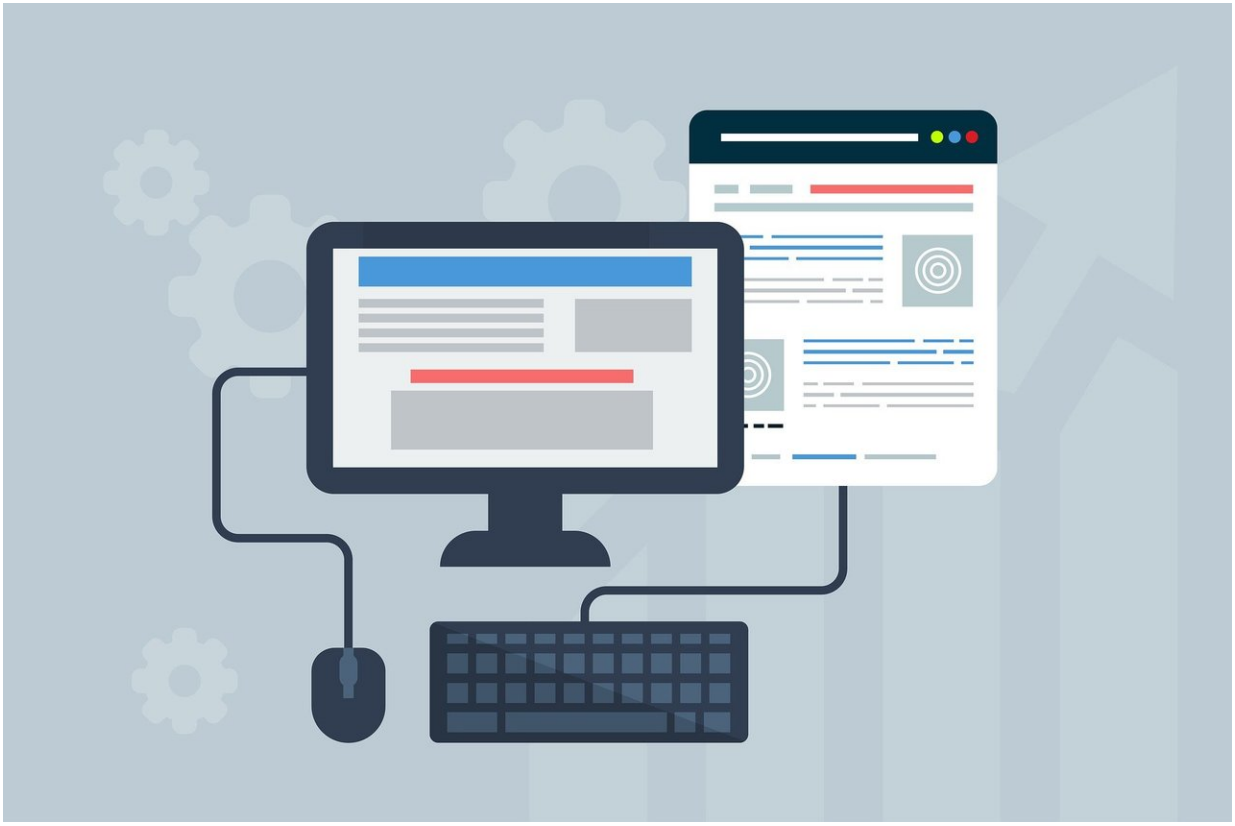
Consumer Privacy Protection Act could lead to fines for deceptive designs in apps and websites

March 15 2023, by Jonathan Obar



Credit: CC0 Public Domain

Canada's proposed Consumer Privacy Protection Act (CPPA) prohibits online consent processes that are deceptive or misleading.

Companies may face fines for breaking the act's rules. This could be trouble for social media platforms, online shopping companies and other services that use deceptive user interface designs in their apps and websites.

The CPPA is a component of Bill C-27, described by the federal government as an attempt to improve Canadian privacy law and ensure responsible use of personal information and artificial intelligence by companies.

The possibility of fines for deceptive or misleading consent processes suggests the government views consent as fundamental to personal information protections. As a result, companies may be held accountable for deceptive user interface designs associated with app and website consent processes.

