also links your preferences to an anonymous ID, and the News app uses your reading preferences to supply ads within the app.

What can I do about it? For all of its holier-than-thou attitude towards advertising, Apple doesn't put the process to opt out of targeted advertising front and center. Time and again, Apple says that you can reset the identifier it uses to link you to the content you want to see, or opt out; however, that process is left to the user to discover for himself or herself.

Microsoft

Microsoft's a bit different than Facebook, for example, in that it owns your operating system as well as its associated services. That means that it can peer into your OS and discover that a particular graphics driver was at fault. Allowing

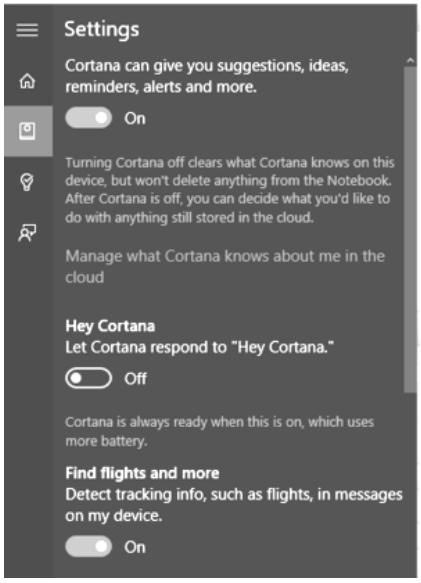
Microsoft to see what's inside your PC isn't always the worst idea, as updates can be tailored to your PC's particular hardware.



Microsoft admits to collecting information to personalize your experience, but says it does not scan your email to collect that. "Unlike some other platforms, no matter what privacy options you choose, neither Windows 10 nor any other Microsoft software scans the content of your email or other communications, or your files, in order to deliver targeted advertising to you," Microsoft senior vice president Terry Myerson wrote in a blog post.

What information does Microsoft collect? Microsoft also does a good job comprehensively spelling out what information it collects: name and contact data, credentials, demographic data, payment data, and more. But don't buy the line that Microsoft doesn't read your email—the privacy policy states very clearly that it does. It not only reads the subject line and body of an email, but also the text or other content of an instant message, the audio and video recording of a video message, and the audio recording and transcript of a voice message you receive or a text message you dictate. It just doesn't sell ads against it.

There's also an additional layer of input that Microsoft samples, because it is an OS.



If you'd like, you can turn features like Cortana off.

"Additionally, your typed and handwritten words are collected to provide you a personalized user dictionary, help you type and write on your device with better character recognition, and provide you with text suggestions as you type or write. Typing data includes a sample of characters and words you type, which we scrub to remove IDs, IP addresses, and other potential identifiers. It also includes associated performance data, such as changes you manually make to text as well as words you've added to the dictionary."

What can I do about it? For a comprehensive primer, please refer to Ian Paul's guide to reclaiming your privacy in Windows 10, piece by piece, as well as Lincoln Spector's tip about turning off the Windows keylogger.

And that's just some if it.

Yes, your privacy is for sale: One of Robert A. Heinlein's most famous contributions to popular culture was an acronym: TANSTAAFL—There Ain't No Such Thing As A Free Lunch. That certainly goes for today's online services. Bing, Outlook, Gmail, Yahoo Mail, and the like—they may not cost you a dime, but they're not free. The only sure way to avoid paying is to surf anonymously, never buy a smartphone, and never take advantage of a free Web service that you have to log into.