August 28, 2017

How to stop the tracking of every digital move you make

Device lets you block your browsing habits, keep online life private

FEATURED STORY **BY RODIKA TOLLEFSON, THIRDCERTAINTY**

Consumers' digital trails—from their browsing and social media habits to search-engine inquiries—are a boon to financial institutions, which can use this treasure trove of data to analyze borrowing risk and other factors. More than 3,000 services worldwide track and gather this data, aggregating and selling it for banks' use, unbeknown to consumers.

"The trackers are gathering our browsing habits down to our mouse movement and all the data we're entering into forms," said Christian Bennefeld, co-founder and CEO of eBlocker, a German startup that has developed a device that provides complete online anonymity.

Some financial institutions use their own trackers for purposes like improving their websites and tailoring marketing campaigns. Brokers, on the other hand, may gather information like online poker habits, use of payday lenders and even multiple corrections to salary in an online loan calculator.

Related article: *Consumers becoming much more protective of their privacy*

"Banks can take this browsing data and the aggregated data from brokers and use algorithms for loan risk calculation," Bennefeld said.

An eBlocker analysis of 10 major U.S. banks' websites found a total of at least 110 third-party trackers in use. PNC had the biggest number (33), followed by

TD Bank (20) and BNY Mellon (14). On the lower end were HSBC (2) and Wells Fargo (5).

"We were surprised about the quantity of trackers on American websites and that Facebook and Google (trackers) were widespread," Bennefeld said. "In Germany, it would be prohibited, but I fear the U.S. is more liberal in data brokerage, and there are no negative consequences for banks for doing so."

Companies of all sizes use trackers

Smaller banks and credit unions appear to use the practice as well, even if on a smaller scale. From an arbitrary list of nine U.S. regional banks and credit unions provided by Third Certainty, eBlocker found that all but one had website trackers. One credit union used 19, including one that tracks and records mouse movements.

Christian Bennefeld, eBlocker co-founder and CEO

Bennefeld said it was remarkable to see that even most of the smaller banks use Google services to reveal "who are their customers and what their standing is to Google."

"In comparison, you will hardly find a bank in Europe that is using Google services at all," he said.

Bennefeld's four-year-old company, eBlocker, is hoping to attract U.S. customers who are concerned about tracking practices, common for businesses of all kinds. The eBlocker device uses a variety of techniques, such as traffic routing through a VPN or Tor, IP address anonymizing, user agent spoofing, DNS spoofing and ad blocking, to block data collection and provide online privacy.

"We make sure you're not leaving any traces on the internet," Bennefeld said.

The device, which plugs into the home router, is popular in Germany and Switzerland, where it's sold by retailers that are equivalent to Best Buy, according to Bennefeld. U.S. consumers can buy eBlocker directly from the company. The plan is to sell it through distributors in the near future. If all goes well, a U.S. office will open by the first quarter of 2018.

The timing to enter the U.S. market seems fortuitous, considering that the recent congressional repeal of FCC's privacy rules now allows ISPs to collect and sell customer data.

"We feel we can help those consumers who are not trusting the current situation in the U.S., and our technology is perfect to disguise customers from their providers," Bennefeld said.

How it works

Once eBlocker is connected to the router, all inbound and outbound TCP/IP packets (from the browser only) are routed to the device for what's called deep package inspection. Using pattern-matching technology, the packets are compared against known patterns.

"We have a team compiling every day, from different sources and from our users, the patterns of tracking services," Bennefeld said.

If a matching packet is found, it's simply not sent to the router. Bennefeld estimates that as much as 40 percent of web traffic is comprised of trackers, so eBlocker can significantly speed up web browsing.

The device is compatible with all operating systems and can be used not only for computers and tablets but also while browsing the web on a smart TV. The plug-and-play device requires no technical knowledge, but tech-savvy users can buy the eBlockerOS software and instead make their own device using a Raspberry Pi or Banana Pi.

A family version of eBlocker allows for individualized user profiles. Bennefeld said a benefit for parents is the ability to filter out risky websites for their kids, as well as to set surfing timers and limit the hours when their children can be on the web.

Turning the tables on tracking

Bennefeld, a mathematician and computer scientist, has first-hand knowledge of the tracking industry. After working for major data-security and software companies, 17 years ago he founded etracker, a German web-analytics and online-marketing optimization company. As the CEO for 13 years, Bennefeld made etracker a market leader. But he wasn't happy about what he saw happening in the background, Bennefeld said.

He invested $1 million of his own funds into eBlocker, which also has received money from a public innovation fund in Hamburg. Sales have been brisk—$1.2 million last year, with the goal of doubling that this year.

An employee base of 12 is poised to grow once a current round of funding closes. A U.S. subsidiary already is in place, and Bennefeld sees the U.S. as a core market.

Plans are in the works for a mobile version and an enterprise product, which Bennefeld expects to be in demand by legal practices, doctors' offices and other businesses that handle sensitive customer data.

"We try to avoid all the mistakes I've made with etracker," Bennefeld said. "We are following a redline, we have a focus, and we're executing on that."

More stories related to online privacy:

With no global standard for data privacy, laws outside U.S. differ in scope