

# Sweep on “dark patterns” sheds light on privacy commissioner expectations for obtaining meaningful consent in an online environment

August 29, 2024

In early 2024, Canadian privacy commissioners participated in the Global Privacy Enforcement Network (the GPEN) annual international privacy sweep (the Sweep). The theme of this year’s sweep was online deceptive design patterns (also known as “dark patterns”).

Deceptive design patterns are described as patterns “used on websites and mobile apps to influence, manipulate, or coerce users to make decisions that are not in their best interests.”<sup>1</sup> Further, “[t]hey can prevent users from making informed decisions about the collection, use, and disclosure of their personal information, and cause them to give up more privacy than they would like.”<sup>2</sup>

On July 9, 2024, the Office of the Privacy Commissioner of Canada (the OPC) published the [\*Sweep Report 2024: Deceptive Design Patterns\*](#) (the Report) on the results of the Sweep and its key findings.

In conjunction with releasing the Report, the OPC also issued new guidance for individuals on navigating, and for organizations on avoiding, deceptive design patterns (the Guidance). See OPC publications [\*Beware of deceptive design: Tips for individuals when navigating websites and mobile apps\*](#) and [\*Design with privacy in mind: Five business best practices to avoid deceptive design\*](#).

Together, the Report and the Guidance shed light on the OPC’s expectations when it comes to obtaining meaningful consent in an online environment.

Organizations doing business in Canada should assess their online platforms and consider any changes required to meet the OPC’s expectations. While the Report and the Guidance set out best practices, rather than binding rules, they serve as warning signals of the OPC’s priorities for potential future enforcement actions and provide concrete, illustrative examples of what the OPC finds acceptable and unacceptable. Organizations wanting to stay ahead of the curve should consider taking proactive steps to implement the OPC’s recommendations for avoiding deceptive design patterns now, rather than after a formal complaint or investigation.

## The Sweep

The Sweep occurred between Jan. 29, 2024 and Feb. 2, 2024 and involved collaboration by the OPC and 25 other privacy enforcement authorities. Over 1,000 websites and mobile apps were examined in the Sweep, including 145 websites and mobile apps examined by the OPC. The Sweep focused on the following five specific deceptive design patterns:

1. **Complex and confusing language:** technical and/or excessively long privacy policies that are difficult to understand.
2. **Interface interference:** design elements that can influence users' perception and understanding of their privacy options.
3. **Nagging:** repeated prompts for users to take specific actions that may undermine their privacy interests.
4. **Obstruction:** the insertion of unnecessary, additional steps between users and their privacy-related goals.
5. **Forced action:** requiring or tricking users into disclosing more personal information to access a service than is necessary to provide that service.<sup>3</sup>

While the use of deceptive design patterns is not specifically prohibited under Canadian privacy laws, their use can increase an organization's risk of failing to fulfill its personal information protection obligations, such as obtaining consent that is "meaningful".

The Report and the Guidance urge organizations to ensure their privacy policies and preferences are accessible to their users, and to take into consideration their target audience (e.g., children). In the context of consumer protection legislation, the Supreme Court of Canada has [previously applied a legal test](#) on the basis that an "average consumer" is one that is "credulous and inexperienced." Organizations should be aware of the courts' perception of the "average consumer" when using deceptive design patterns, as this standard might be relevant in determining whether the design pattern impedes users' access to, or understanding of, privacy policies and preferences, and accordingly that the organization has failed to fulfill its privacy law obligations.

## The Report and the Guidance

Below is a summary of the Report and the Guidance, including examples of each type of deceptive design pattern, the key findings identified in the Report, and the OPC's recommendations for avoiding each type of deceptive design pattern.

### 1 Complex and confusing language: Technical and/or excessively long privacy policies that are difficult to understand

Websites and mobile apps that use complex and confusing language in their privacy policies make it difficult for users to understand how their personal information is collected, used and disclosed.

#### Examples:



Long and difficult to understand privacy policies



Confusing pop-up privacy notices

#### OPC key findings:

- **Complex and confusing language** was the most common type of deceptive design pattern and appeared in 96 per cent of websites and mobile apps
- 83 per cent of privacy policies were **difficult to read** (required university or graduate education reading level)
- 76 per cent of privacy policies were **very long** (over 3,000 words)

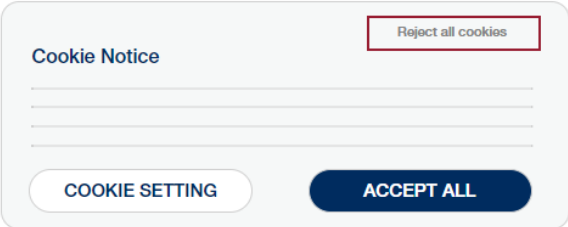
#### OPC recommendations:

- ✓ Privacy information should be **easy to understand**
- ✓ Privacy policies should **include simple explanations with key information** (additional details could be linked)

## 2 Interface interference: Design elements that can influence users' perception and understanding of their privacy options


Interface interference occurs when a website or mobile app uses design elements that are distracting, conflicting or confusing, making it difficult for users to understand their privacy options.

