OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

News Release

For immediate release

July 9, 2024

GPEN Sweep finds majority of websites and mobile apps use deceptive design to manipulate privacy choices

VICTORIA— A global privacy sweep that examined more than 1,000 websites and mobile applications (apps) has found that nearly all of them employed one or more deceptive design patterns that made it difficult for users to make privacy-protective decisions.

Deceptive design patterns – otherwise known as 'dark patterns' - are features that steer users towards options that may result in the collection of more of their personal information. These patterns may also force users to take multiple steps to find a privacy policy, log out, or delete their account, or present them with repetitive prompts aimed at frustrating them and ultimately pushing them to give up more of their personal information than they would like.

This year's annual Global Privacy Enforcement Network (GPEN) Sweep took place between January 29 and February 2, 2024. It involved participants, or "sweepers," from 26 privacy enforcement authorities from around the world.

The OIPC BC focused on websites targeting children to further its commitment to promoting and protecting the privacy rights of young people. That commitment has included calling for a Children's Code, which would bolster guidance to businesses on safeguards for handing the data of young people that address the specific challenges and unique harms youth face when they engage online.

"Our children are particularly vulnerable to overcollection of their personal information online," said Michael Harvey, Information and Privacy Commissioner for British Columbia. "We found a higher incidence of deceptive design patterns in Canada than in other countries, and that children are more often the targets. These websites are deceiving and manipulating our kids into revealing their private information - so that they can use it to further deceive and manipulate them. These are real harms to our children and when a child is harmed, so are we all. We call upon websites and apps to end these 'dark patterns' and limit the collection and use of our kids' personal information."

For the first time, the GPEN sweep was coordinated with the International Consumer Protection and Enforcement Network (ICPEN), which represents consumer protection authorities. The collaboration recognizes the growing intersection between privacy and other regulatory spheres. In the case of deceptive design patterns, it was clear to both privacy and consumer protection sweepers that many websites and apps employ techniques that interfere with individuals' ability to make choices that best protect their privacy or consumer rights.

Both GPEN and ICPEN, who are working together to improve privacy and consumer protection for individuals around the world, published reports today outlining their findings.

Those involved in the privacy sweep replicated the user experience by engaging with websites and apps to assess the ease with which they could make privacy choices, obtain privacy information, and log out of or delete an account.

Sweepers evaluated the sites and apps based on five indicators identified by the Organisation for Economic Co-operation and Development (OECD) as being characteristic of deceptive design patterns.

For each indicator, the GPEN report found:

- **Complex and confusing language:** More than 89% of privacy policies were found to be long or use complex language suited for those with a university education.
- **Interface interference:** When asking users to make privacy choices, 42% of websites and apps swept used emotionally charged language to influence user decisions, while 57% made the least privacy protective option the most obvious and easiest for users to select.
- **Nagging:** 35% of websites and apps repeatedly asked users to reconsider their intention to delete their account.
- **Obstruction:** In nearly 40% of cases, sweepers faced obstacles in making privacy choices or accessing privacy information, such as trying to find privacy settings or delete their account.
- **Forced action:** 9% of websites and apps forced users to disclose more personal information when trying to delete their account than they had to provide when they opened it.

Canadian results

The Office of the Information and Privacy Commissioner for BC (OIPC BC) collaborated with the Office of the Information and Privacy Commissioner for Alberta (OIPC AB) and the Office of the Privacy Commissioner for Canada (OPC) to examine deceptive design patterns on websites that appear to be aimed at children.

Canadian sweepers found that 56% of children's websites and apps displayed a false hierarchy by making the option to sign up to the service more prominent than that to continue without an account. On 54% of the children's websites and apps, Canadian sweepers encountered charged language that may dissuade users from choosing more privacy protective options, and in 45% of cases, they encountered some form of nagging when interacting with children's websites and apps, i.e., they were repeatedly confronted with the same prompts or requests. The full results can be found in the OPC's report *Use of Deceptive Design Patterns on Websites and Apps that Appear to be Aimed at Children*, that outlines the Canadian Sweep findings.

Parents and guardians should talk to kids about what information they should always be careful about sharing online, how to customize their privacy settings, and how to spot dark patterns when using websites and apps. The OIPC has developed an infographic *How to identify dark patterns* that provides tips for families as they navigate the digital landscape.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

News Release

What is next?
The Sweep was not an investigation, nor was it intended to generate formal findings regarding confirmed violations of privacy legislation. However, as in previous years, concerns identified during the Sweep could result in follow-up work such as outreach to organizations and may also lead to the initiation of enforcement action to address identified concerns. Decisions on further specific enforcement action will be made by each GPEN member independently.

GPEN encourages organizations to design their platforms, including associated privacy communications and choices, in a manner that supports users in making informed privacy choices that reflect their preferences. Good design includes default settings that best protect privacy; an emphasis on privacy options; neutral language and design to present privacy choices in a fair and transparent manner; fewer clicks to find privacy information, log out, or delete an account; and 'just-in-time' contextually relevant consent options. By offering users online experiences that are free from influence, manipulation, and coercion, organizations can build user trust and make privacy a competitive advantage.

Links
GPEN Sweep 2024 – Deceptive Design Patterns – Report
ICPEN - Report
Use of Deceptive Design Patterns on Websites and Apps that Appear to be Aimed at Children - Report
How to identify dark patterns – Infographic

About GPEN
GPEN was established in 2010 upon recommendation by the OECD. Its aim is to foster cross-border cooperation among privacy regulators in an increasingly global market in which commerce and consumer activity relies on the seamless flow of personal information across borders. Its members work together to strengthen personal privacy protections in this global context. The informal network is comprised of over 80 privacy enforcement authorities from around the world.

The privacy sweep is an annual initiative aimed at increasing awareness of privacy rights and responsibilities, encouraging compliance with privacy legislation, and enhancing cooperation between international privacy enforcement authorities. This year's sweep was chaired by the Office of the Privacy Commissioner of Canada.

Media Contact
Michelle Mitchell | Director of Communications
Office of the Information and Privacy Commissioner for BC
250 217-7872 | mmitchell@oipc.bc.ca
Twitter: @BCInfoPrivacy
LinkedIn: https://www.linkedin.com/company/office-of-the-information-and-privacy-commissioner-for-british-columbia/mycompany/