Rapport sur le ratissage du Commissariat à la protection de la vie privée du Canada de 2024

Mécanismes de conception trompeuse

Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

Table des matières

La version html de ce rapport a préséance sur le présent document en cas de divergence.
Ce document est diffusé sur Internet à l'adresse suivante : www.priv.gc.ca

Contexte

Le Commissariat à la protection de la vie privée du Canada a non seulement coordonné le ratissage du Global Privacy Enforcement Network (GPEN) de cette année sur les mécanismes de conception trompeuse (aussi appelées « interfaces truquées »), mais il y a également participé. Outre le Commissariat, 25 autres autorités chargées de l'application des lois sur la protection de la vie privée du monde entier ont pris part à cet effort. Le GPEN est un réseau informel d'autorités chargées de l'application des lois sur la protection de la vie privée qui favorise l'échange d'information, le renforcement des capacités et la collaboration internationale sur les questions en lien avec l'application de la loi. Le ratissage a été mené pour la première fois en collaboration avec l'International Consumer Protection and Enforcement Network (ICPEN), étant donné l'importance mutuelle que revêtent les mécanismes de conception trompeuse pour la protection de la vie privée et des consommateurs.

Les mécanismes de conception trompeuse sont utilisés sur les sites Web et les applications mobiles dans le but d'influencer, de manipuler ou de contraindre les utilisateurs à prendre des décisions qui ne sont pas dans leur intérêt[1].

Ces mécanismes peuvent empêcher les utilisateurs de prendre des décisions éclairées sur la collecte, l'utilisation et la communication de leurs renseignements personnels et les amener à renoncer à leurs droits en la matière dans une mesure plus grande qu'ils ne le souhaiteraient. Les mécanismes de conception trompeuse peuvent être utilisés séparément ou de manière combinée. Lorsque deux ou plusieurs de ces mécanismes sont utilisés de manière combinée, ils peuvent influencer plus efficacement les décisions des utilisateurs en matière de protection de leur vie privée. L'utilisation d'un mécanisme de conception trompeuse peut aussi faciliter le recours à d'autres pratiques du genre en aval.

Les « ratisseurs » du Commissariat ont passé en revue 145 sites Web et applications[2] accessibles au Canada dans divers secteurs, dont la vente au détail, les médias sociaux, les actualités et le divertissement, ainsi que des sites Web et applications qui semblent être destinés aux enfants[3].

1 OCDE, Dark Commercial Patterns (en anglais seulement), 2022; EDPD, Guidelines on Deceptive Design Patterns (en anglais seulement), 2023.

2 Certains sites Web ou applications appartenaient à une même organisation. Le Commissariat a ratissé au total 103 sites Web et 42 applications.

3 Afin de déterminer quelles organisations son ratissage pour la protection de la vie privée allait cibler, le Commissariat a recensé les sites Web et applications les plus populaires consultés au Canada dans divers secteurs.

Le Commissariat était à la recherche de cinq mécanismes précis de conception trompeuse, en fonction des critères établis par l'Organisation de coopération et de développement économiques (OCDE) :

1. Langage complexe et déroutant
Des politiques de confidentialité difficiles à comprendre, car elles sont trop longues ou rédigées dans un langage trop technique.

2. Interférence d'interface
Des éléments de conception qui peuvent influencer la perception et la compréhension par les utilisateurs de leurs options en matière de protection de la vie privée.

3. Harcèlement
Des invites répétées demandant aux utilisateurs de prendre des mesures précises susceptibles de porter atteinte à leurs intérêts en matière de protection de la vie privée.

4. Obstruction
L'ajout d'étapes supplémentaires inutiles entre les utilisateurs et leurs objectifs en matière de protection de la vie privée.

5. Action forcée
Le fait d'exiger des utilisateurs qu'ils communiquent plus de renseignements personnels pour accéder à un service que ce qui est nécessaire pour fournir ce service, ou de les inciter à le faire par la ruse.

D'autres explications, résultats et exemples de ces modèles sont présentés ci-dessous.

Résumé des principales observations du Commissariat

La quasi-totalité des 145 sites Web et applications examinés par les ratisseurs étaient conçus à partir de mécanismes de conception trompeuse : 99 % des sites Web et applications examinés présentaient au moins un indicateur de conception trompeuse (contre 97 % observés à l'échelle mondiale par le GPEN)[4].

Les formulations complexes et déroutantes des politiques de confidentialité représentent le type le plus courant de mécanisme de conception trompeuse qui a été observé. Les ratisseurs ont constaté que, dans 96 % des cas (par rapport à 89 % à l'échelle mondiale), les politiques de confidentialité des sites Web et applications étaient soit trop longues (plus de 3 000 mots), soit rédigées dans un langage technique et déroutant, ce qui les rendait difficiles à lire et à comprendre. Plus précisément, les ratisseurs du Commissariat ont constaté que 33 % des politiques de confidentialité étaient très difficiles à lire (par rapport à la moyenne de 20 % à l'échelle mondiale). En outre, les politiques de confidentialité examinées se sont révélées très longues (76 % d'entre elles comptaient plus de 3 000 mots, comparativement à 55 % à l'échelle mondiale).

Les ratisseurs ont également constaté une utilisation fréquente de deux mécanismes de conception trompeuse : l'obstruction et l'interférence d'interface.

Les ratisseurs ont constaté qu'une proportion importante de sites Web et d'applications avaient recours à l'obstruction et créaient ainsi des obstacles entre les utilisateurs et leurs objectifs, pouvant les dissuader de faire les choix prévus. Plus particulièrement, lorsqu'ils cherchaient à supprimer leurs comptes, les ratisseurs du Commissariat n'ont pu trouver l'option de suppression de compte en deux clics ou moins que sur 25 % des sites Web et applications (par rapport à 17 % à l'échelle mondiale). En outre, dans 43 % des sites Web et applications passés en revue, les ratisseurs n'ont pas été en mesure de trouver l'option pour supprimer leur compte (contre 55 % à l'échelle mondiale).

Les ratisseurs ont également constaté qu'une proportion importante de sites Web et d'applications avaient recours à des interférences d'interface qui encourageaient les utilisateurs à accepter des options protégeant le moins leur vie privée.

4 Le présent rapport compare les mécanismes de conception trompeuse relevés par le Commissariat à ceux observés par les représentants d'autres juridictions. Bien que ces comparaisons soient révélatrices, le ratissage n'avait rien d'une étude scientifique.

Plus précisément, dans 65 % des sites Web et applications ratissés par le Commissariat qui proposaient dès le début de la navigation de faire des choix en matière de protection de la vie privée, les options les plus attentatoire à la vie privée étaient sélectionnées par défaut (comparativement à 48 % à l'échelle mondiale). Les ratisseurs du Commissariat ont observé des éléments visuels qui orientent les utilisateurs vers des options de paramétrage protégeant le moins la vie privée dans pratiquement la même proportion de cas (soit 65 %, par rapport à 57 % à l'échelle mondiale).

Les mécanismes de conception trompeuse observés par les ratisseurs empêchent les utilisateurs de prendre des décisions éclairées concernant leurs renseignements personnels et servent souvent les intérêts de l'entreprise.

Voici une répartition des sites Web et des applications mobiles examinés dans le cadre du ratissage du Commissariat :

Répartition des sites Web et des applications mobiles par secteur

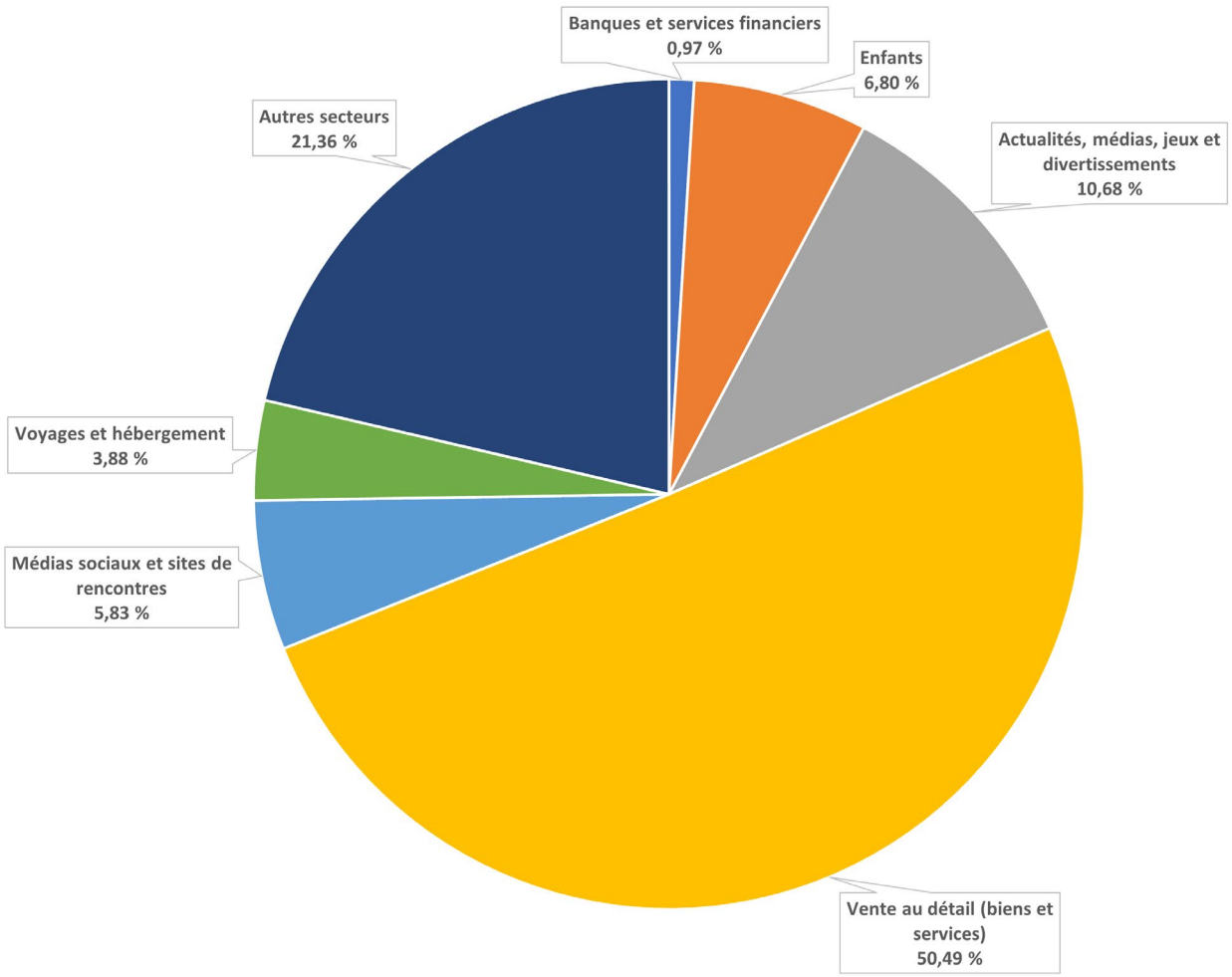


Figure 1 : Répartition des sites Web et des applications mobiles par secteur

Résultats du ratissage du Commissariat

Ci-dessous sont présentés les résultats, les observations et les exemples obtenus dans le cadre du ratissage du Commissariat pour chacun des cinq types de mécanismes de conception trompeuse (ou indicateurs) que les ratisseurs ont recherchés en examinant les sites Web et applications.

