

MARCH 19, 2017 | BY [JEREMY GILLULA](#)

Five Creepy Things Your ISP Could Do if Congress Repeals the FCC's Privacy Protections



Why are we [so worried about Congress repealing the FCC's privacy rules for ISPs](#)? Because we've seen ISPs do some disturbing things in the past to invade their users' privacy. Here are five examples of creepy practices that could make a resurgence if we don't stop Congress now.

TAKE ACTION

[Call Congress and help keep creepy ISP practices a thing of the past!](#)

5. Selling your data to marketers

Which ISPs did it before? We don't know—but they're doing it as you read this!

It's no secret that many ISPs think they're sitting on a gold mine of user data that they want to sell to marketers. What some people don't realize is that some are already doing it. (Unfortunately they're getting away with this for now because the FCC's rules haven't gone into effect yet.)

According to Ad Age, [SAP sells a service called Consumer Insights 365](#), which "ingests regularly updated data representing as many as 300 cellphone events per day for each of the 20 million to 25 million mobile subscribers." What type of data does Consumer Insights 365 "ingest?" Again, according to Ad Age, "The service also combines data from telcos with other information, telling businesses whether shoppers are checking out competitor prices... It can tell them the age ranges and genders of people who visited a store location between 10 a.m. and noon, and link location and demographic data with shoppers' web browsing history." And who is selling SAP their customers' data? Ad Age says "SAP won't disclose the carriers providing this data."

[Donate to EFF](#)

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying



eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. [Learn more](#) about what the program is, how it works, and what you can do.

Follow EFF

Pls plan to call your House Rep Monday, "vote no FCC privacy repeal" If your rep is Republican, ask 5 friends to <https://eff.org/gopp>

MAR 24 @ 4:18PM

A loophole in Australia's copyright safe harbor rules will stay open, endangering local user-generated content sites <https://www.eff.org/deeplinks>

MAR 24 @ 1:37PM

In all, @agcrocker addressed the appeals court on NSLs for more than 25 minutes. Here's the full recording. <https://youtu.be/ccS06CFkZ5I>

MAR 24 @ 1:09PM

[Twitter](#) [Facebook](#) [Identi.ca](#)

Projects

In other words, mobile broadband providers are too afraid to tell you, their customers, that they're selling data about your location, demographics, and browsing history. Maybe that's because it's an incredibly creepy thing to do, and these ISPs don't want to get caught red-handed.

And speaking of getting caught red-handed, that brings us to...

4. Hijacking your searches

Which ISPs did it before? Charter, Cogent, DirecPC, Frontier, Wide Open West (to name a few)

Back in 2011, [several ISPs were caught red-handed working with a company called Paxfire to hijack their customers' search queries to Bing, Yahoo!, and Google](#). Here's how it worked.

When you entered a search term in your browser's search box or URL bar, your ISP directed that query to Paxfire instead of to an actual search engine. Paxfire then checked what you were searching for to see if it matched a list of companies that had paid them for more traffic. If your query matched one of these brands (e.g. you had typed in "apple", "dell", or "wsj", to name a few) then Paxfire would send you directly to that company's website instead of sending you to a search engine and showing you all the search results (which is what you'd normally expect). The company would then presumably give Paxfire some money, and Paxfire would presumably give your ISP some money.

In other words, ISPs were hijacking their customers' search queries and redirecting them to a place customers hadn't asked for, all while pocketing a little cash on the side. Oh, and the ISPs in question hadn't bothered to tell their customers they'd be [sending their search traffic to a third party that might record some of it](#).

It's hard to believe we're still on the subtle end of the creepy spectrum. But things are about to get a whole lot more in-your-face creepy, with...

3. Snooping through your traffic and inserting ads

Which ISPs did it before? AT&T, Charter, CMA

This is the biggest one people are worried about, and with good reason—ISPs have every incentive to snoop through your traffic, record what you're browsing, and then inject ads into your traffic based on your browsing history.

Plenty of ISPs have done it before—[AT&T did it on some of their paid wifi hotspots](#); [Charter did it with its broadband customers](#); and a [smaller ISP called CMA did the same](#).

We don't think this one requires much explaining for folks to understand just how privacy invasive this is. But if you need a reminder, we're talking about the company that carries all your Internet traffic examining each packet in detail¹ to build up a profile on you, which they can then use to inject even more ads into your browsing experience. (Or, even worse—they could hire a third-party company like [NebuAd](#) or [Phorm](#) to do all this for them.) That's your ISP straight up spying on you to sell ads—and turning the creepiness factor up to eleven.² And speaking of spying, we'd be remiss if we didn't mention...