User interface design means deciding how to present buttons, links, prompts, images, video, text and other visual elements on-screen. Decisions about the shape, color, size and placement of these elements influence what people see first or second, where they click/tap, whether a purchase is made, a complaint is lodged or consent is given.

Deceptive designs (sometimes problematically called dark pattern designs) are design choices that can mislead, coerce and exploit people for the benefit of for-profit companies. A study of about 11,000 shopping sites describes 15 types of deceptive designs, each with a unique approach to manipulation.

Fines for deceptive design

Deceptive design is a top information policy issue internationally, and problematic consent processes are a primary focus of current enforcement efforts. In 2022, the Commission Nationale de

l'Informatique et des Libertés (CNIL), a data protection authority in France, fined Google the equivalent of C$215 million and Facebook the equivalent of C$86 million for deceptive design.

CNIL said the companies provided people with a button to accept online cookies "immediately," but did not provide a similar prompt for refusal. CNIL claimed that requiring multiple clicks to refuse all cookies improperly influenced the consent process.

Action by the U.S. Federal Trade Commission (FTC) led to internet telephone company Vonage having to refund the equivalent of C$133 million to customers for deceptive designs that made it easy to sign up for a service, but very difficult to cancel. FTC action also led to the company that runs the online learning program ABCMouse having to pay the equivalent of C$13 million for similar designs.

The company Noom, which owns an app for tracking food and exercise consumption, recently settled the equivalent of a C$83 million class action suit after customers alleged they were unfairly charged subscription fees.

Commenting on deceptive designs, the FTC stated that "more and more companies are using digital dark patterns to trick people into buying products and giving away their personal information…these traps will not be tolerated."

The clickwrap

A deceptive design common to online consent processes is the clickwrap. The clickwrap, or clickthrough agreement, is a set of user interface designs people often encounter when signing up for a new app or website, or when terms of service and privacy policies change.

Clickwraps can include an appealing "accept" button and less-noticeable links to policies. As people read from the top of the screen to the bottom, they might notice the colorful accept button first and miss links to policies below the button or elsewhere on screen.

In a previous study I co-authored about clickwraps, study participants said they saw a prominently displayed accept/join button first, while links to policies were small and "easy to miss."

A recent paper I co-authored that has yet to be peer-reviewed suggests the text on clickwrap accept buttons rarely says "agree," and often says something like "sign up" or "create account" instead. This choice of text may distract people from the consent process taking place, keeping the focus on a quick sign up.

Clickwraps are a problem if the goal is to ensure an engaging online consent process. They raise concerns about for-profit companies moving individuals quickly towards monetized parts of services, instead of encouraging people to question if joining the service is a good idea.

An online consent process is a unique opportunity to engage people in far more than a boring contract.

Information on the future of artificial intelligence (AI), the benefits and drawbacks of data sharing and use, opt-in/out mechanisms, contact information for policymakers and privacy advocates, and digital literacy tools could all be available for review before consent is provided.

Instead, clickwraps make it easy to skip the fine print, as well as the opportunity to understand how service use has implications for the future.

Implications for AI and the future

One implication is the connection between deceptive user interface designs and the future of AI development. This is perhaps one reason the Canadian government is prioritizing the issue.

As big data expands through the ubiquity of the internet, endless data sets are now available across the global economy. Some AI developers don't engage directly with consumers, which raises questions about who is responsible for ensuring data is acquired via lawful consent processes.

The Office of the Privacy Commissioner of Canada emphasizes that the lack of a direct relationship with some AI developers, along with the challenge of understanding how data may be used in the future, further burdens people with having to decide whether clicking "sign up" is wise.

As governments figure out how to ensure meaningful consent is central to AI development, digital service providers must do their part to design user interfaces that are not deceptive or misleading.

If Canada's Bill C-27 becomes law, will government-imposed monetary penalties move companies away from clickwraps and towards interface designs that facilitate education and understanding? It's difficult to tell. It may depend on whether the Canadian government follows the lead of policymakers in the U.S. and France to hold companies accountable for deceptive designs.

Provided by The Conversation