Langage complexe et déroutant – indicateur 1

Le ratissage du GPEN a permis de se pencher sur l'accessibilité des politiques de protection de la vie privée, en évaluant la fréquence à laquelle les sites Web et applications ont recours à un langage très complexe et déroutant. Les politiques de confidentialité qui sont longues et qui prêtent à confusion compliquent la prise de décisions des utilisateurs en la matière.

Le langage complexe et déroutant des politiques de confidentialité constitue le mécanisme de conception trompeuse le plus fréquemment observé par les ratisseurs, soit dans 96 % des cas (par rapport à 89 % à l'échelle mondiale).

En général, les ratisseurs du Commissariat ont facilement pu trouver les politiques de confidentialité. Dans 52 % des sites Web et applications passés en revue (par rapport à 59 % à l'échelle mondiale), les ratisseurs ont été en mesure de trouver la politique de confidentialité en un seul clic, et 76 % des politiques ont pu être trouvées en deux clics (par rapport à 73 % à l'échelle mondiale).

Cependant, lorsque les ratisseurs du Commissariat trouvaient ces politiques, elles étaient souvent très longues : 76 % d'entre elles comptaient plus de 3 000 mots (comparativement à la moyenne de 55 % à l'échelle mondiale). En outre, d'après l'indice de lisibilité de Flesch, 83 % des politiques de confidentialité ratissées par le Commissariat se sont avérées difficiles à lire, nécessitant un niveau de lecture de premier cycle universitaire ou des cycles supérieurs, comparativement à 76 % à l'échelle mondiale[5].

De nombreuses personnes pourraient avoir de la difficulté à comprendre le contenu rédigé à un niveau de lecture supérieur à la huitième année[6]. Les gens ne devraient pas avoir à posséder une formation universitaire pour être en mesure de comprendre la politique de confidentialité d'une organisation. Les sites Web et applications doivent mieux communiquer leurs politiques de confidentialité, et celles ci doivent être rédigées en langue claire et simple afin que les utilisateurs puissent prendre des décisions éclairées quant à la collecte, à l'utilisation et à la communication de leurs renseignements personnels.

5 L'indice de lisibilité de Flesch évalue la lisibilité d'un passage en fonction de sa longueur, de la longueur des phrases et du choix de la langue. Plus le score est bas, plus le passage est difficile et plus le niveau d'éducation nécessaire pour le comprendre est élevé. Les ratisseurs ont utilisé Microsoft Word pour déterminer l'indice de lisibilité de Flesch pour chaque application ou site Web.

6 Littératie Ensemble, « Alphabétisation des adultes. Les compétences pour réussir. Rapport national 2022 »; Tourisme et Centre de la statistique de l'éducation.

Lisibilité des politiques de confidentialité

Statistiques mondiales	Statistiques du Commissariat	Lisibilité des messages
2,88 %	0 %	Très facile à lire
6,58 %	0,69 %	Facile à lire
2,33 %	0,69 %	Assez facile à lire
3,29 %	4,14 %	Langage clair
8,77 %	6,90 %	Assez difficile à lire
55,75 %	50,34 %	Difficile à lire
18,22 %	31,72 %	Très difficile à lire
2,19 %	1,38 %	Extrêmement difficile à lire

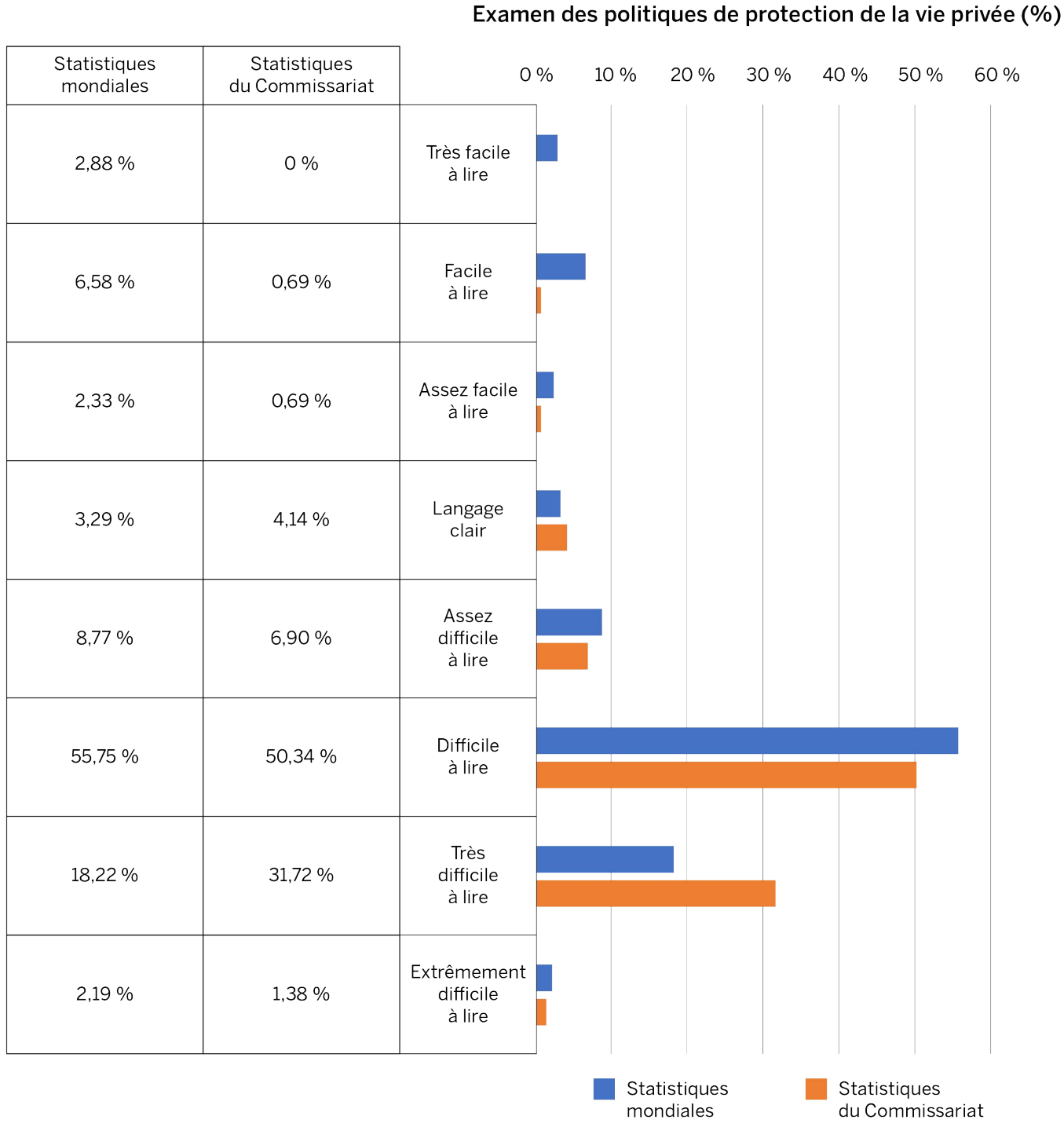


Figure 2 : Lisibilité des politiques de confidentialité : Statistiques du Commissariat comparées aux statistiques mondiales

Interférence d'interface – indicateur 2

Les ratisseurs du Commissariat ont observé, à de nombreuses reprises, des pratiques d'interférence d'interface, soit des éléments d'une interface distrayants et/ou conflictuels qui peuvent occasionner des perturbations ou de la confusion chez l'utilisateur. Les ratisseurs se sont penchés sur trois types d'interférences d'interface : la fausse hiérarchie, la présélection et l'exploitation du sentiment de culpabilité.

Fausse hiérarchie

Une fausse hiérarchie met l'accent sur certains éléments visuels et en escamote d'autres pour diriger les utilisateurs vers des options qui protègent le moins la vie privée. Ces tactiques peuvent, par exemple, consister à rendre certains choix plus grands, plus colorés et plus en évidence (par exemple, « **ACCEPTER TOUT** »), tout en rendant l'option de protection protégeant le plus la vie privée plus petite, plus pâle et plus discrète (par exemple, « refuser tout »). En plaçant l'option qui protège le moins la vie privée au premier plan et au centre de l'écran, ou en rendant moins visible (ou non visible sans faire défiler la page) l'option qui protège le plus la vie privée, la fausse hiérarchie manipule la façon dont les éléments sont affichés à l'écran pour que les utilisateurs choisissent plus facilement l'option protégeant le moins la vie privée.

Au cours de leur examen, les ratisseurs du Commissariat ont constaté que, au moment de l'inscription ou de la suppression d'un compte, on avait recours à la fausse hiérarchie dans 24 % des sites Web et applications (contre une moyenne mondiale de 31 %).

En outre, pendant l'examen des paramètres de confidentialité, les ratisseurs ont observé la pratique de la fausse hiérarchie dans 65 % des sites Web et applications qui ont fait l'objet du ratissage (par rapport à 57 % à l'échelle mondiale).

