Atelier 1 - Ce que racontent nos smartphones sur nous (*et ce qu'ils partagent sans nous le dire*)

L'objectif de cet atelier est d'introduire le sujet **des pisteurs présents sur les smartphones** et de découvrir Exodus Privacy, un **outil pour analyser la présence de ces pisteurs** sur son smartphone Android.

Durée de l'atelier : environ 2h pour une dizaine de personnes.

Matériel nécessaire :

- Salle avec tables et chaises permettant l'accueil d'une dizaine de personnes
- Un vidéo-projecteur, écran et ordinateur connecté à Internet pour l'animateur.trice,
- Une connexion wifi à partager avec le public (pour télécharger l'application Exodus en fin d'atelier), mais les personnes peuvent utiliser leurs données personnelles si il n'y a pas de WIFI disponible,
- Les personnes participantes sont invitées à utiliser leur propre smartphone et leur ordinateur si elles en ont un.

Introduction :

Pour débuter, proposez à votre groupe de faire connaissance en se mettant par binôme avec comme consigne de savoir ***comment se nomme son binôme, depuis combien de temps elle a son smartphone et qu'est ce qu'il/elle fait avec ?*** Au bout de deux minutes, on inverse les rôles et au bout de 5 minutes chaque personne va pouvoir présenter son binôme avec les informations qu'il/elle a collecté. Exemple : « J'étais avec Annick, qui a son nouveau smartphone depuis 2 ans et qui est venue pour savoir quelles applications sont vraiment utiles sur son appareil ». Notez les attentes des participants à l'atelier cela permettra d'orienter la suite de votre atelier et de faire le lien entre les sujets qui vont être abordés et les différentes attentes faites par les personnes présentes et que vous avez notées dans le précédent moment.

N'hésitez pas à **préciser aussi ce qui ne sera pas abordé**, tout en laissant la porte ouverte car ces sujets pourront être abordés dans d'autres ateliers, en collectif ou en individuel.

Présentation des sujets abordés lors de ce premier atelier :

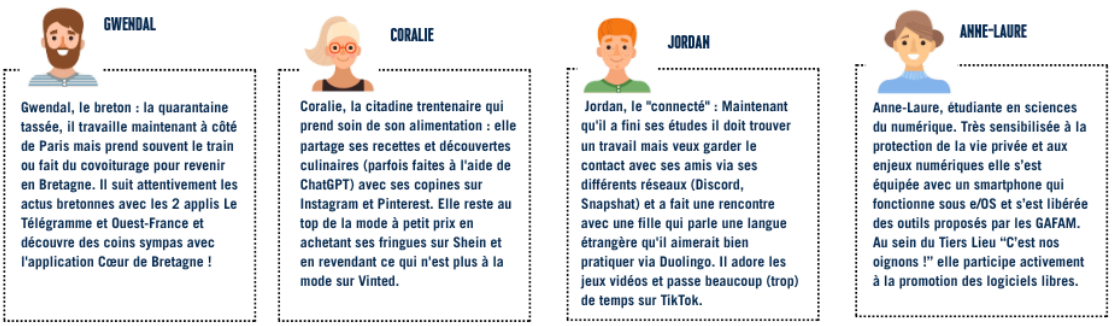
- Ce que disent les téléphones de nous, avec le jeu **A qui est ce smartphone ?**
- Les données à caractère personnel,
- Les applications, pisteurs et autorisations,
- Comment se protéger

Jeu - A qui est ce smartphone ?
C'est un jeu de cartes qui va permettre de mieux comprendre le lien entre les données à caractère personnel et les smartphones.

À partir du visuel d'un smartphone dont on voit les applications installées les participant.e.s vont devoir deviner quelques éléments (5 suppositions ou affirmations) de la vie de la personne qui le possède.

En tant qu'animateur de l'atelier on peut choisir parmi les cartes représentant les smartphones et aiguiller les participants en leur indiquant qu'ils peuvent chercher sur Internet pour découvrir les applications peu ou pas connues.

