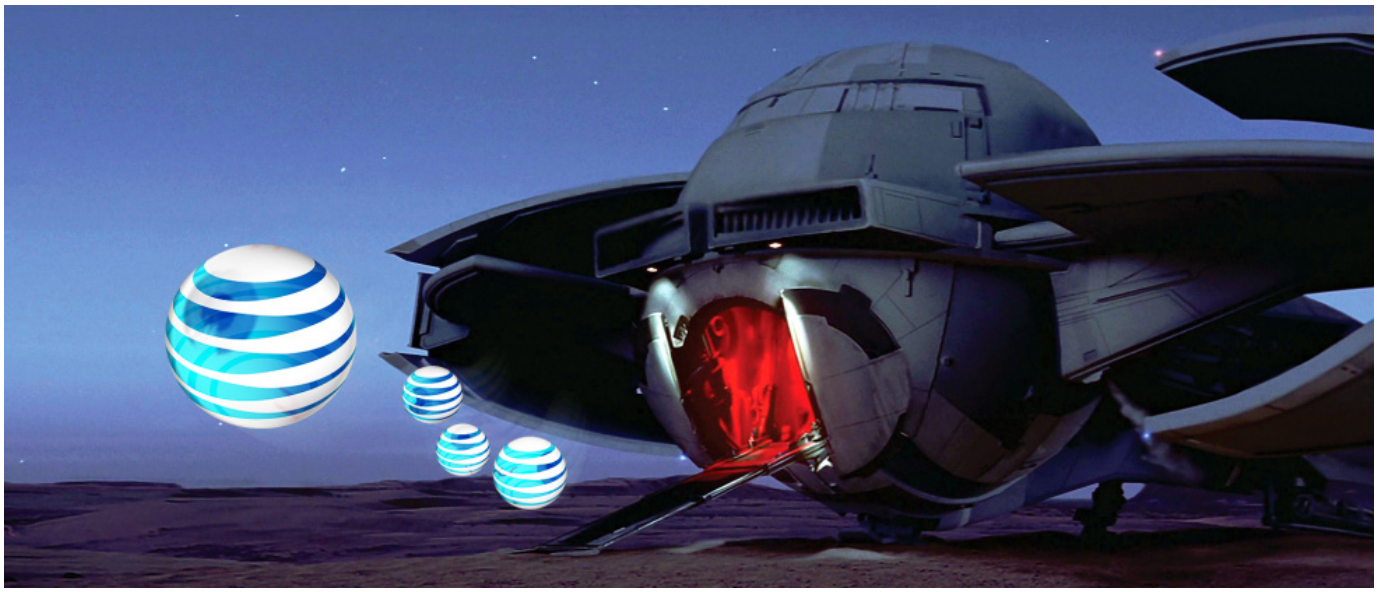
TECHNOLOGY LAB —

AT&T's plan to watch your Web browsing—and what you can do about it

Want to opt out? It could cost up to $744 extra per year.

JON BRODKIN - 3/27/2015, 9:00 AM



Aurich vs Star Wars

Enlarge

If you have AT&T's gigabit Internet service and wonder why it seems so affordable, here's the reason—AT&T is boosting profits by rerouting all your Web browsing to an in-house traffic scanning platform, analyzing your Internet habits, then using the results to deliver personalized ads to the websites you visit, e-mail to your inbox, and junk mail to your front door.

In a few select areas including Austin, Texas, and Kansas City, Missouri—places where AT&T competes against the $70-per-month Google Fiber—Ma Bell offers its own $70-per-month "GigaPower" fiber-to-the-home Internet access. But signing up for the deal also opts customers in to AT&T's "Internet Preferences" program, which gives the company permission to examine each customer's Web traffic in exchange for a price that matches Google's.

AT&T charges at least another $29 a month ($99 total) to provide standalone Internet service that *doesn't* perform this extra scanning of your Web traffic. The privacy fee can balloon to more than $60 for bundles including TV or phone service. Certain modem

FURTHER READING
AT&T charges $29 more for gigabit fiber that doesn't watch your Web browsing

rental and installation fees also apply only to service plans without Internet Preferences.