**Examples:**




**False hierarchy:**  
The privacy option that the organization wants the user to choose is emphasized/more obvious, while the more privacy-protective option is obscured/less visible (e.g., a cookie banner that has a prominent "ACCEPT ALL" button and a muted "Reject all cookies" button)

**Pre-selection:**



The privacy option that the organization wants the user to choose is a default setting, while the more privacy-protective option requires the user to take action (e.g., pre-selection of a setting that allows the organization to sell personal information)

**Confirm-shaming:**



Emotionally charged language is used to persuade the user to choose the privacy option that the organization wants the user to select, when the user attempts to make a more privacy-protective choice (e.g., using "we're sad to see you go" language when a user attempts to delete an account)

**OPC key findings:**

- 65 per cent of websites and mobile apps used a **false hierarchy** in the privacy settings
- 65 per cent of websites and mobile apps had default privacy settings where a **less privacy-protective option was pre-selected**
- 20 per cent of websites and mobile apps used **confirm-shaming in the account deletion process**

**OPC recommendations:**

- ✓ Privacy options should be **displayed equally and be equally visible**
- ✓ Even where opt-out consent is a valid form of consent under privacy laws, organizations should **require users to take action** to provide consent
- ✓ Less privacy-protective options should **not be pre-selected** as a default setting
- ✓ Privacy options should be **presented in neutral language**

### 3 Nagging: Repeated prompts for users to take specific actions that may undermine their privacy interests

Nagging occurs when repeated prompts or requests are used to frustrate users into choosing the privacy option that the organization wants users to select.

**Example:**



Repeated requests/prompts to sign up for an account or provide an email address (e.g., pop-ups, persistent banners, etc.)

<p><b>OPC key findings:</b></p> <ul style="list-style-type: none"> <li>15 per cent of websites and mobile apps engaged in nagging generally</li> <li>30 per cent of websites and mobile apps engaged in nagging during the account registration and deletion processes</li> </ul>	<p><b>OPC recommendations:</b></p> <ul style="list-style-type: none"> <li>✓ Avoid repeatedly asking users to provide more personal information than necessary, especially once they have declined the first request</li> </ul>
---	--

### 4 Obstruction: The insertion of unnecessary, additional steps between users and their privacy-related goals

Obstruction occurs when the design of a website or mobile app makes it difficult for users to make privacy-protective choices.

**Examples:**



User experiences “click-fatigue” (i.e., an unreasonable number of steps/clicks) in the account deletion process, and are discouraged from completing the process



Privacy information, settings and options are difficult to find

<p><b>OPC key findings:</b></p> <ul style="list-style-type: none"> <li>36 per cent of websites and mobile apps engaged in obstruction</li> <li>25 per cent of websites and mobile apps allowed users to find the option to delete their account in two clicks or less</li> </ul>	<p><b>OPC recommendations:</b></p> <ul style="list-style-type: none"> <li>✓ Limit the number of steps (and clicks) it takes to complete a task</li> <li>✓ Make it easy to find privacy information, settings and options</li> </ul>
--	---

## 5 Forced action: Requiring or tricking users into disclosing more personal information to access a service than is necessary to provide that service

Forced action occurs when a website or mobile app forces users to take a specific action to access a service, when that action is not necessary to provide the service.

**Example:**



User is unnecessarily forced to sign up for an account to access the service

### OPC key findings:

- 16 per cent of websites and mobile apps had forced actions

### OPC recommendations:

- Do not force users to provide more personal information than necessary to access a service

## Children’s privacy rights

As part of the Sweep, the OPC, the Office of the Information and Privacy Commissioner of Alberta (the OIPC-AB) and the Office of the Information and Privacy Commissioner of British Columbia (the OIPC-BC) also examined the use of deceptive design patterns in 67 websites and mobile apps targeted at children. The Report highlights the commitments that each of these three information and privacy commissioner offices have recently made to children’s privacy rights and discusses the vulnerability of children in online environments.

The Report states: “While it is important for organizations to avoid deceptive design patterns on their websites and apps so that users can make informed privacy choices free of manipulation, the OPC, OIPC-AB and OIPC-BC wish to emphasise that it is particularly crucial to ensure privacy-protective design by default for websites and apps that may be appealing to children.”<sup>4</sup>

## International collaboration and a potential area for future enforcement

The Sweep exemplifies a trend of increased international collaboration among privacy and other regulatory enforcement authorities. Notably, 2024 was the first year that GPEN coordinated the Sweep with the International Consumer Protection and Enforcement Network. [GPEN’s report](#) identified the Sweep as “the most extensive example of cross-regulatory cooperation between privacy and consumer protection authorities, to date”, recognizing “the increasing intersection of the two regulatory spheres in the digital economy.”<sup>5</sup>

This year’s theme of online deceptive design patterns signals that this might be an area for future increased attention by privacy and other regulatory enforcement authorities in Canada and globally. If deceptive design patterns become a priority for enforcement actions, we may see Canadian privacy commissioner investigations into not only the substance of privacy policies and practices employed on organizations’ websites and mobile apps, but also the form. Accordingly, organizations should be aware of deceptive design patterns and how to avoid implementing these, particularly when seeking to obtain meaningful consent online.