Voici un exemple tiré du site Web de Prada :

Figure 3 – Exemple de fausse hiérarchie (voir description ci-dessous)

L'« avis relatif aux cookies » (témoins) du site Web de Prada contient deux grandes cases invitant les utilisateurs à ajuster la **CONFIGURATION DES COOKIES** ou simplement à **TOUS ACCEPTER**. L'option « continuer sans accepter » les témoins apparaît dans une zone moins évidente, en caractères gris clair sur fond blanc. Ainsi, la manière dont l'avis est conçu rend l'option protégeant le plus la vie privée plus difficile à voir.

Les sites Web et applications devraient être conçus de manière à ce que les choix relatifs à la protection de la vie privée soient, au moins, également visibles. Nul ne devrait avoir à plisser les yeux pour savoir comment protéger ses renseignements personnels.

Présélection

Ce mécanisme de conception trompeuse fait en sorte que l'option la plus attentatoire à la vie privée est présélectionnée par défaut. Même si les utilisateurs peuvent toujours cliquer sur d'autres options, bon nombre d'entre eux se contenteront d'accepter les choix présélectionnés, car c'est le choix le plus facile. Pour ce qui est des paramètres de confidentialité, 65 % des applications et des sites Web qui ont fait l'objet du ratissage ont présélectionné le choix qui protège le moins la vie privée (comparativement à une moyenne de 48 % à l'échelle mondiale).

Voici un exemple de la présélection d'une option pouvant possiblement porter atteinte à la vie privée tiré du site Web de La-Z-Boy :

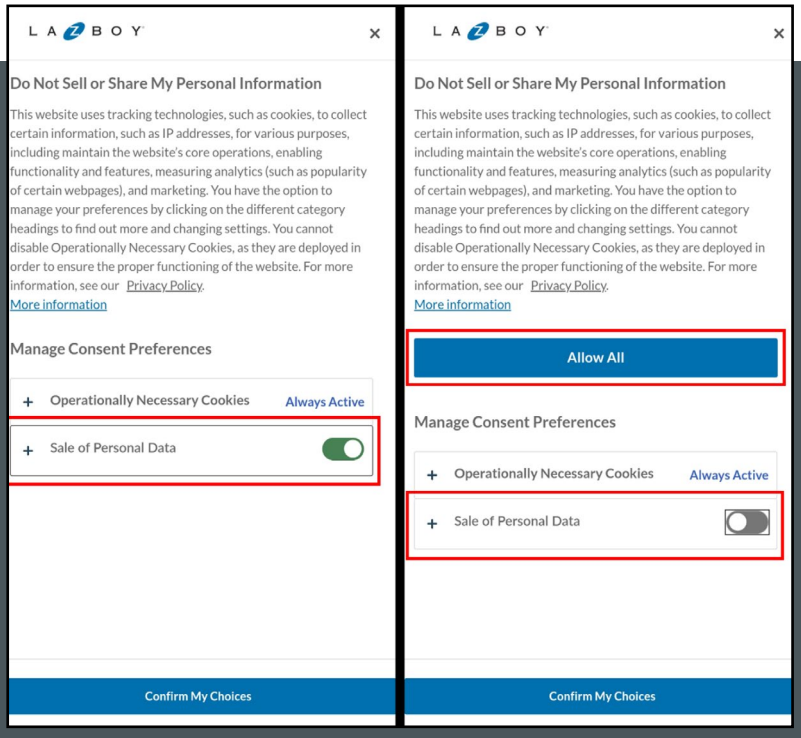


Figure 4 – Exemple de présélection (voir la description ci-dessous)

Les mécanismes de conception trompeuse sont souvent utilisés de manière combinée. L'illustration ci-dessus est un autre exemple de **langage déroutant** (expliqué sous l'indicateur 1), où le titre de l'image peut induire les utilisateurs en erreur et leur faire croire que le choix présélectionné est celui qui protège le plus la vie privée. En dépit de l'en tête indiquant « Do Not Sell or Share My Personal Information » (Ne pas vendre ou partager mes renseignements personnels), l'image de gauche montre que, par défaut, La-Z-Boy peut en effet vendre les renseignements personnels des utilisateurs, sauf si ces derniers prennent des mesures pour refuser.

Comme le montre l'illustration, ce site Web a aussi recours à une **fausse hiérarchie**. Lorsque les utilisateurs désélectionnent l'option « Sale of Personal Data » (Vente de données personnelles), un nouveau bouton « **Allow All** » (Autoriser tout) apparaît au milieu de l'écran. Ce bouton ressemble au bouton « **Confirm my choices** » (Confirmer mes choix) qui se trouve au bas de l'écran, mais il est plus visible que ce dernier, qui a plutôt l'apparence d'un pied de page. Ce mécanisme de conception pourrait amener les utilisateurs à accepter tous les témoins par accident, ce qui irait possiblement à l'encontre de ce qu'ils veulent réellement. En outre, il n'est pas clair pourquoi l'option « Allow All » (Autoriser tout) apparaît lorsqu'un utilisateur décide expressément de désélectionner l'un des choix proposés.

Même lorsque la loi autorise le consentement négatif, les organisations devraient envisager de présélectionner par défaut les options qui protègent le plus la vie privée ou d'exiger des utilisateurs qu'ils choisissent activement s'ils souhaitent donner leur consentement.

Manipulation émotionnelle

La pratique de la manipulation émotionnelle exploite un langage à connotation émotionnelle pour pousser les utilisateurs à se tourner vers les options privilégiées par l'organisation. À titre d'exemple, lorsqu'ils veulent supprimer un compte, les utilisateurs peuvent être confrontés à des expressions comme « Il serait dommage de vous voir partir! » ou, lorsqu'ils sont invités à s'inscrire, ils peuvent être amenés à fermer une fenêtre où il est écrit « Non merci, je préfère payer le plein prix ».

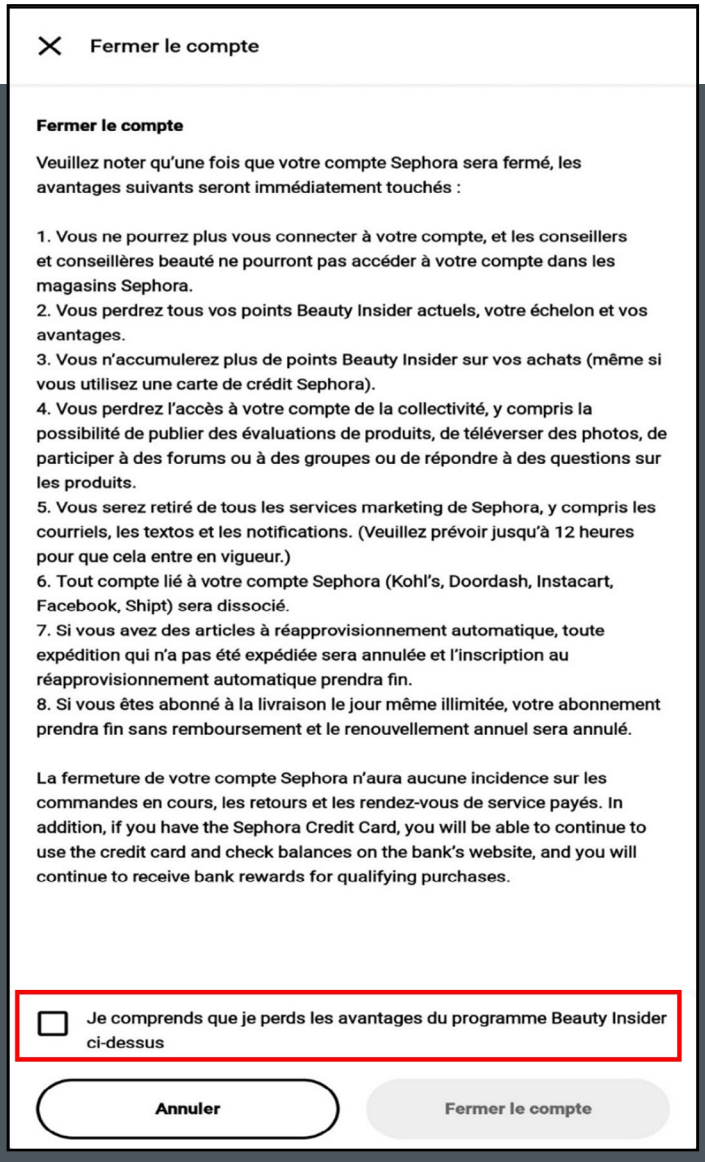


Figure 5 – Exemple de manipulation émotionnelle

Par exemple, la manipulation émotionnelle a été observée dans 20 % des sites Web et applications lorsque les ratisseurs ont essayé de supprimer un compte (contre une moyenne de 29 % à l'échelle mondiale).

Voici un exemple de manipulation émotionnelle tiré du site Web de Sephora :

Sephora informe – à juste titre – les utilisateurs des conséquences de la fermeture de leur compte. Cependant, en présentant ces conséquences comme la « perte » d'une longue liste d'« avantages », l'application exploite un langage à connotation émotionnelle qui peut influencer la décision de l'utilisateur.