2. Pre-installing software on your phone and recording every URL you visit

Which ISPs did it before? AT&T, Sprint, T-Mobile

When you buy a new Android phone, you probably expect it to come with some bloatware—apps installed by the manufacturer or carrier that you're never going to use. You *don't* expect it to come preinstalled with [software that logs which apps you use and what websites you visit and sends data back to your ISP](#). But that's exactly what was uncovered when security researcher and EFF client [Trevor Eckhart did some digging into Carrier IQ](#), an application that came preinstalled on phones sold by AT&T, Sprint, and T-Mobile.

[Bloggers' Rights](#)

[Coders' Rights](#)

[Encrypt the Web](#)

[Free Speech Weak Links](#)

[Global Chokepoints](#)

[HTTPS Everywhere](#)

[Manila Principles](#)

[Medical Privacy Project](#)

[Open Wireless Movement](#)

[Patent Busting](#)

[Privacy Badger](#)

[Student Activism](#)

[Student Privacy](#)

[Surveillance Self-Defense](#)

[Takedown Hall of Shame](#)

[Teaching Copyright](#)

[Transparency Project](#)

[Trolling Effects](#)

[Ways To Help](#)

This is even creepier than number three on our list (watching your traffic and injecting ads), because at least with number three, your ISP can only see your unencrypted traffic. With Carrier IQ, your ISP could also see what encrypted (HTTPS) URLs you visit and record what apps you use.

Simply put, preinstalled software like Carrier IQ gives your ISP a window into *everything* you do on your phone. While mobile ISPs may have backed down on using Carrier IQ in the past (and the situation led to a [class action lawsuit](#)), you can bet that if the FCC's privacy rules are rolled back there'll be ISPs be eager to start something similar.

But none of these creepy practices holds a candle to the ultimate, creepiest thing ISPs want to do with your traffic, which is...

1. Injecting undetectable, undeletable tracking cookies in all of your HTTP traffic

Which ISPs did it before? AT&T, Verizon

The number one creepiest thing on our list of privacy-invasive practices comes courtesy of Verizon (and AT&T, which [quickly killed a similar program](#) after Verizon started getting blowback).

Back in 2014 Verizon Wireless decided that it was a good idea to insert supercookies into *all of its mobile customers' traffic*. Yes, you read that right—it's as if some Verizon exec thought "inserting tracking headers into all our customers' traffic can't have a down side, can it?" Oh, and, for far too long, they didn't bother to explicitly tell their customers ahead of time.

But it gets worse. Initially, there was no way for customers to turn this "feature" off. It didn't matter if you were browsing in Incognito or Private Browsing mode, using a tracker-blocker, or had enabled Do-Not-Track: Verizon ignored all this and inserted a unique identifier into all your unencrypted outbound traffic anyway. According to the [FCC](#), it wasn't until "two years after Verizon Wireless first began inserting UIDH, that the company updated its privacy policy to disclose its use of UIDH and began to offer consumers the opportunity to opt-out of the insertion of unique identifier headers into their Internet traffic."

As a result, anyone—not just advertisers—could track you as you browsed the web. Even if you cleared your cookies, [advertisers could use Verizon's tracking header to resurrect them](#), which led to something called "zombie cookies." If that doesn't sound creepy, we don't know what does.

As you can see, there's a lot at stake in this fight. The FCC privacy rules congress is trying to kill would limit all of these creepy practices (and even ban some of them outright). So don't forget to call your senators and representative *right now*—because if we don't stop Congress from killing the FCC's ISP privacy rules now, we may end up with a lot more than five creepy ISP practices in the future.

TAKE ACTION

Call Congress and help keep creepy ISP practices a thing of the past!

-
1. To be absolutely precise, your ISP could track and record all your HTTP traffic, and the domain name you visit for HTTPS websites.
 2. We've heard some arguments that is just what Google or Facebook do, but there's a big difference. You can choose not to use Google or Facebook, and it's easy to install free tools that block their tracking on other parts of the web. EFF even makes such a tool, called [Privacy Badger!](#) But changing ISPs or paying for a VPN is hard (and some people don't have more than one choice of ISP). For more, [see our post on busting three ISP privacy rollback myths](#).