Chaque carte est liée à un profil (qui a été un peu exagéré pour permettre une identification plus facile) que l'on peut éventuellement montrer à la fin du jeu quand chaque groupe a identifié les 5 suppositions/affirmations sur le profil de l'utilisateur du smartphone.



Et on peux ainsi aborder le fait que nos applications permettent de deviner si on est une personne sportive, si on a des enfants ou si on est célibataire, on peut aussi deviner notre lieu d'habitation et les endroits où on a l'habitude d'aller faire du sport (merci la géolocalisation comme Strava qui a permis de localiser la position du porte-avions Charles de Gaule en mars 2026).

On peut potentiellement deviner l'orientation sexuelle de l'utilisateur (certaines applications de rencontre sont dédiées par exemple à un public homosexuel) mais aussi découvrir des éléments concernant son régime alimentaire et par extension potentiellement sa religion ou ses opinions politiques via des applications de journaux par exemples.

Si on a réussi à cerner l'identité de l'utilisateur du smartphone, vous vous doutez bien que les éditeurs de ces applications vont, eux aussi, tenter de collecter le maximum d'informations ! Voyons cela de plus près avec Exodus Privacy !

Mais avant ça quelques ressources informationnelles

Je rajoute au sein du déroulement de cet atelier quelques informations à avoir en tête pour pouvoir répondre aux questionnements des participants à l'atelier. Je vous invite à creuser le sujet par le biais de quelques liens collectés ici ou là au fil de ma préparation de cet atelier et de son amélioration. Et si vous en avez à partager, n'hésitez pas à améliorer ce contenu en me contactant !

Données personnelles et profilage

En faisant la "correction" de ce premier jeu il va alors être possible d'aborder le principe des données personnelles car on a commencé à en lister quelques-unes !

Les **données à caractère personnelle**, selon la CNIL (Commission Nationale Informatique et Libertés) sont des informations relatives « à une personne physique susceptible d'être identifiée, directement ou indirectement. » Vous pouvez demander aux participant.e.s de citer des exemples et compléter par d'autres éléments : nom, prénom, numéro de sécurité sociale, numéro de carte bancaire, adresse postale, adresse mail, empreinte digitale ...

Si on revient au jeu précédent et à la liste des éléments que l'on a pu découvrir via les applications présentes sur le smartphone, on s'aperçoit que ce ne sont pas forcément des données à caractère personnelle que l'on a pu trouver mais que à partir de cet ensemble de données on peut faire des recoupements et plus on a d'éléments, plus c'est précis.

C'est **le principe du profilage :** on constitue, à partir de données collectées, des profils détaillés avec des dizaines, voire des centaines de critères : le genre, l'âge, la pointure ou la taille mais aussi les données de santé ...

Et cela permet ainsi à certains annonceurs de proposer une publicité la mieux adaptée au profil du public visé. Il existe aujourd'hui des entreprises, les databrokers, dont le métier consiste en la revente de fichiers avec des profils

détaillés. Et plus le profil est complet, plus il peut se vendre cher. Il ressort des études sur le sujet que les données personnelles de base sur un individu, par exemple, l'âge, le sexe et le lieu d'habitation, ne valent que 0,0005 € par personne mais dès qu'elles sont agrémentées d'informations plus personnelles elles peuvent valoir un peu plus.

Dans le cas de Facebook, la valeur moyenne des données d'un utilisateur actif pour Facebook est d'un peu moins de 2 euros. En se basant sur les revenus publicitaires de Google il a été calculé qu'en 2020, chaque utilisateur a généré environ 26 euros. « Si vous ne payez pas le produit, alors vous êtes le produit », en conséquence de nombreux services que nous utilisons « gratuitement » sur le web gagnent de leur argent en collectant des données personnelles qu'elles fournissent ensuite aux annonceurs.

