Paxfire: our search query intercepts are not wiretapping

By Timothy B. Lee | Published about 2 hours ago

Last month we covered the controversy over Paxfire, a firm that researchers have accused of "hijacking" search results by placing a proxy server between users and major search engines and modifying some responses. Paxfire and one of its customers, RCN, was soon hit with a class-action lawsuit claiming that the use of search hijacking violated the Wiretap Act, consumer protection laws, and RCN's contractual obligations.

Now Paxfire has responded with a countersuit, charging the lead plaintiff, Betsy Feist, with slander, libel, and tortious interference with its business relationships. Paxfire strenuously denies that it shares user information with third parties. It argues that its actions don't constitute interception of user communications under wiretapping law and that users consented to Paxfire's activities when they signed RCN's acceptable use policy. Paxfire asked the court to award it compensatory and punitive damages of at least $50 million.

Ars talked to Mike Sullivan, Paxfire's vice president for engineering, about Paxfire's technology. In this article, we'll describe the technology Sullivan explained to us, discuss whether Paxfire's actions pass muster under federal wiretapping laws, and conclude with an analysis of whether the technology is good for users.

Error correction

Originally, Paxfire simply offered technology to help ISPs to monetize invalid DNS queries. When a user entered a nonexistent domain name into the URL bar of his browser, Paxfire's DNS server would direct the user to a Paxfire-sponsored page of search results rather than returning an error message. This search page would generate advertising revenue, which Paxfire would share with its ISP clients. This practice has been criticized by some as a violation of network neutrality, but it's becoming increasingly common and isn't generally regarded as being against the law.

Then (from Paxfire's perspective at least) browser vendors began encroaching on Paxfire's turf. Some browsers began merging the functions of the address and search bars. If the user entered an invalid URL into the address bar, the browser itself would interpret it as a search term and automatically submit it to a search engine. Google's Chrome takes this trend to its logical extreme, eliminating the search bar entirely in favor of a combined address/search bar. This reduced demand for Paxfire's DNS error-correction "service."

Apparently seeing a threat to its business model, Paxfire took an aggressive countermeasure. Its DNS servers began responding to queries for the IP addresses of search engines with the IP address of proxy servers operated by Paxfire itself. That

effectively made Paxfire a "man in the middle" between the user and search engines. For most queries, the proxies would simply relay the query to the appropriate search engine and send the result back to the user. But the proxy server would handle a limited number of queries itself.

For example, if the user searched for "apple," the proxy server might redirect the user to apple.com. This allowed Paxfire to claim a referral fee that might otherwise have gone to the user's chosen search engine. Paxfire shares the resulting revenue with the user's ISP.

In his conversation with us, Sullivan stressed two points about this technology. First, it's highly customizable, and the final decision about how (and whether) to use the proxying capability is up to each individual ISP.

Second, he said, the technology is conservative about which queries get redirected. By examining query parameters, Paxfire's proxy server can detect whether a query was generated from a search engine home page, from the search box in the browser's chrome, or from a browser's unified search/address bar. Sullivan said Paxfire servers only intervene in this final case. He said that if a user goes to google.com and enters search terms, the user will always get ordinary search results, as expected.

Finally, Sullivan flatly denied the allegation that Paxfire shared the contents of queries with others. "We don't give any information to any third parties," he said.

Is this wiretapping?

So is this legal? To help us answer that question, Ars talked to Julian Sanchez, a privacy scholar at the Cato Institute (and Ars Technica alumnus). He told Ars that it's complicated.

Federal law distinguishes between addressing information and the content of communications, with the latter receiving stricter legal protection. "To run afoul of the Wiretap Act, Paxfire and the ISP would have to be 'intentionally' divulging or intercepting 'content' without consent," Sanchez said. "If they were redirecting or logging queries from the Google-branded search bar, I think that would pretty clearly be an interception of the contents of a communication whose intended recipient was Google."

However, if a user types "apple" into the browser's unified search/address bar, it's not clear if the user considers "apple" to be a search term or an address. If the user is trying to go to Apple's website, then "apple" could be addressing information. "Depending on the details of what they're doing, the companies might be able to argue that they're only looking at faulty or incomplete addressing information in an effort to get a web request to its intended recipient."

Paxfire also argues that its service is legal because users consented to it via Paxfire's agreements with ISPs. But Chris Soghoian, a security researcher at Indiana University,

rejected that argument. He noted that users rarely read the fine print of privacy policies, and tend to assume that the existence of privacy policies means their privacy is protected.

Sanchez agreed. "I think they'd have an uphill battle trying to lean on vague legalese buried in the ISP terms of service to claim 'consent,'" he said. "Providers can't disavow liability under the Electronic Communications Privacy Act that easily."

Maybe not illegal, but definitely bad for users

The best that can be said for Paxfire is that the company is operating in a legal grey area. There's limited case law about what exactly counts as wiretapping in a packet-switched network, and the Paxfire case may give the courts an opportunity to establish clearer principles on the topic.

But whatever the outcome of the legal debate, we think it's clear that Paxfire's "service" is bad for users. The Internet was designed with an end-to-end architecture for good reasons. The user experience should be controlled by users, the browsers they choose to run, and the websites they choose to visit. Paxfire's technology undermines that principle by giving themselves the ability to tamper with search results as they traverse the Internet.

Even if Paxfire's proxy servers never modified communications between users and search engines, the unnecessary man-in-the-middle would still add unnecessary complexity, degrading performance and creating unnecessary security risks. And Paxfire admits it does sometimes modify requests as they flow across the network. While the specific modifications Paxfire makes seem relatively innocuous, the principle is a dangerous one. Users shouldn't have to worry about ISPs tampering with their communications.