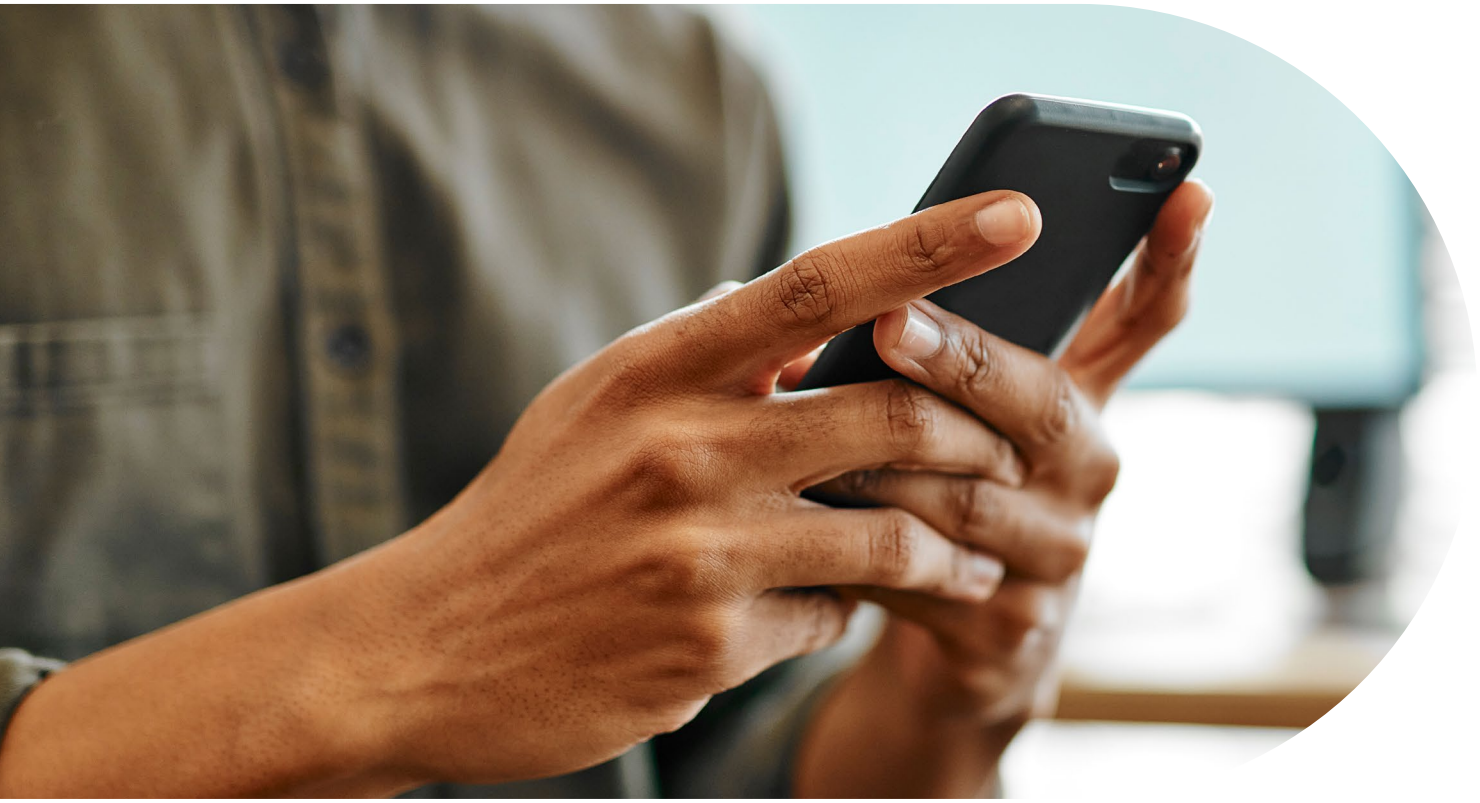
Les sites Web et applications devraient présenter les décisions à prendre en matière de vie privée dans un langage neutre. Après tout, pour bon nombre d'entre nous, la protection de la vie privée est tout aussi importante que la possibilité de réaliser des économies.

Harcèlement – indicateur 3

Le harcèlement est un mécanisme de conception trompeuse qui consiste à envoyer de manière répétée aux utilisateurs les mêmes invites ou requêtes. L'objectif est d'inciter les utilisateurs à faire ce qu'ils ne feraient pas normalement, comme ouvrir un compte, fournir leur adresse électronique sur un site Web ou une application ou passer à la version mobile de l'application ou télécharger celle-ci, ce qui entraînerait une plus grande collecte de renseignements personnels.

En moyenne, les ratisseurs du Commissariat ont observé du harcèlement dans 15 % des interactions sur les sites Web et applications qui ont fait l'objet du ratissage (par rapport à une moyenne de 14 % à l'échelle mondiale)[7].

Toutefois, en ce qui concerne tout particulièrement l'ouverture et la suppression d'un compte, les ratisseurs ont constaté que 30 % des sites Web et des applications avaient recours au harcèlement (comparativement à 35 % à l'échelle mondiale).



7 Dans la suite du présent rapport, le terme « interactions » désigne les tâches précises que les ratisseurs devaient accomplir lors de l'examen des applications et des sites Web (par exemple, prendre une décision concernant les témoins à la demande d'un site Web est une interaction, trouver la politique de confidentialité d'une application en est une autre, etc.).

Voici un exemple de harcèlement tiré du site Web et de l'application de LinkedIn :

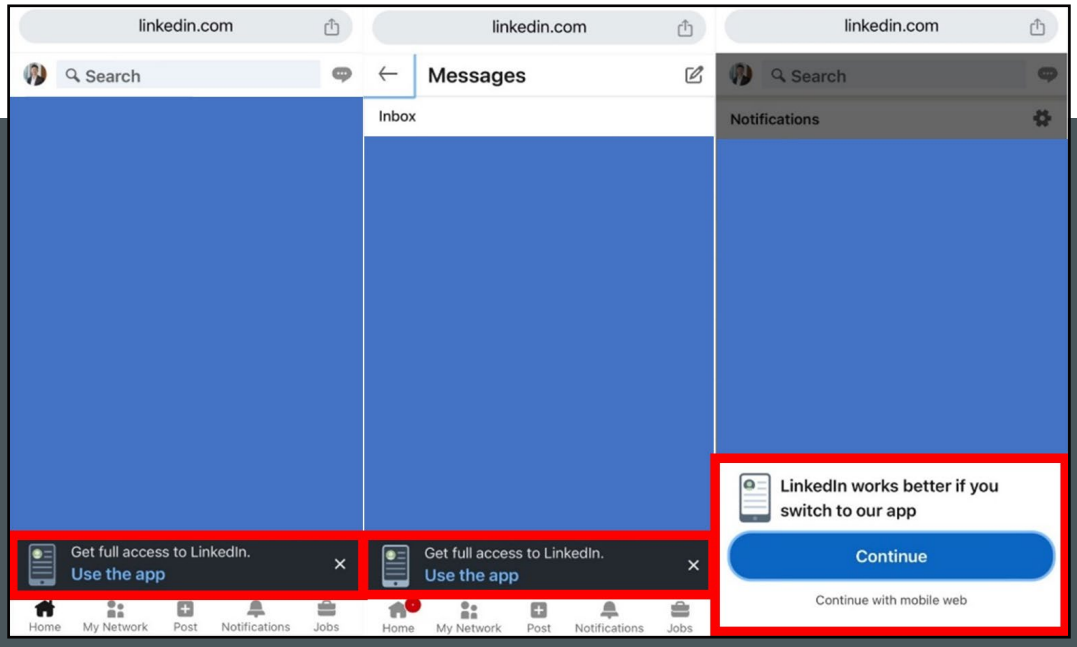


Figure 6 – Exemple de harcèlement[8] (voir l'explication ci-dessous)

Les ratisseurs du Commissariat ont observé que LinkedIn a recours au harcèlement pour inciter les utilisateurs à télécharger son application. L'application peut permettre la collecte et l'utilisation d'une plus grande quantité de renseignements personnels que le site Web, comme l'emplacement GPS en temps réel, les contacts téléphoniques et l'accès à l'appareil photo et au microphone pour la messagerie. Dans le cas présent, le harcèlement se manifeste par des invites répétées qui perturbent l'expérience de l'utilisateur et l'incitent à utiliser l'application plutôt que la version mobile du site Web (mis en évidence dans les encadrés rouges ci-dessus).

Par exemple, le site Web de LinkedIn présente, au bas de l'écran, une bannière persistante qui incite les utilisateurs à « Obtenir un accès complet à LinkedIn » (Get full access to LinkedIn) en utilisant l'application. La bannière se retrouve sur différentes pages, notamment dans les messages et les publications.

Même si les utilisateurs peuvent fermer la bannière afin de naviguer sur la page sur laquelle ils se trouvent, elle réapparaît lorsqu'ils passent à une autre page.

Les ratisseurs ont relevé une variante du harcèlement à l'onglet « Notifications » du site Web de LinkedIn, où les utilisateurs se voient proposer un bouton « Continue » (Continuer) qui apparaît en gras et contraste avec le fond d'écran. Le harcèlement est utilisé en combinaison avec une **fausse hiérarchie**, puisque l'option qui protège le plus la vie privée, soit « Continue with mobile web » (Continuer avec la version mobile du site Web) est présentée en gris clair en dessous et en caractères nettement plus petits.

Le recours à ce type de harcèlement peut éroder la confiance des utilisateurs et la crédibilité du site Web ou de l'application en question.

8 Dans ces exemples, il n'y a pas eu d'interaction avec les utilisateurs ni de collecte de renseignements personnels.

Obstruction – indicateur 4

L'obstruction est un mécanisme de conception trompeuse qui rend la réalisation de certaines tâches, par exemple la recherche des paramètres de confidentialité ou la suppression d'un compte, plus complexe, ce qui dissuade les utilisateurs de les accomplir. La « lassitude du clic », qui oblige les utilisateurs à accomplir un nombre déraisonnable d'étapes pour réaliser une tâche précise, est un type répandu d'obstruction. Ce mécanisme peut frustrer les utilisateurs et les amener à renoncer à leurs intentions ou à agir à l'encontre de celles-ci, ce qui n'est pas forcément dans leur intérêt.

En moyenne, les ratisseurs du Commissariat ont observé des obstructions dans 36 % des interactions sur les sites Web et applications qui ont fait l'objet du ratissage (par rapport à la moyenne de 39 % à l'échelle mondiale).

Plus précisément, lorsqu'ils ont tenté de supprimer des comptes, les ratisseurs du Commissariat n'ont pu trouver l'option de supprimer un compte en deux clics ou moins que sur 25 % des sites Web et applications (comparativement à 17 % à l'échelle mondiale).

En outre, les ratisseurs ont constaté que 43 % des sites Web et applications exigeaient des utilisateurs qu'ils prennent des mesures supplémentaires pour supprimer leur compte (contre une moyenne de 27 % à l'échelle mondiale).

