Dark patterns: Research reveals the dirty tricks of online shopping

November 29 2019

Credit: CC0 Public Domain

As millions of people begin their holiday shopping, they'll come across many familiar tricks online. In some cases, sites will hype limited-time deals with a countdown clock, warn you that the product you're looking

at is running out of stock, or tell you that 65 people in your area have recently purchased the item. In others, they'll quietly add items to your cart, or sign you up for recurring payments under the guise of a free trial.

Many of these manipulative retail strategies have existed since long before the internet—think of the store with the never-ending "Going Out of Business" sale, or the Columbia House "8 Albums for a Penny" deal. But online shopping has pushed these shady practices into overdrive, deploying them in newly powerful and sneaky ways. In a first-of-its kind survey, a group of University of Chicago and Princeton researchers found that "dark patterns" on shopping websites were startlingly common—appearing on more than 1 out of 10 sites and used frequently by many of the most popular online merchants.

"Dark patterns are basically tactics a user interface design uses to lead a user down a certain path for the benefit of the service provider," said Marshini Chetty, assistant professor of computer science at UChicago and co-author of the paper presented at the Conference on Computer-Supported Cooperative Work and Social Computing (CSCW) in November. "Often, it's trying to get the user to make a decision that they may not have made if they were otherwise fully informed. On the internet, they could be affecting thousands or millions of people, and we don't really fully understand what their impact is on decision-making."

The term "dark patterns" was coined by user experience designer Harry Brignull in 2010 to describe deceptive online practices. These could include pre-web retail tricks such as hidden costs or forced enrollment, but also new strategies unique to the internet, such as "confirmshaming"—when a pop-up uses manipulative language ("No thanks, I don't want to take advantage of this incredible offer.") to lead users away from declining a purchase—or social proof ("97 other users are viewing this item").

While previous research either described these patterns or collected anecdotal evidence on their usage, the new project, led by Princeton graduate student Arunesh Mathur, built a web-crawling tool to analyze more than 50,000 product pages from 11,000 shopping sites. By grabbing the text from these pages, the team could look for both known and new "dark patterns," as well as measure how frequently they appear. In total, they found more than 1,800 instances of dark pattern usage on 1,254 websites, which likely represents a low estimate of their true presence, the authors said.

"The goal of these patterns in the shopping context is to get you to buy more things," Mathur told the Wall Street Journal. "Once you know about them, you see them everywhere."

On a subset of 183 online shopping websites, the researchers found these patterns were outright deceptive. Some commonly used tricks on this subset of websites included countdown timers for "limited-time" sales that reset every time the user reloaded the page, faked customer testimonials, low-stock or high-demand notifications that appear on a recurring schedule, and messages or layouts that pressure consumers to buy higher-cost items. By looking at the computer code behind these website elements, the researchers found third-party services that provide these options to shopping websites, enabling dark patterns to proliferate as easy-to-install plugins.

To help consumers recognize these misleading practices, the research team created a website to raise awareness of different dark patterns. They have also discussed their findings with the Federal Trade Commission—the government agency charged with regulating deceptive retail practices—and provided information to the sponsors of the Deceptive Experiences To Online Users Reduction (DETOUR) Act, introduced in the U.S. Senate earlier this year.

"It wasn't the goal of the work to name and shame people; it's unclear, in some cases, whether people are fully aware that they're being utterly deceptive," Chetty said. "But we wanted to get a sense of: Is this a problem and should we be doing something about it? Then the government can pass legislation that would make it very difficult for service providers to use certain dark patterns, particularly those that try to trick users into giving up information or that are directed at children."

Future directions of the research could look for dark patterns on travel websites or in games marketed to children, Chetty said. There's also important research questions on how effective these methods are at influencing user behavior—an area explored in a recent working paper by Jamie Luguri and Lior Strahilevitz of the UChicago Law School. Through UChicago SUPERgroup—the research team she co-directs with assistant professor Blase Ur—Chetty continues to explore how similar kinds of internet design and practices can affect vulnerable and marginalized populations.

"I study how people use the internet and I try to empower them with information and control of the different aspects of internet use," said Chetty, who joined the University of Chicago this past summer. "I try to answer fundamental questions and then develop systems to help people actually manage or understand more about their usage in some way."

Provided by University of Chicago