OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Identifying and mitigating harms from privacy-related deceptive design patterns

Federal, Provincial, Territorial Information and Privacy Commissioners and Ombuds Resolution - November 2024

Resolution

1 Context

In recent years, both international and domestic regulatory authorities have been seized with the issue of deceptive design patterns (or 'dark patterns'), identifying and analysing such practices from angles of competition, consumer protection and privacy. Deceptive design patterns ('DDPs') are used on websites and mobile apps to influence, manipulate, or coerce users to make decisions that are not in their best interests.[1] This phenomenon has grown more pronounced as more and more commercial activity takes place online.

Internationally, several data protection authorities and intergovernmental organizations have published reports on deceptive designs.[2] Most of these reports seek to define design patterns that have effects on a variety of regulatory issues, such as competition policy (i.e. drip pricing)[3], privacy (i.e. default privacy settings) and consumer protection more broadly (i.e. baseless countdown timers[4]). Until recently, there has been a lack of international reports specifically addressing narrower privacy related DDPs.

In 2024, the Global Privacy Enforcement Network (GPEN) launched a Sweep focused on privacy-related DDPs. The 'Sweepers', which included Canadian federal, provincial, and territorial privacy regulators/ombudspersons as well as international privacy authorities, examined over 1000 websites and apps across various sectors, such as retail, social media, news and entertainment, health and fitness, as well as websites and apps that appear to be aimed at children.

In this Sweep, the authorities encountered different DDPs with the potential to affect user privacy, many of which have been seen by Canadian privacy regulators in investigations and research projects. Examples of DDPs most frequently affecting privacy include the following categories[5]:

- The use of complex and confusing language on websites or apps, often found within highly technical and excessively long privacy policies or terms of service;

- Interface interference – where design elements on the website or app can be used to influence a user's perception and understanding of their privacy options;

- Nagging – where repeated prompts for users to take specific actions may undermine their privacy interests;

- Obstruction – where a website or app inserts unnecessary, additional steps between users and their privacy-related goals;

- Forced action – where a website or app requires or tricks users into providing more personal information to access a service than is necessary to provide that service.

The international report concluded that there is 'an extremely high occurrence' of DDPs across websites and apps worldwide, and that 'users are likely to encounter, in the vast majority of cases, at least one DDP when interacting with websites and apps.'[6] In the Canadian context, the OPC Sweep team found examples of at least one privacy-related DDPs in 99% of the 145 websites and apps it examined.[7]

These results are concerning, but not surprising. Provincial and territorial privacy regulators/ombudspersons have also identified areas in which deceptive design patterns are appearing more prominently.

Given the number of privacy-related DDPs encountered within the digital landscape and the harms that can come from them, it is clear that action must be taken. The signatories believe it is important for businesses and governments to avoid certain practices when designing websites for users to provide their personal information and to meet fundamental legal obligations and basic privacy principles when collecting personal information online.

2 Therefore

Canada's federal, provincial and territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight are calling on public and private organizations to design their platforms to avoid practices that would manipulate or coerce users into making decisions that go against their privacy interests and to provide users with the ability to make informed privacy decisions.

More specifically, they collectively urge public and private organizations to:

1. Ensure that privacy is built into the website or app by default, using the concept of privacy-by-design as the basis for a design framework.
2. Limit personal information collection to that which is necessary for the purpose of its collection, use and disclosure, as DDPs such as forced action and interface interference are often used to obtain more personal information than is necessary for the service;
3. Promote transparency when collecting personal information using clear and simple language as a way of both complying with privacy laws as well as fostering trust between the organization and its users;
4. Examine the design architecture of their website(s) and/or app(s) in order to determine the prevalence of DDPs and to make changes to these platforms to limit a user's exposure to DDPs as well as provide users with the ability to make informed privacy decisions;
5. Choose design patterns that adhere to privacy principles as found in Canadian privacy legislation, have the best interest of the user in mind and avoid the use of designs that create negative habitual behaviours, which may violate those principles.[8]

Good privacy design practices include:

- Defaulting websites and apps to their most privacy-protective settings and, in the case of apps, ensure that this is applied to any subsequent updates made to newer versions;
- Emphasizing privacy-protective options to users and not selecting privacy-invasive ones;
- Using neutral language and designs to present privacy choices to users;
- Ensuring that privacy settings are accessible at all times, not only upon the first visit to a webpage or use of an app in order to empower individuals to make privacy decisions when they want to;
- Reducing the volume of clicks required to navigate and adjust users' privacy choices; and
- Providing just-in-time consent options that allow users to make privacy decisions when they are contextually relevant.

For their part, Federal, Provincial and Territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight commit to engaging with government and other stakeholders in the modernization of design architecture for websites and apps that reduces the number of DDPs while promoting privacy-protective design patterns.

Endnotes

1 OECD, Dark Commercial Patterns, 2022; EDPB, Guidelines on Deceptive Design Patterns, 2023; OPC, Canada Sweep Report 2024: Deceptive Design Patterns, 2024.

2 For example, in 2022, the Organisation for Economic Cooperation and Development ('OECD') issued a report on dark commercial patterns. Similarly, the European Commission ('EC') published a behavioural study on unfair commercial practices in the digital environment centered on DDPs and the European Data Protection Board ('EDPB') issued guidelines on deceptive design patterns in social media platform interfaces. The Federal Trade Commission ('FTC') also put forward a report on dark patterns under its role as a consumer protection agency.

3 Drip pricing, as per the definition in the FTC's report on dark patterns, is a DDP 'in which firms advertise only part of a product's total price to lure in consumers, and do not mention other mandatory charges until late in the buying process.'

4 Baseless countdown timers, as per the definition in the FTC's report on dark patterns, are a DDP that create 'pressure to buy immediately by showing a fake countdown clock that just goes away or resets when it times out.'

5 GPEN, 'GPEN Sweep 2024: Deceptive Design Patterns', 2024.

6 GPEN, 'GPEN Sweep 2024: Deceptive Design Patterns', 2024.

7 OPC, 'Sweep Report 2024: Deceptive Design Patterns', 2024.

8 5Rights Foundation, 'Disrupted Childhood: the cost of persuasive design', 2023.