Voici un exemple tiré du site Web de Ticketmaster :

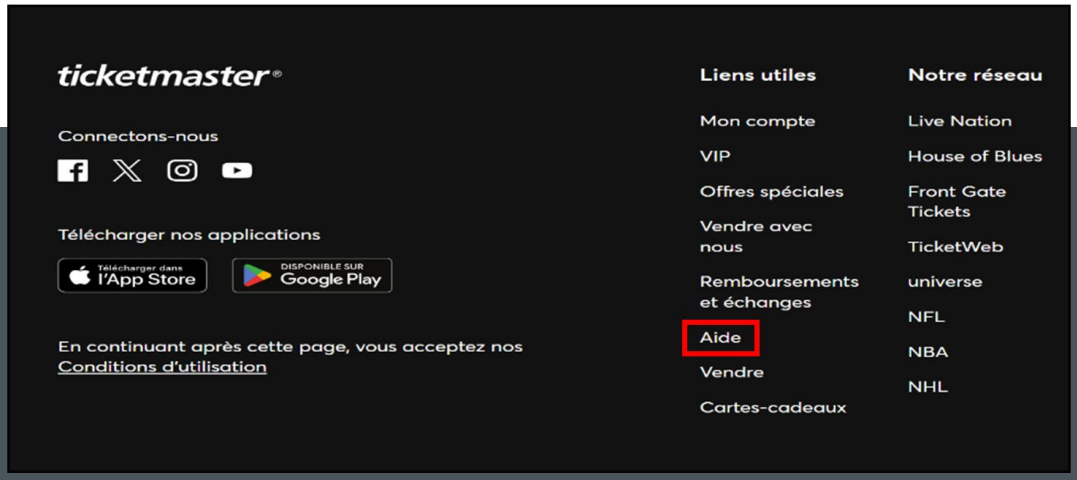


Figure 7 – Exemple d'obstruction (lassitude du clic)

Si un utilisateur souhaite fermer son compte, aucune option claire ne s'offre à lui sur la page « Mon compte » du site Ticketmaster. Il doit naviguer jusqu'au bas de la page Web et cliquer sur le lien « Aide » (voir ci-dessus).

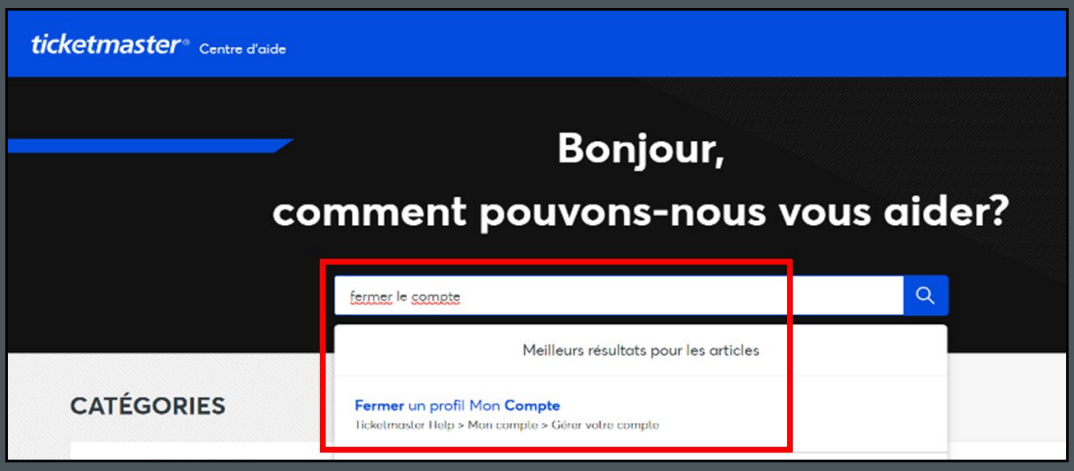


Figure 8 – Exemple d'obstruction (lassitude du clic)

L'utilisateur est ensuite redirigé vers la page du Centre d'aide, où une barre de recherche l'invite à saisir la tâche qu'il souhaite accomplir. Si l'utilisateur tape « fermer le compte », il recevra un lien vers la page « Fermer un profil Mon Compte ».

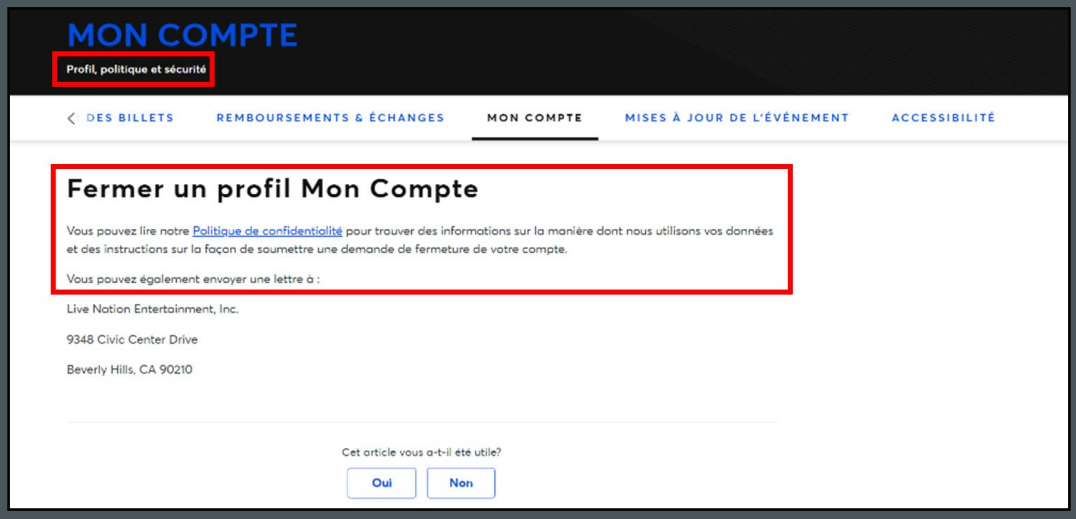


Figure 9 – Exemple d'obstruction (lassitude du clic)

Les utilisateurs qui cliquent sur ce lien sont redirigés vers une page où leur est présentée une adresse physique à laquelle ils peuvent envoyer une lettre pour fermer leur compte (aucune adresse électronique ne leur est fournie) ainsi qu'un lien vers la politique de confidentialité, où il est indiqué qu'ils peuvent trouver des « instructions sur la façon de soumettre une demande de fermeture de [leur] compte ». Or, rien dans la politique de confidentialité Ticketmaster ne précise explicitement comment les utilisateurs peuvent fermer leur compte. En fait, le mot « fermer » ne se trouve nulle part dans cette politique. Au bas de la page, comme le montre la figure 9, Ticketmaster pose la question : « Cet article vous a t il été utile? » Manifestement, la réponse semble être « Non ».

Action forcée – indicateur 5

Les mécanismes de conception trompeuse à action forcée obligent les utilisateurs à prendre des mesures précises sur le site Web ou l'application afin d'accomplir la tâche visée. Une action forcée peut, par exemple, forcer les utilisateurs à communiquer des renseignements personnels en ouvrant un compte, alors que le site Web ou l'application n'a pas réellement besoin de ces renseignements pour fonctionner, ou les obliger à fournir des renseignements supplémentaires avant de pouvoir supprimer leur compte. Ce mécanisme de conception trompeuse limite la capacité des utilisateurs à gérer leurs renseignements personnels.

En moyenne, les ratisseurs du Commissariat ont observé un mécanisme de conception à action forcée dans 16 % des interactions sur les sites Web et applications qui ont fait l'objet du ratissage (contre une moyenne de 21 % à l'échelle mondiale).

Les ratisseurs ont également constaté que 22 % des sites Web et applications n'offraient pas d'options autres que « accepter » ou « tout accepter » en ce qui concerne les paramètres de confidentialité et les témoins (par rapport à une moyenne de 26 % à l'échelle mondiale).

Dans l'exemple suivant, on constate que, sur le site Web de Burger King, la suppression d'un compte force les utilisateurs à communiquer plus de renseignements que lors de la création d'un compte :

Lorsqu'un utilisateur veut créer un compte sur le site de Burger King, il lui suffit de fournir son adresse électronique et son prénom (ou de s'inscrire par l'intermédiaire d'un tiers, comme Google ou Facebook). Or, si l'utilisateur souhaite supprimer son compte, il est contraint de communiquer des renseignements personnels qu'il n'était pas tenu de fournir au départ, notamment son lieu de résidence.

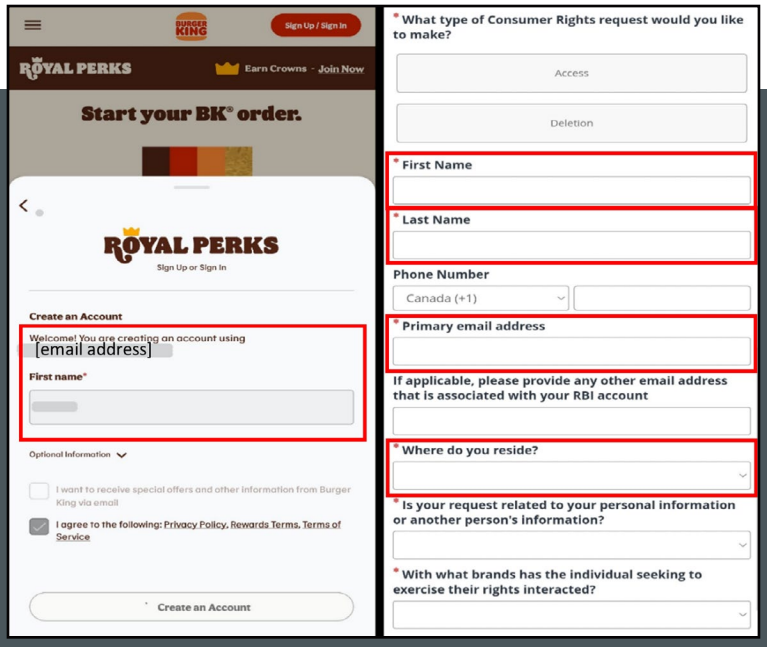


Figure 10 – Exemple d'action forcée

Voici un autre exemple de communication forcée à laquelle les utilisateurs se retrouvent confrontés lorsqu'ils tentent de créer un compte sur le site Web de Zara :