FURTHER READING
AT&T offers gigabit Internet discount in exchange for your Web history

It wouldn't be accurate to say that paying extra gives customers "enhanced" privacy; paying those monthly fees that add up to hundreds of dollars more per year simply provides the same level of privacy customers would get from other Internet providers, or from AT&T's slower DSL and fiber-to-the-node services.

AT&T says Internet Preferences tracks "the webpages you visit, the time you spend on each, the links or ads you see and follow, and the search terms you enter." This helps AT&T serve ads targeted to each user based on that person's interests. And advertisers are willing to pay more when they know their ads will be shown only to the people most likely to be interested in their products.

Because AT&T can see almost everything you do online, no matter what websites you visit, the company may be in even better position to serve targeted ads than Web behemoths like Google and Facebook. While Google apparently doesn't impose anything similar to Internet Preferences on its fiber Internet, the company's cable service is delivering targeted TV ads based on its customers' viewing history.

As a side note, AT&T's best pricing may not be available in cities where it doesn't compete against Google Fiber. In Dallas, where Google Fiber hasn't arrived, AT&T was charging $120 a month for gigabit service and still requiring the customer to opt in to Internet Preferences.

"AT&T watches everything"

Some Ars readers think AT&T has gone too far. "Google watches you use Google services, AT&T watches everything and only matches Google's price. Scumbag AT&T," Ars forum member arkiel wrote.

"A customer may receive an ad or a promotion on behalf of an advertiser—through an ad network placement on a website or otherwise," an AT&T spokesperson told Ars. "Customers' personal information is never given to that advertiser."

The personalized offers don't just appear on websites, they also come "via e-mail or through direct mail," AT&T says. "If you search for concert tickets, you may receive offers and ads related to restaurants near the concert venue. After you browse hotels in Miami, you may be offered discounts for rental cars there. If you are exploring a new home appliance at one retailer, you may be presented with similar appliance options from other retailers... if you search for a car online, you may receive an e-mail notifying you of a local dealership's sale."

You can't opt out from AT&T's e-mail spam without paying the higher price, so worried customers should make sure not to give AT&T a preferred e-mail address. "Based on your consent to receive ads and offers through AT&T Internet Preferences, we will continue to send you marketing e-mails related to the program. You may opt-out of receiving these e-mails by choosing not to participate in the AT&T Internet Preferences and switching to GigaPower Standard pricing," AT&T says.

AT&T describes Internet Preferences as "opt-in," but its website advertises the lower price without mentioning the traffic scanning unless you click "See offer details." Even then, you have to click another link to find out what Internet Preferences actually is. Take a look:

AT&T's advertised prices are the lower ones that require customers to opt in to Internet Preferences, AT&T's program that examines its customers' browsing and serves personalized ads. But nothing on the home page makes that clear.

Is it legal?

US laws against wiretapping have exceptions for cases in which there is "consent." If Internet Preferences was ever challenged in court, the question would be whether AT&T's disclosures and opt-in system provide enough information to users.

"There are always questions about consent being willful and informed," Electronic Frontier Foundation (EFF) Senior Staff Attorney Lee Tien told Ars. "The reason legally it's important is under

federal law it won't be unlawful for them to look at this stuff if you consent to them looking at it."

Federal regulators could examine the program to see whether it breaks privacy laws, but "AT&T has tried very hard to cover its bases" by disclosing the basic parameters of the data collection, Tien said. "I think they've done a decent job... they would have an argument that they have made reasonable disclosures. I think that someone challenging it would have arguments that they didn't really get consent in the right way."

AT&T's website certainly pushes customers to opt in to Internet Preferences. Even if you read the disclosures and understand exactly what Internet Preferences consists of, declining the offer makes Internet, TV, and phone service significantly more expensive.