## Meaningful consent

Under Canadian privacy laws, private sector organizations must generally obtain meaningful consent for the collection, use and disclosure of personal information. While the specific wording used and obligations vary amongst Canadian personal information protection statutes, this generally means that individuals must be informed of the type of personal information being collected, used and disclosed and the purposes for such collection, use and disclosure. In addition, consent must not be obtained through deception and organizations must not mislead or deceive individuals in connection with obtaining consent.

Canadian privacy commissioners have previously issued guidelines to provide organizations with additional information on how to obtain meaningful consent. See for example [Guidelines for obtaining meaningful consent](#) published jointly by the OPC, the OIPC-AB and the OIPC-BC, [PIPEDA Fair Information Principle 3 – Consent](#) published by the OPC, and [Lignes directrices 2023-1 – Consentement: critères de validité](#), published by the Québec Commission d'accès à l'information (please see [BLG's unofficial translation](#) for more information).

Canadian privacy commissioners have also previously issued best practices and tips for organizations operating in online environments. See for example OPC publications [Seizing opportunity: Good privacy practices for developing mobile apps](#), [Ten tips for a better online privacy policy and improved privacy practice transparency](#), and [Ten tips for communicating privacy practices to your app's users](#).

In the Report and the Guidance, the OPC builds upon these previous Canadian privacy commissioner publications and takes an even more hands-on approach by providing organizations with actionable items to implement into the design of their online platforms. Together, the Report and the Guidance emphasize a “privacy by design” and “privacy by default” approach and illustrate the OPC’s expectations when it comes to obtaining meaningful consent in an online environment.

While Canadian personal information protection laws are generally technology-neutral and do not specifically prohibit the use of online design patterns that the OPC has characterized as “deceptive”, organizations risk failing to obtain meaningful consent by implementing these designs in their websites and mobile apps.

Canadian privacy commissioners have previously considered design features such as length (e.g., number of pages and words), means of access (e.g., mobile device), and readability (e.g., font size and links) of online privacy policies, as well as the use of consent toggles, when determining issues around consent. See for example [Investigation Report P2021-IR-02 Investigation into Babylon by TELUS Health's compliance with Alberta's Personal Information Protection Act](#).

## Key takeaways

Canadian privacy commissioners have signalled that they have online deceptive design patterns on their radars. Organizations should be prepared for examination of both the substance and form of the privacy policies and practices on their websites and mobile apps, in the event of a complaint or an investigation. Additionally, a higher level of scrutiny may be deployed on websites and mobile apps targeted at children.

Organizations should review the Report and the Guidance, as well as their current privacy management policies, procedures and practices with respect to their online platforms and work with their UX design teams to reduce the occurrences of deceptive design patterns. Organizations should ensure that when they are obtaining consent online, that the consent is meaningful and valid in light of the OPC’s expectations around avoiding deceptive design patterns.

<sup>1</sup> Canada, Office of the Privacy Commissioner of Canada, [Office of the Privacy Commissioner of Canada Sweep Report 2024: Deceptive Design Patterns](#) (2024), at p 3.

<sup>2</sup> The Report at p 3.

- 3 The privacy enforcement authorities participating in the Sweep selected the five deceptive design patterns based on criteria set out by the Organisation for Economic Co-operation and Development (OECD) in its [Dark Commercial Patterns](#) paper published on Oct. 26, 2022, which set out a working definition of dark commercial patterns.
- 4 The Report at p 28.
- 5 Global Privacy Enforcement Network, [GPEN Sweep 2024: "Deceptive Design Patterns" Report](#) (2024), at p 3.

[Danielle Windt](#), [Eliot Escalona](#)

Expertise

[Cybersecurity, Privacy & Data Protection](#), [Retail & Hospitality](#), [Technology](#)

---

## BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

[blg.com](#)

### BLG Offices

#### Calgary

Centennial Place, East Tower  
520 3rd Avenue S.W.  
Calgary, AB, Canada  
T2P 0R3

T 403.232.9500  
F 403.266.1395

#### Ottawa

World Exchange Plaza  
100 Queen Street  
Ottawa, ON, Canada  
K1P 1J9

T 613.237.5160  
F 613.230.8842

#### Vancouver

1200 Waterfront Centre  
200 Burrard Street  
Vancouver, BC, Canada  
V7X 1T2

T 604.687.5744  
F 604.687.1415

#### Montréal

1000 De La Gauchetière Street West  
Suite 900  
Montréal, QC, Canada  
H3B 5H4

T 514.954.2555  
F 514.879.9015

#### Toronto

Bay Adelaide Centre, East Tower  
22 Adelaide Street West  
Toronto, ON, Canada  
M5H 4E3

T 416.367.6000  
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing [unsubscribe@blg.com](mailto:unsubscribe@blg.com) or manage your subscription preferences at [blg.com/MyPreferences](http://blg.com/MyPreferences). If you feel you have received this message in error please contact [communications@blg.com](mailto:communications@blg.com). BLG's privacy policy for publications may be found at [blg.com/en/privacy](http://blg.com/en/privacy).

© 2024 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.