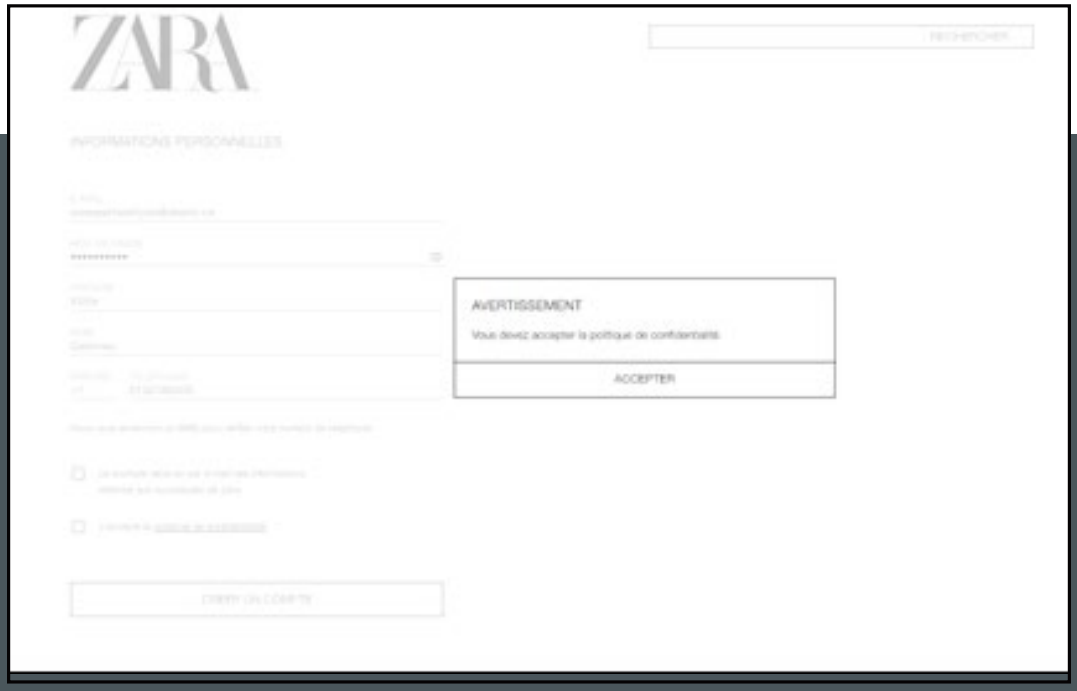


Figure 11 – Exemple de communication forcée et de manipulation émotionnelle

Si un utilisateur tente de créer un compte sur le site de Zara sans cocher la case « J'accepte la politique de confidentialité », une fenêtre contextuelle s'affiche : « AVERTISSEMENT – Vous devez accepter la politique de confidentialité ». La fenêtre contextuelle n'offre pas à l'utilisateur la possibilité de changer d'avis et de renoncer à se créer un compte. En fait, le site empêche l'utilisateur de faire quoi que ce soit sur le site Web, sauf de cliquer sur le bouton « ACCEPTER ». De plus, l'utilisateur ne peut même pas cliquer sur la politique de confidentialité pour la lire. L'utilisateur est donc forcé d'accepter des modalités qu'il ne peut pas lire, ce qui peut l'amener à communiquer plus de renseignements personnels qu'il ne le souhaiterait, ce qui n'est pas forcément dans son intérêt.

Utilisation de mécanismes de conception trompeuse sur les sites Web et applications qui semblent être destinés aux enfants

Contexte

Le Commissariat a collaboré avec le Commissariat à l'information et à la protection de la vie privée de l'Alberta (Office of the Information and Privacy Commissioner of Alberta, ou l'OIPC-AB) et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (Office of the Information and Privacy Commissioner for British Columbia, ou l'OIPC-BC) pour examiner l'utilisation de mécanismes de conception trompeuse sur les sites Web et applications qui semblent être destinés aux enfants (« sites Web et applications destinés aux enfants »). Ensemble, les trois commissariats ont examiné 67 sites Web et applications destinés aux enfants; les conclusions et les statistiques qu'ils en ont tirées figurent ci-dessous.

Le Commissariat a fait de la défense du droit à la vie privée des enfants l'une des trois priorités stratégiques autour desquelles s'articuleront ses travaux de 2024 à 2027. De même, dans son plan d'activités de 2024 à 2027, l'OIPC-AB s'est donné comme priorité stratégique de [traduction] « relever, faciliter et soutenir les possibilités d'améliorer l'accès et la sensibilisation ainsi que les mesures de protection en matière de vie privée des enfants et des jeunes ». Dans le cadre du présent ratissage, l'OIPC-BC s'est concentré sur les sites Web destinés aux enfants pour faire avancer son engagement à promouvoir et à protéger le droit à la vie privée des jeunes.

Cet engagement formulait le souhait d'un « code des enfants », qui imposerait aux entreprises des exigences plus strictes quant aux mesures de protection lors du traitement des données des jeunes et qui tiennent compte des défis et des préjudices auxquels les jeunes sont confrontés lorsqu'ils pratiquent des activités en ligne. Les 4 et 5 octobre 2023, les trois commissariats, en collaboration avec leurs homologues des autres provinces et territoires et des ombuds responsables de la protection de la vie privée, ont également signé une résolution conjointe visant à mettre l'intérêt supérieur des jeunes à l'avant-plan en matière de vie privée et d'accès aux renseignements personnels[9].

Si l'on peut s'attendre à ce que les parents prennent la plupart des décisions relatives à la protection de la vie privée de leurs enfants, des recherches ont montré qu'ils ne comprennent pas toujours bien les activités en ligne de leurs enfants, et que beaucoup sous-estiment le temps que ces derniers passent sur leurs appareils[10]. En d'autres mots, les enfants pourraient naviguer sur des sites Web et des applications à l'insu de leurs parents, ce qui les rend particulièrement vulnérables aux mécanismes de conception trompeuse.

9 Dans la résolution on recommande que les organisations des secteurs public et privé rejettent les pratiques trompeuses.

10 Jenny S. Radesky, Heidi M. Weeks, Rosa Ball, Alexandria Schaller, Samantha Yeo, Joke Durnez, Matthew Tamayo Rios, Mollie Epstein, Heather Kirkorian, Sarah Coyne, Rachel Barr, Young Children's Use of Smartphones and Tablets, Pediatrics, 146 (1) : e20193518, juillet 2020 (en anglais seulement). 10.1542/peds.2019 3518

Résumé des principales observations

Les ratisseurs des trois commissariats ont constaté que certains mécanismes de conception trompeuse, comme la fausse hiérarchie, la manipulation émotionnelle et le harcèlement, étaient beaucoup plus courants sur les sites Web et applications destinés aux enfants que sur ceux qui semblent être à l'intention de la population en général[11].

- En ce qui concerne la création ou la suppression d'un compte, les ratisseurs ont constaté que 56 % des sites Web et applications destinés aux enfants affichent une fausse hiérarchie en mettant en évidence l'option d'inscription au service au détriment du choix de poursuivre sans créer un compte (par rapport à 24 % pour les autres sites Web et applications).

- De même, dans 54 % des sites Web et applications destinés aux enfants qu'ils ont examinés, les ratisseurs ont constaté de la manipulation émotionnelle, c'est à dire à un langage à connotation émotionnelle dans le but de dissuader les utilisateurs de supprimer leur compte (contre 17 % pour les autres sites Web et applications).

- En moyenne, les ratisseurs ont observé une certaine forme de harcèlement dans 45 % des interactions sur les sites Web et applications destinés aux enfants qu'ils ont examinés, c'est-à-dire qu'ils ont été confrontés de manière répétée aux mêmes invites ou requêtes (trois fois plus que sur d'autres sites Web et applications, soit 15 %).

Les enfants et les jeunes, qui ne saisissent pas toujours les conséquences de leur consentement à la collecte, à l'utilisation ou à la communication de leurs renseignements personnels, sont particulièrement vulnérables dans le monde numérique. Il importe donc que les parents puissent facilement prendre des décisions éclairées en matière de protection des renseignements personnels de leurs enfants en ligne.

11 Pour cette section, les statistiques des sites Web et des applications destinés aux enfants sont comparées aux statistiques des autres sites Web et applications examinés par les ratisseurs du Commissariat.

Études de cas

Comme l'indiquent les statistiques ci dessus, de nombreux exemples de mécanismes de conception trompeuse ont été trouvés dans les 67 sites Web et applications destinés aux enfants qui ont été examinés. Toutefois, les ratisseurs ont également trouvé quelques exemples de « bonnes pratiques » qui pourraient contribuer à protéger la vie privée des enfants. Les études de cas ci-dessous visent à illustrer des pratiques préoccupantes et d'autres encourageantes découvertes lors du ratissage des sites Web et applications destinés aux enfants.

Étude de cas : Poki Games

Poki Games est un site Web qui héberge des jeux en ligne gratuits. On y retrouve certains des mécanismes de conception trompeuse les plus couramment observés sur les sites Web et applications destinés aux enfants.

Comme indiqué ci-dessous, il y a deux versions du site, soit Poki.com et kids.poki.com (Poki Kids) :

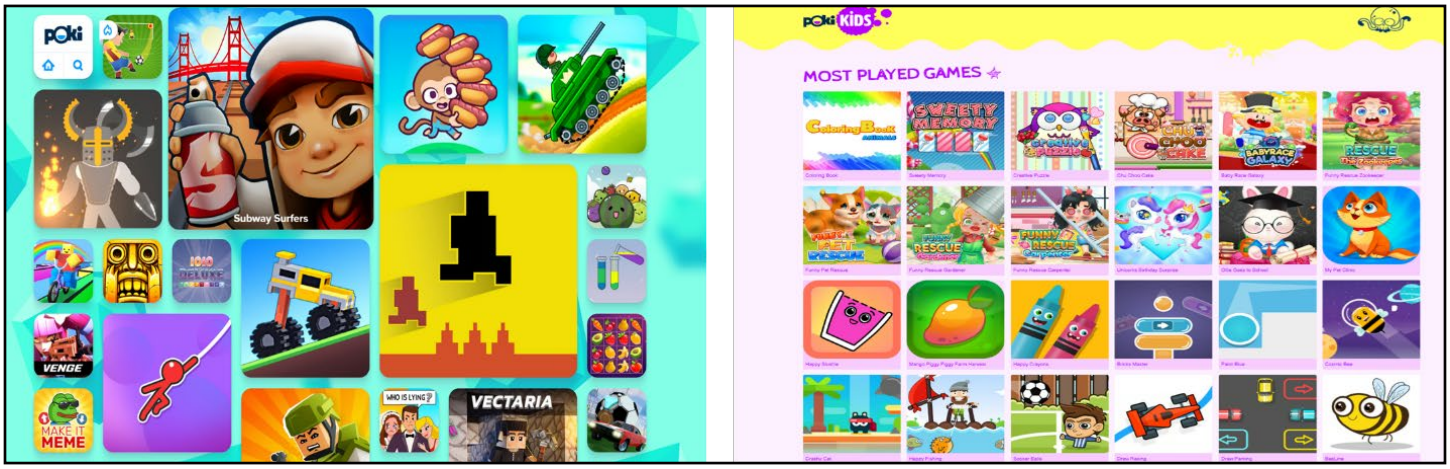


Figure 12 – Poki.com (à gauche) et kids.poki.com (à droite)

Bien que le site Poki Kids soit explicitement destiné aux enfants, la politique de confidentialité de Poki.com prévoit ce qui suit : « Si vous avez moins de 16 ans, ce site n'est pas conçu pour vous » (If you are under the age of 16, this website is not meant for you). Or, nulle part sur la page d'accueil de Poki.com, il est indiqué que le site est destiné aux utilisateurs âgés de 16 ans et plus. En fait, les images colorées des jeux affichés, qui portent des noms qui contiennent des mots comme « singe » ou « ar-en-ciel » (Monkey Mart ou Rainbow Obby), semblent être destinées à des enfants de moins de 16 ans (voir la partie gauche de la figure 12 ci-dessus).