To find out exactly how much it costs to opt out of traffic scanning and personalized ads, you have to go through AT&T's checkout process. GigaOm's Stacey Higginbotham tested this last month and found that for bundled services including TV, the privacy fee was actually as high as $66 per month.

Prices change over time. When testing this out directly last week, we found price differences ranging from $29 to $62 a month—up to $744 a year. But it's actually worse than that. Only service with Internet Preferences can be hooked up without installation or activation fees. Declining Internet Preferences thus adds another $49 or $99 in up-front costs.

Additionally, service with Internet Preferences comes with a three-year price guarantee (with a one-year contract required). There is no such guarantee without Internet Preferences, so AT&T could raise your bill whenever it wants.

One Ars reader viewed the lack of a one-year commitment as a positive: "[T]he surcharge also eliminates the annual contract requirement," TexasFight wrote. "I refuse to sign up for GigaPower for a year at a time, so I pay the surcharge." Still, the pace at which Internet and TV prices rise makes three-year price guarantees attractive to many consumers.

JUMP TO END PAGE 1 OF 3

One reason the true price difference is more than $29 a month is that Internet Preferences customers get the modem and wireless gateway at no extra charge; opting out requires paying extra for equipment, which AT&T will supply for another $7 a month. There is another charge for getting video in high definition instead of standard, a perk that comes for free with Internet Preferences. HBO and HBO GO are also included with Internet Preferences but cost extra without.

A Triple Play package with HD and HBO that costs $150 a month with Internet Preferences costs $212 a month plus a $49 activation fee without Internet Preferences. Here's how the pricing differences stack up:

Standalone Internet service without personalized advertising costs $29 more per month, plus an additional $7 equipment and a $99 one-time installation fee.

Deep packet inspection

Changing browser settings won't keep your Web browsing private.

"AT&T Internet Preferences works independently of your browser's privacy settings regarding cookies, do-not-track, and private browsing," the company says. "If you opt-in to AT&T Internet Preferences, AT&T will still be able to collect and use your Web browsing information independent of those settings."

So how exactly is AT&T scanning the traffic of its GigaPower customers? While the company is vague on those details, some experts say AT&T may be using deep packet inspection, technology used for everything from preventing the spread of computer viruses to tracking down criminal hackers and terrorists.

If AT&T is your Internet provider, your traffic has to go through AT&T systems before reaching the rest of the Internet. There's no changing that whether you opt in to or out of Internet Preferences. But the

AT&T website's description of Internet Preferences indicates that customers' traffic makes one extra stop within AT&T's network.

"Using the IP address assigned to each GigaPower account, AT&T scans for your AT&T Internet Preferences election," the company says. "AT&T will treat your Internet browsing activity in accordance with your election. If you chose to participate in the AT&T Internet Preferences program, your Internet traffic is routed to AT&T's Internet Preferences Web browsing and analytics platform."

The statement that AT&T is re-routing traffic to a special platform "to me is the red flag that says deep packet inspection," EFF Staff Technologist Jeremy Gillula told Ars. Gillula continued:

> This is the one time when the post office analogy works pretty well for the Internet, when you're transmitting data back and forth it has some header information that describes where it's going. It might say roughly what the contents are. You could think of it as media mail vs. parcel post vs. first class or something... These are the sorts of things that show up in the headers that ISPs usually look at when they're figuring out where to send your traffic.
>
> But deep packet inspection is as if the post office would open up your mail and look at the letters or look at, 'what does this package contain. Look, he ordered a new Xbox from Amazon or something like that, maybe he wants to buy an Xbox game now, so let's show him ads for that.' It really is about looking at the inside of the content of your communications.

GigaPower with Internet Preferences launched in Kansas City on February 16 this year. AT&T has declined to make anyone available for a phone interview since then. While the company answered some of our questions over the past few weeks, AT&T did not tell Ars whether it is using deep packet inspection, and the company declined to provide any further description of the technology it uses to collect data.

In 2013 when the service launched in Austin, AT&T said it would "use various methods to collect Web browsing information," without specifying further.