MORE DEEPLINKS POSTS LIKE THIS

MARCH 2017

[Three Myths the Telecom Industry is Using to Convince Congress to Repeal the FCC's Privacy Rules, Busted](#)

AUGUST 2011

[An update on Paxfire and search redirection](#)

JANUARY 2014

[Why the FCC Can't Actually Save Net Neutrality](#)

NOVEMBER 2014

[Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls](#)

AUGUST 2011

[Widespread Hijacking of Search Traffic in the United States](#)

RECENT DEEPLINKS POSTS

MAR 24, 2017

[Another Loss For Broadcast TV Streaming, And A Dangerous Shift Of Decision-Making Power](#)

MAR 24, 2017

[Australia Stalls Copyright Safe Harbor Proposal](#)

MAR 24, 2017

[House Schedules Vote on Eliminating Consumer Online Privacy Rights Next Week](#)

MAR 23, 2017

[Senate Puts ISP Profits Over Your Privacy](#)

MAR 22, 2017

[The Bill of Rights at The Border: The First Amendment and the Right to Anonymous Speech](#)

DEEPLINKS TOPICS

[Fair Use and Intellectual Property: Defending the Balance](#)

[Free Speech](#)

[Innovation](#)

[UK Investigatory Powers Bill](#)

[International](#)

[Know Your Rights](#)

[Privacy](#)

[Trade Agreements and Digital Rights](#)

[Security](#)

[State-Sponsored Malware](#)

[Abortion Reporting](#)

[Analog Hole](#)

[Anonymity](#)

[Anti-Counterfeiting Trade Agreement](#)

[Artificial Intelligence & Machine Learning](#)

[Biometrics](#)

[Bloggers' Rights](#)

[Border Searches](#)

[Broadcast Flag](#)

[Broadcasting Treaty](#)

[CALEA](#)

[Cell Tracking](#)

[Coders' Rights Project](#)

[Computer Fraud And Abuse Act Reform](#)

[Content Blocking](#)

[Copyright Trolls](#)

[Council of Europe](#)

[DRM](#)

[E-Voting Rights](#)

[EFF Europe](#)

[Electronic Frontier Alliance](#)

[Encrypting the Web](#)

[Export Controls](#)

[Eyes, Ears & Nodes Podcast](#)

[FAQs for Lodsys Targets](#)

[File Sharing](#)

[Fixing Copyright? The 2013-2016 Copyright Review Process](#)

[FTAA](#)

[Genetic Information Privacy](#)

[Government Hacking and Subversion of Digital Security](#)

[Hollywood v. DVD](#)

[How Patents Hinder Innovation \(Graphic\)](#)

[ICANN](#)

[International Privacy Standards](#)

[Internet Governance Forum](#)

[Law Enforcement Access](#)

[Legislative Solutions for Patent Reform](#)

[Locational Privacy](#)

[Mandatory Data Retention](#)

[Mandatory National IDs and Biometric Databases](#)

[Mass Surveillance Technologies](#)

[Medical Privacy](#)

[Mobile devices](#)

[National Security and Medical Information](#)

[Patent Trolls](#)

[Patents](#)

[PATRIOT Act](#)

[Pen Trap](#)

[Policy Analysis](#)

[Printers](#)

[Public Health Reporting and Hospital Discharge Data](#)

[Reading Accessibility](#)

[Real ID](#)

[Reclaim Invention](#)

[RFID](#)

[Search Engines](#)

[Search Incident to Arrest](#)

[Section 230 of the Communications Decency Act](#)

[Shadow Regulation](#)

[Social Networks](#)

[SOPA/PIPA: Internet Blacklist Legislation](#)

[Student Privacy](#)

[Stupid Patent of the Month](#)

[Surveillance and Human Rights](#)

[Surveillance Drones](#)

[Terms Of \(Ab\)Use](#)

[Test Your ISP](#)

[The "Six Strikes" Copyright Surveillance Machine](#)

[The Global Network Initiative](#)

[The Law and Medical Privacy](#)

[TPP's Copyright Trap](#)

[Trans-Pacific Partnership Agreement](#)

[Cyber Security Legislation](#)

[CyberSLAPP](#)

[Defend Your Right to Repair!](#)

[Development Agenda](#)

[Digital Books](#)

[Digital Radio](#)

[Digital Video](#)

[DMCA](#)

[DMCA Rulemaking](#)

[Do Not Track](#)

[National Security Letters](#)

[Net Neutrality](#)

[No Downtime for Free Speech](#)

[NSA Spying](#)

[OECD](#)

[Offline : Imprisoned Bloggers
and Technologists](#)

[Online Behavioral Tracking](#)

[Open Access](#)

[Open Wireless](#)

[Patent Busting Project](#)

[Travel Screening](#)

[TRIPS](#)

[Trusted Computing](#)

[Video Games](#)

[Wikileaks](#)

[WIPO](#)

[Transparency](#)

[Uncategorized](#)



[Thanks](#) | [RSS Feeds](#) | [Copyright Policy](#) | [Privacy Policy](#) | [Contact EFF](#)