Par conséquent, nous sommes d'avis que de nombreux jeunes enfants sont susceptibles d'utiliser le site Web de Poki, même s'il est censé être destiné à un auditoire de 16 ans et plus. Dans ce contexte, les ratisseurs ont relevé certains mécanismes de conception trompeuse particulièrement préoccupants.

Fausse hiérarchie

D'abord, dans le cas de Poki Games, on constate le recours au mécanisme de fausse hiérarchie : l'option protégeant le plus la vie privée est moins en évidence que l'option de continuer vers le site destiné aux 16 ans et plus. Pour trouver le lien vers Poki Kids (qui prétend recueillir beaucoup moins de renseignements personnels et qui n'utilise pas de témoins de suivi), les utilisateurs doivent cliquer sur un lien en petits caractères gris au bas de la page poki.com. Le Commissariat est d'avis que très peu d'utilisateurs feront défiler de nombreuses pages (plus de 20 écrans dans l'application mobile) et passeront devant des dizaines de jeux vidéo aux couleurs attrayantes pour trouver l'option « Poki Kids » (voir la figure 13 ci-dessous).

Figure 13 – Fausse hiérarchie – l'option qui protège le plus la vie privée se trouve au bas de la page d'accueil

De même, peu d'utilisateurs sont susceptibles de trouver, et encore moins de lire, la politique de confidentialité (qui se trouve à côté de Poki Kids au bas de la page) pour apprendre que Poki Games est, contrairement aux apparences, destiné à des utilisateurs âgés de 16 ans ou plus. Ces utilisateurs n'auraient donc aucune raison de chercher la version pour enfants du site Web.

En outre, les enfants plus âgés qui naviguent sur le site Poki Kids trouveront des jeux qui semblent conçus pour les très jeunes enfants (voir la figure 14 ci-dessous) et pourraient être tentés de retourner sur le site pour 16 ans et plus, ce qui pourrait amener Poki Game à recueillir leurs renseignements personnels.

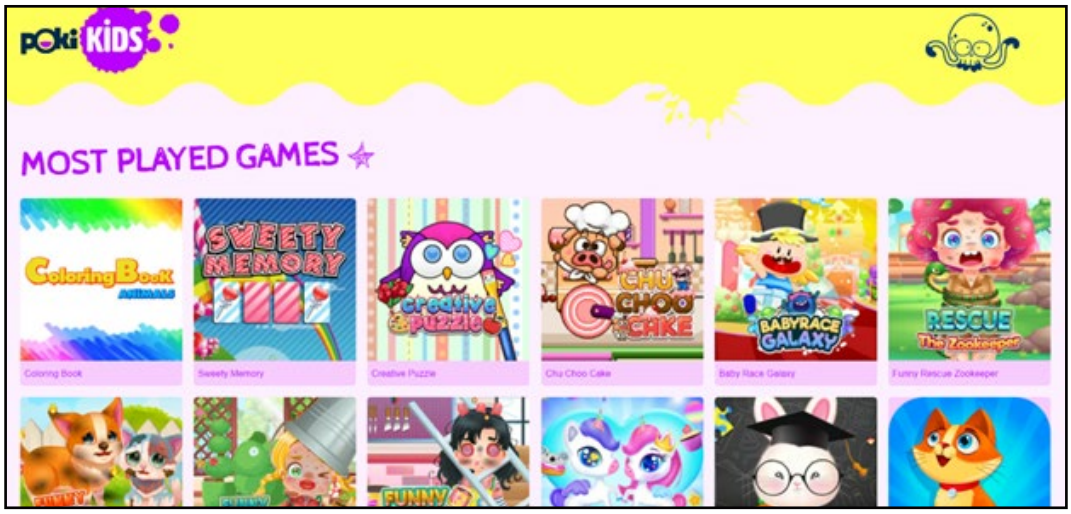


Figure 14 – Page d'accueil du site Poki Kids destiné aux moins de 16 ans

Présélection

Dans le coin inférieur droit de la page d'accueil (voir la figure 15 ci-dessous), le site Poki Games invite les utilisateurs qui visitent le site pour la première fois à tenir compte de leurs paramètres relatifs aux témoins. Une bonne pratique pour les sites Web et les applications consiste généralement à encourager dès le départ les nouveaux utilisateurs à se demander comment leurs renseignements personnels seront recueillis, utilisés et communiqués. Cependant, comme cela est expliqué ci-dessus, ce site est susceptible d'être visité par des enfants, voire par de jeunes enfants (âgés de moins de 13 ans). Il est préoccupant qu'il soit peu probable que ces jeunes utilisateurs attendent d'avoir visité le « Centre responsable de la confidentialité » (Privacy Center) de Poki Games avant de commencer à jouer. Toutefois, même s'ils le faisaient, il est peu probable qu'ils comprennent les décisions relatives à la protection de la vie privée que Poki Games leur demande de prendre ou qu'ils demandent à leurs parents de les aider à prendre ces décisions avant de commencer à jouer (voir la figure 15 ci-dessous).

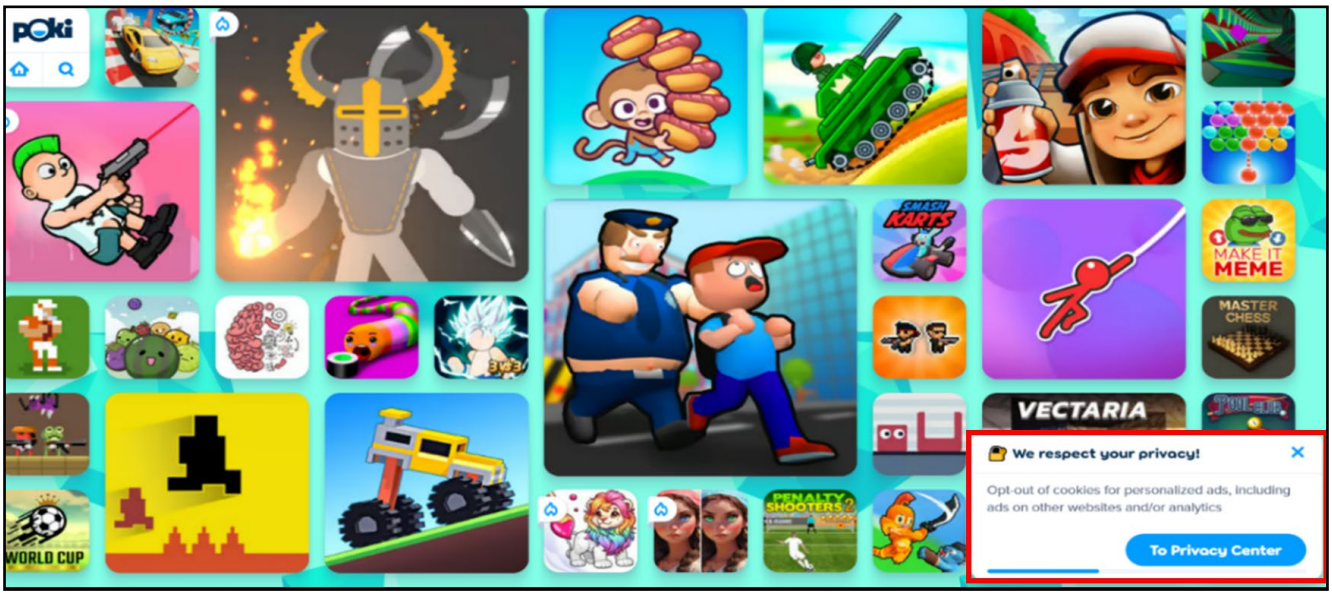


Figure 15 – Poki.com – Page d'accueil avec invite relative à la confidentialité

En outre, même si un utilisateur âgé de 16 ans ou plus se trouvait sur ce site et cliquait sur le lien permettant de visiter le « Centre responsable de la confidentialité » de Poki Game, il constaterait que chacune des options qui protègent le moins la vie privée est sélectionnée par défaut :

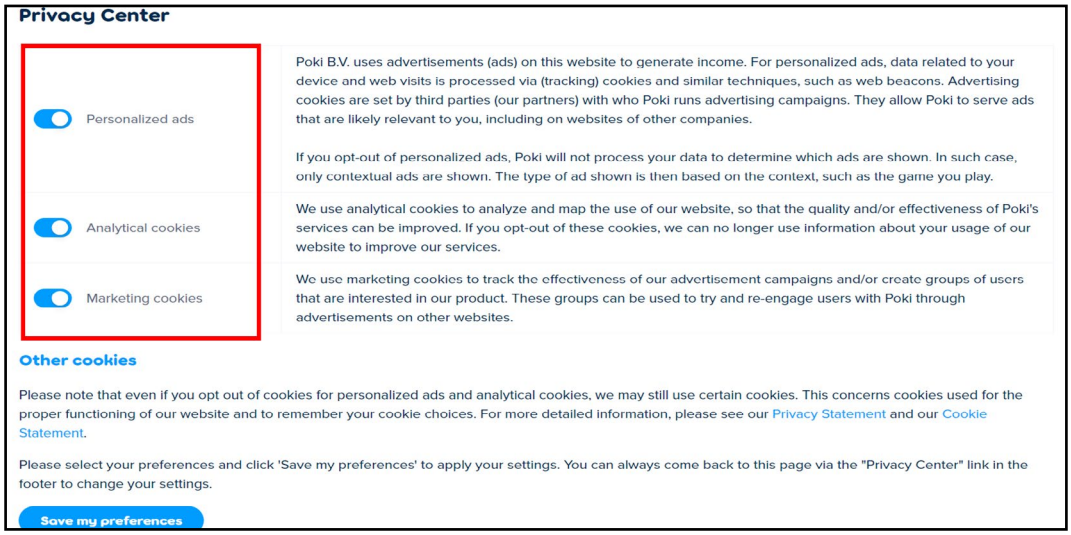


Figure 16 – Présélection

Il s'agit d'un exemple de présélection, un mécanisme de conception trompeuse. Comme l'illustre la figure 15, si les utilisateurs ne cliquent pas sur le bouton « To Privacy Center » (Aller au centre responsable de la confidentialité) dans l'invite sur la confidentialité, ou s'ils cliquent sur le « X » dans le coin supérieur droit de l'invite, les options qui protègent le moins la vie privée demeureront activées.