It is possible that AT&T is scanning traffic without using deep packet inspection, according to Lukasz Olejnik, a security and privacy researcher.

"When it comes to the information retrieval of Web use patterns, the publicly available information about [AT&T's] scheme [for] analyzing the user-accessed websites does not suggest the application of any specialized methods such as deep packet inspection," Olejnik told Ars. "This may resemble the (recently ruled as invalid) EU Data Retention law, where ISPs were obliged to store the information about the network connections performed by users—to make them available to any future request from law-enforcement agencies. AT&T will be collecting, storing, and analyzing this data to gain insight about their users."

AT&T says it's looking at everything except encrypted traffic, i.e. sites using HTTPS, "such as when you enter your credit card to buy something online or do online banking on a secure site."

Using Amazon as an example, AT&T might see what products you search for and add to your cart, because that's all done without HTTPS enabled. Amazon creates an encrypted session as soon as you click "proceed to checkout," though, so AT&T can't see what credit card number you type in or verify that you completed a purchase.

But even for HTTPS connections, AT&T may gain information about your browsing habits without trying to break the encryption, because AT&T can see that you're sending HTTPS traffic to a specific website. AT&T may not know with 100 percent certainty what you're buying on Amazon or what you're typing in Gmail, but AT&T can tell if you open an encrypted link to a shopping site and then check your e-mail—perhaps a sign that you just bought a product and are looking for an e-mail confirmation.

AT&T says it uses "appropriate controls to protect customer information."

"If you choose to participate in the AT&T Internet Preferences program, your traffic may be analyzed to assist with tailoring ads and offers," the company told Ars. "We maintain our customers' privacy inside and outside the Internet Preferences program. We have established electronic and administrative safeguards, and we secure our computer storage and network. We apply encryption or other appropriate controls to protect customer information, and we limit access to only those with jobs requiring access."

Why privacy experts are alarmed

Using the Web often entails sacrificing a bit of privacy, but AT&T's program has alarmed even jaded privacy experts.

An Internet service provider keeping track of your Web browsing in order to serve personalized ads is more concerning than a website doing so, Kenneth White, a security researcher and co-director of the Open Crypto Audit Project, told Ars.

"There is a strong expectation that my ISP is the transport layer and not trying to monetize that."

"If people go to Facebook or Google or Pinterest or whatever and they search for consumer stuff, there is a common expectation that the business model is funded by ads. I think everybody recognizes that," White said. "But when I'm at home and I go to WebMD... there is a strong expectation that my ISP is the transport layer and not trying to monetize that. I think it's very

different. I think it's a very dangerous place to go when consumer websites that are ad-driven become the model our basic Internet connectivity is based on."

Our readers agree. "Wow. They actually put a dollar value on privacy," Ars forum member rick*d wrote. "The problem with this is that I don't trust AT&T to not spy on me anyway, even if I pay them not to. What proof does the customer have? Does AT&T grant them access to their database and let them search for their (lack of) records? How does AT&T prove they're **not** spying on their customers?"

Perhaps worse for those concerned about such privacy, paying more to opt out of Internet Preferences turns off the most invasive scanning—but not *all* data collection.

"If you chose not to participate in the AT&T Internet Preferences program, your Internet traffic is not routed to the Internet Preferences analytics platform," the company says on its website. "AT&T may collect and use Web browsing information for other purposes, as described in our Privacy Policy, even if you do not participate in the Internet Preferences program."

That privacy policy, which applies to both home Internet and cellular service, says AT&T collects network performance and usage information to analyze "how you use our network, our products and our services, and how well our equipment and network is performing." Additionally, AT&T collects Web browsing information that "tells us about the websites you visit and the mobile applications you use on our network."

AT&T shares data with other entities in order to serve up advertising. "We use and share this information in many ways including research, media analysis, and retail marketing and Relevant Advertising," the privacy policy says.

