The Atlantic

People's Deepest, Darkest Google Searches Are Being Used Against Them

On the Internet, search queries are used to target vulnerable consumers.

Beck Diefenbach / Reuters

ADRIENNE LAFRANCE

NOV 3, 2015 | TECHNOLOGY

Google knows the questions that people wouldn't dare ask aloud, and it silently offers reams of answers. But it is a mistake to think of a search engine as an oracle for anonymous queries. It isn't. Not even close.

In some cases, the most intimate questions a person is asking—about health worries, relationship woes, financial hardship—are the ones that set off a

chain reaction that can have troubling consequences both online and offline.

All this is because being online increasingly means being put into categories based on a socioeconomic portrait of you that's built over time by advertisers and search engines collecting your data—a portrait that data brokers buy and sell, but that you cannot control or even see. (Not if you're in the United States, anyway.)

Consider, for example, a person who googles "need rent money fast" or "can't pay rent." Among the search results that Google returns, there may be ads that promise to help provide payday loans—ads designed to circumvent Google's policies against predatory financial advertising. They're placed by companies called lead generators, and they work by collecting and distributing personal information about consumers online. So while Google says it bans ads that guarantee foreclosure prevention or promise short-term loans without conveying accurate loan terms, lead generators may direct consumers to a landing page where they're asked to input sensitive identifiable information. Then, payday lenders buy that information from the lead generators and, in some cases, target those consumers—online, via phone, and by mail—for the very sorts of short-term loans that Google prohibits.

"It's a sucker list. And people will buy that information for all different kinds of reasons."

"Google has a decent policy—including 'obey the law'—but it's a very hard policy for Google to effectively enforce," said Aaron Rieke, a projects director at Upturn, a technology policy consulting group in Washington, D.C. "As a result, payday advertisers are often violating it and skirting around it. The result is that online payday marketers are reaching out to people nationwide,

even to people who live in states where payday lending—and the solicitation of payday loans—is effectively illegal." Google declined multiple requests to describe how it developed its policies on ads for financial services.

Lead generators are increasingly under scrutiny by federal agencies and consumer advocates. Upturn recently released a damning report about lead generators, and the practice was at the center of a workshop held by the Federal Trade Commission last week.

"I find the entire online ecosystem that is designed to track consumers and then to place them in boxes … too opaque and too under-regulated," said Ed Mierzwinski, the consumer-program director at the consumer-advocacy group U.S. PIRG, during the FTC workshop on Friday. "So I think the entire online marketing, and advertising, and lead-generation system is a consumer protection problem of both deception, and unfairness, and maybe abuse as well."

Online lead generation is complicated in part because it involves a long chain of different companies, including but not limited to search engines, lead aggregators, and the businesses that end up buying the leads. The practice also entails several layers of privacy and consumer-protection concerns.

Not only are lenders taking advantage of people in vulnerable financial situations, not only are lead generators sometimes skirting Google's ad policies and even violating state laws, but companies are sharing individual data in a way that puts consumers directly at risk. All this comes down to the widespread availability and longevity of personal data online.

Imagine again the person who turns to Google with a search term like "need money fast." Let's say that person ends up at a lead generator's landing page, providing various information in hopes of getting a quick loan. "A very small percentage of those folks are actually qualified for a loan," said Michael

Waller, an attorney in the Bureau of Consumer Protection's enforcement division at the FTC. "And so the vast majority—95 percent of those applications, which means 95 percent of the folks whose social-security numbers and bank-account numbers fall to the cutting room floor—are referred to in the industry as 'remnants.'"

RELATED STORY

Why Can't Americans Find Out What Big Data Knows About Them?

Those so-called remnants aren't discarded, though. They are sold and resold and resold again. "What's created over a period of time is the consumers just become suckers," Waller said in the FTC workshop. "It's a sucker list. And people will buy that information for all different kinds of reasons."

"Data brokers, publishers, folks who have this information—and a lot of people have access to this information along the chain because it's shared freely even if it isn't purchased—there's a lot of pressure on them to use, to monetize what they consider an asset," Waller said. "Which is just a big pile of data, a big pile of data points."

As the big piles of data online continue to grow, these issues will become more pronounced. Information filters that control what version of the Internet a person sees are calibrated based on how much money various algorithms think you have. Which means distinct digital-advertising landscapes are increasingly drawn on socioeconomic lines.

The effect may be a more pleasant online experience for someone who is perceived to have more income. In the same way that startups have put a premium on cutting out human interaction for those who can afford it, adlessness can be a luxury for those who choose to buy ad blockers so their

webpages load faster. But distinct ad landscapes aren't just about seeing more elegant corporate messages, or encountering fewer pop-up ads—or even none at all. Companies and individuals are working together to target consumers on a personal level, to use their most vulnerable Google searches against them.

"Fraudsters buy this data," Waller said. "It's easy to access, easy to buy, easy to find. They use it sometimes for really shocking, outright fraud and theft. Sometimes it's a little more subtle than that."

ABOUT THE AUTHOR

ADRIENNE LAFRANCE is a staff writer at *The Atlantic*, where she covers technology. She was previously an investigative reporter for *Honolulu Civil Beat*, Nieman Journalism Lab, and WBUR.

Twitter