De plus, les utilisateurs qui choisissent de visiter le centre responsable de la confidentialité devront lire trois explications distinctes et prendre trois décisions distinctes, sans avoir la possibilité de simplement « désactiver tous les témoins » (turn off all cookies), voire de « désactiver tous les témoins sauf ceux qui sont nécessaires » (turn off all but necessary cookies).

Enfin, comme le site Web semble s'adresser à de jeunes enfants et qu'il est susceptible de les attirer, il est particulièrement troublant que le suivi (notamment aux fins de diffusion de publicités personnalisées) soit utilisé sur ce site, et encore plus qu'il soit activé par défaut, ce qui expose les jeunes visiteurs du site au risque d'un suivi inapproprié.

Les concepteurs doivent être conscients que leurs sites Web et applications peuvent attirer ou intéresser les enfants. Ils devraient donc déployer des efforts supplémentaires pour éviter le recours aux mécanismes de conception trompeuse. Il ne suffit pas que les entreprises précisent dans leur politique de confidentialité que la plateforme n'est pas destinée aux enfants; la plateforme devrait également être conçue de manière à réduire le plus possible la probabilité de suivre et de cibler les enfants, et à permettre aux parents ou aux tuteurs à prendre des décisions éclairées en ce qui a trait à la protection des renseignements personnels de leurs enfants.

Étude de cas : LEGO

Les ratisseurs ont relevé certaines bonnes pratiques de conception sur les sites Web de LEGO.

Comme le montrent les exemples ci-dessous, LEGO offre à la fois aux parents et aux tuteurs, ainsi qu'aux enfants, la possibilité de s'informer sur ses politiques de confidentialité et de mieux comprendre la collecte et l'utilisation des renseignements personnels.

Tout d'abord, nous constatons que la politique de confidentialité de Lego.com (la boutique officielle de LEGO) comporte des sections distinctes pour les parents et les enfants (voir la figure 17 ci-dessous) :

Figure 17 – Politique de confidentialité accessible pour les parents et pour les enfants

L'information destinée aux parents et aux tuteurs est rédigée dans un langage correspondant à un niveau de lecture de 12e année, d'après l'indice de lisibilité de Flesch[12], ce qui la rend plus facile à lire que la grande majorité des politiques de confidentialité des sites Web et applications que les ratisseurs canadiens ont examinés (83 %). La section « Information pour les parents » explique, dans un format bien structuré et dans lequel il est facile de se retrouver, comment le site Web recueille et utilise les renseignements personnels des enfants, ainsi que les mesures que les parents ou les tuteurs peuvent prendre pour protéger la vie privée de leurs enfants.

12 Voir la note de bas de page 5.

La section « Information pour les enfants » de la politique de confidentialité de Lego.com comprend un lien vers une courte vidéo adaptée aux enfants qui porte sur les politiques de confidentialité de Lego sur kids.lego.com, un site où les enfants peuvent jouer à des jeux en ligne. De même, les enfants ou les parents ou tuteurs qui visitent le site kids.lego.com trouveront un lien vers la politique de confidentialité dans le coin inférieur droit de l'écran, sans avoir à faire défiler les différents jeux présentés sur la page. Ce lien amène l'utilisateur directement à une vidéo présentant le « Capitaine Sécurité ». La vidéo fournit aux enfants, de manière créative et accessible, des renseignements sur les pratiques de LEGO en matière de protection de la vie privée et sur son utilisation des témoins, et encourage les enfants qui ont d'autres questions sur le sujet à en parler à leurs parents ou à regarder à nouveau la vidéo avec eux (voir la figure 18 ci-dessous) :

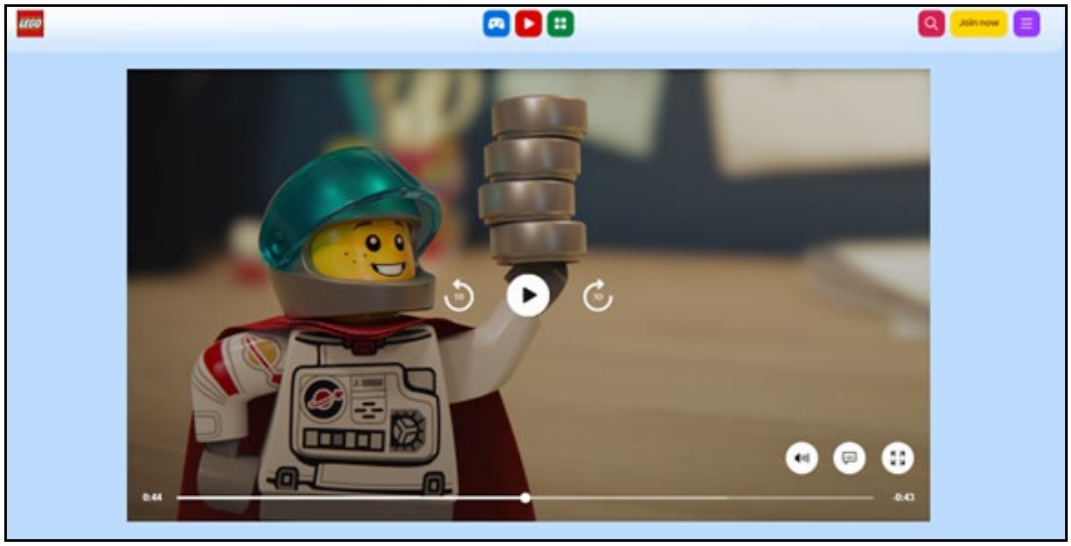


Figure 18 – Vidéo éducative sur la protection de la vie privée destinée aux enfants

En fin de compte, lorsqu'un site Web ou une application est susceptible d'attirer les enfants, les entreprises devraient éviter ou à tout le moins réduire le plus possible la collecte de renseignements personnels auprès des utilisateurs. Dans des cas où il est nécessaire et approprié de recueillir des renseignements personnels auprès des enfants, les entreprises devraient présenter les renseignements relatifs à la vie privée aux enfants dans un format et un langage qui leur sont accessibles, et concevoir leur site Web et leur application de manière à permettre aux parents de facilement faire des choix éclairés pour protéger la vie privée de leurs enfants.

Conclusion

Les ratisseurs ont constaté que les mécanismes de conception trompeuse étaient extrêmement courants sur les sites Web et applications, qu'il s'agisse de ceux destinés aux enfants ou de ceux destinés aux adultes.

Pour certains des indicateurs, les ratisseurs canadiens ont constaté que les mécanismes de conception trompeuse étaient plus fréquemment utilisés au Canada que dans le reste du monde. Par exemple, les ratisseurs du Commissariat semblent avoir trouvé plus de politiques de confidentialité longues et complexes, plus d'options qui protègent le moins la vie privée sélectionnées par défaut, ainsi que plus d'éléments visuels qui incitent les utilisateurs à faire des choix protégeant le moins la vie privée.

Les ratisseurs canadiens se sont aussi heurtés à des obstacles importants. Par exemple, ils ont été incapables de trouver l'option de suppression d'un compte dans près de la moitié des sites Web et applications examinés (où ils avaient l'option de créer un compte).

S'il importe que les organisations évitent les mécanismes de conception trompeuse sur leurs sites Web et leurs applications pour que les utilisateurs puissent faire des choix éclairés en matière de protection de la vie privée, et ce, sans être manipulés, le Commissariat, le Commissariat à l'information et à la protection de la vie privée de l'Alberta et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique souhaitent souligner qu'il est crucial de garantir aux utilisateurs des pratiques qui protègent la vie privée par défaut sur les sites Web et applications susceptibles d'être attrayants pour les enfants. Cela dit, une conception qui souligne l'importance de la protection de la vie privée veille à ce que la protection des renseignements personnels soit intégrée au site Web ou à l'application, quel que soit l'âge de l'utilisateur.

Sur les sites Web et applications destinés principalement aux enfants, on devrait mettre en œuvre par défaut les paramètres protégeant le plus la vie privée et encourager les enfants à parler à leurs parents/tuteurs pour les aider à prendre des décisions en matière de vie privée. De même, les parents/tuteurs devraient pouvoir prendre aisément des décisions éclairées en la matière lorsqu'il s'agit des renseignements personnels de leurs enfants sur les sites Web et applications.

Malheureusement, le Commissariat a constaté que les pratiques trompeuses étaient tout aussi fréquentes, voire plus fréquentes, sur les sites Web et les applications destinés aux enfants. Aussi, le Commissariat encourage vivement les exploitants de sites Web et d'applications à prendre connaissance du présent rapport (ainsi que du rapport sur le ratissage du GPEN 2024) et à évaluer la conception de l'interface de leur plateforme afin de réduire le recours à des mécanismes de conception trompeuse, comme l'obstruction, l'interférence d'interface et le harcèlement. Le fait de garantir le respect et la protection de la vie privée dès la conception des sites Web et applications permettra de créer un environnement en ligne plus sûr pour tous, en particulier pour les enfants, et d'accroître la confiance de tous envers l'environnement numérique à l'échelle mondiale.