While AT&T shares personal information for some purposes, such as to comply with court orders and to work with credit bureaus and collection agencies, AT&T told Ars that "Relevant Advertising" relies only on "aggregate information about groups of people to develop advertising that is more likely to be useful to that group." That sets it apart from Internet Preferences, which uses specific information about each user to serve personalized ads.

AT&T also told Ars, "We don't sell your personal information to anyone, for any reason."

JUMP TO END PAGE 2 OF 3

User-tracking systems rare but not unprecedented

Programs like AT&T's Internet Preferences are not unprecedented. Charter, a cable company, planned to implement a similar tracking and advertising system in 2008, but decided not to after facing criticism. A rural provider called CMA Communications apparently inserted ads onto Apple.com and other websites a couple of years ago.

Comcast has been serving Comcast ads to devices connected to its public Wi-Fi hotspots, but not on its home Internet service. Comcast does deliver targeted ads based on viewing history to its TV subscribers.

Verizon Wireless customers' browsing is tracked by an online advertising clearinghouse that "tak[es] advantage of a hidden undeletable number that Verizon uses to monitor customers' habits on their smartphones and tablets," ProPublica reported in January. Verizon later agreed to let customers opt out of the tracking. Verizon also has a "Verizon Selects" service that delivers personalized marketing in exchange for "Smart Rewards" points that can be turned in for prizes. The program is opt-in and there is no fee to avoid joining.

Although AT&T has gone further than its biggest competitors, any Internet provider could track its customers' browsing and use the information to make money on advertising.

"Internet service providers provide Internet connection to end users, and the natural consequence is that it is possible to monitor the network traffic over those channels. In this light, any ISP is capable of performing such analyses," Olejnik told Ars.

"If you're an engineer you know that every ISP has every scrap of data of everything coming in," White said. "They have to manage their networks, they have to on the DNS side, they have to on the attack side, on peering, all of that. It's really not a question of 'do we have your data,' it's which groups in house are going to be able to see that."

Olejnik described in detail what kinds of information Internet service providers could collect about their users:

> According to the information on their website, AT&T will be analyzing the websites accessed by users—the websites, frequency of visits, time spent on them.
>
> Web browsing history conveys rich information about the users' preferences. Methods exist to analyze this data and extract various insight about users and their interests—the content they like. It may be, for example, possible to infer the user's age, gender, even incomes or racial profile, just based on Web browsing history. Consequently, this allows the profiling of users and it can be typically leveraged to target the user with specific advertising content. Similar [profiling] is also possible in the traditional model of Web advertising. However, [an] ISP is in a privileged position due to the potential of controlling virtually all network activities of its users. In particular, ISPs have perfect user identification and tracking capabilities; it is straight-forward to associate a particular network traffic with specific real users.
>
> Moreover, AT&T mentions the possibility of analyzing data "like search terms." Web browsing histories, and in particular search terms, may reveal the users' interests in specific topics, such as medical information. Consequently, by the analysis of user browsing patterns, as well as the typed search terms it may also be possible to infer medical conditions. In these scenarios, users would be advised to use search engines over secured connections (HTTPS).

> Obviously, Internet Service Providers already may possess some information about their subscribers, for example their names, ages, and genders. But they may not have this information relating to the other household members. Since Web browsing histories carry detailed insight, it may be possible to create other versatile analyses. Perhaps it would be possible to distinguish between the particular household residents, since Web browsing patterns can be attributed to particular people. Research shows that Web use patterns of men and women may differ in some circumstances. But this difference can also be attributed to the psychological traits of users, e.g. introverted people may access different websites than extroverted ones. The datasets of users' Web use patterns may certainly offer a lot of possibilities in these regards.

It's all seamless

The "U-verse with AT&T GigaPower" fiber service is available in Austin, Texas; Dallas-Fort Worth; Kansas City; Raleigh and Winston-Salem, North Carolina; and could be coming to dozens more cities. The Internet Preferences data collection program does not apply to AT&T's slower home Internet services, such as DSL and fiber-to-the-node, or its wireless network, although AT&T could extend Internet Preferences to those networks if it wants to.

AT&T customers probably won't notice any differences between service with Internet Preferences and without. "If AT&T hadn't announced this, you wouldn't even necessarily know that they were doing this sort of deep packet inspection," Gillula said.

FURTHER READING
AT&T copies Google, names 100 cities where it could offer gigabit fiber

AT&T told Ars that targeted ads shouldn't appear any differently from regular ads. "Customers will not necessarily receive more ads when online, instead the ads received may be more suited to his/her interests," AT&T said.

AT&T said it isn't replacing ads on non-AT&T websites with its own—that means AT&T isn't hijacking ad requests and redirecting the requests to its own servers. Instead, AT&T works with publishers to book advertising space on websites like any other ad network would, a company spokesperson told Ars. AT&T also said the program uses "ad network placements."

AT&T runs its own ad network for TV ads called "AdWorks." The online advertising portion of the AT&T ad network was reportedly shut down in 2013, but it apparently still exists in some form. Whether AT&T is using AdWorks or purchasing ads for Internet Preferences through a third-party ad network, the company should be able to place its ads without having to resort to Javascript injection or other means.

Just as Internet Preferences ads probably won't look out of place in your browser, running a traceroute isn't likely to reveal that your traffic is being routed to AT&T's analysis system. "It's possible they've set it up so you could actually see that you're being routed through AT&T's boxes first, but it's also entirely technically feasible that they set it up so it's completely transparent and there's no way for you to tell," Gillula said.

Subscribing to a VPN (virtual private network) service would encrypt your traffic before it hits AT&T's servers, preventing the ISP from analyzing it. VPNs can degrade Internet performance because they cause traffic to also travel through the VPN provider's servers, and you have to decide whether you trust the VPN provider more than you trust AT&T. But some Internet users may think a VPN worth the expense.

"One possibility is you sign up for AT&T's $30 discount and then you sign up for a $5-a-month VPN, and you say, 'Screw you, AT&T,'" Gillula said.

White says AT&T hasn't provided enough detail for experts to determine whether it's really protecting customers' privacy.

"We're down to a fairly limited number of ISPs in the US anyway, and there's not been a good track record of those large providers like Comcast and AT&T, so I think a lot of the skepticism is warranted, and I think a lot of the burden is on them to show that they are honoring their privacy policies," White said. "Some of us think the idea of monetizing ad profiles for consumer ISPs is just unfathomable in the first place... but if there is a tier where they claim there are privacy enhancements and [it's] less invasive, the security community and privacy community are going to be looking very closely at those claims to make sure they're as stated."

We asked AT&T's spokesperson if the company is willing to let its system be examined by privacy experts but did not receive an answer.

If you care about privacy and cost, it's a difficult choice

Consumers can complain to the Federal Trade Commission (FTC) about privacy violations, but AT&T's Internet Preferences doesn't appear to be facing any challenges. When contacted about AT&T's Internet Preferences, an FTC spokesperson said the commission's policy is "not to comment on companies' practices unless it's part of a lawsuit or report."

The FTC's role in investigating Internet service providers could be coming to an end because of the Federal Communications Commission decision last month to reclassify broadband as a common carrier service. Common carriers are exempt from FTC jurisdiction, but the FTC says it can pursue violations that occurred before the reclassification, and the FCC's new Open Internet Order paves the way for new privacy obligations to be imposed on broadband providers.

An FCC spokesperson declined comment on AT&T's Internet Preferences but noted that the Open Internet regulations require the rates and terms of all plans to be disclosed. The FCC will also impose privacy requirements under Section 222 of the Communications Act, but the FCC has not yet written broadband-specific privacy rules. The existing privacy rules are geared toward telephone service.

For now, AT&T customers who value their privacy will continue to face a tough decision.

"For that price, I'd want proof that AT&T is no longer technically capable of tracking users who opt out," Ars forum member kdemmello1980 wrote. "Otherwise, it's bullshit, and all users of U-verse need to start using a VPN for everything."