Pour aller plus loin : Monétisation des données personnelles, combien valent nos données ? CNIL 2025

Reprendre la main sur les données collectées ?
En Europe, le premier paragraphe de l'article 17 du RGPD au titre duquel la personne concernée est en droit « d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais ».

Il en découle que la personne concernée peut exiger l'effacement de données à caractère personnel la concernant dans les cas prévus à l'article 17, notamment à la suite de l'exercice du droit d'opposition, lorsque les données ont fait l'objet d'un traitement illicite ou encore afin de respecter une obligation légale issue du droit de l'Union ou du droit de l'État membre auquel le responsable du traitement est soumis. Malheureusement il n'existe pas de service centralisé pour exercer ce droit et il apparaît impossible de pouvoir contacter toutes les entreprises ayant enregistré nos données pour pouvoir tout supprimer d'un seul coup. Surfant sur ce sujet des services privés comme Incogni promettent de supprimer les informations nous concernant détenues par des courtiers en données … sans réellement garantir de résultats.

La collecte de données via les pisteurs et les permissions / autorisations

Pour pouvoir profiler au mieux, les outils numériques sont donc parfaitement adaptés. Via son ordinateur, en se connectant à son compte Google, Microsoft ou Apple, en s'identifiant sur un site Internet, en acceptant un cookie par exemple (qui est le sujet d'un autre atelier), on donne accès à un certain nombre d'informations qui alimentent notre profil personnel et permettent de mieux nous profiler. Il en

va de même avec notre smartphone et les différentes applications qu'il contient !

Les applications que nous utilisons tous les jours sur notre smartphone comportent des pisteurs. Un pisteur c'est un « morceau » de logiciel qui est chargé de collecter des informations sur nous ou bien sur nos usages ou notre environnement. Le site Exodus en répertorie 432 et il en existe de toutes sortes dont :

- ☐ Les pisteurs de type *Crash reporting* qui permettent de collecter des informations lors du crash de l'application qui permettront de pouvoir corriger le dysfonctionnement.
- ☐ Les pisteurs de type *Analytics* qui sont prévus pour collecter des données d'usage et ainsi permettre à la personne développant une application de mieux connaître son audience par exemple pour savoir sur quelle page vous êtes allés, combien de temps vous restez sur telle ou telle partie de la page.
- ☐ Les pisteurs de type *Profiling* ont vocation à récupérer un maximum d'informations sur la personne qui utilise une application afin d'en construire un profil virtuel. Pour ce faire, ce type de pisteur va, par exemple, s'intéresser à l'historique de navigation ou encore à la liste des applications installées, etc.
- ☐ Les pisteurs de type *Identification* se chargent de déterminer votre identité numérique. Cette identité peut faire référence à une identité officielle ou bien à des identifiants abstraits (pseudonyme, etc).
- ☐ Les pisteurs de type *Ads* ont pour but de d'identifier la personne qui utilise une application afin de lui présenter de la publicité ciblée. L'objectif pour la personne incluant ce type de pisteur est de monétiser son application, c'est-à-dire de gagner de l'argent grâce à la publicité.
- ☐ Enfin les pisteurs de type *Location* sont chargés de déterminer la position géographique d'un mobile. Pour ce faire, ce type de pisteur peut tirer profit de plusieurs capteurs : de la puce GPS, des antennes GSM environnantes, des réseaux wi-fi environnants, des balises Bluetooth environnantes ou encore de sons particuliers émis par des hauts-parleurs.

On voit donc que ces pisteurs peuvent avoir besoin d'accéder à certaines informations. Quand on installe l'application sur son smartphone on accorde un certain nombre de droits dont les permissions d'accès, ou autorisations. Elles peuvent concerner des fonctionnalités ou des informations diverses, comme l'accès à votre géolocalisation, à vos contacts, vos fichiers, votre micro, votre vibreur, votre appareil photo ...

Les autorisations des applications contribuent à respecter la confidentialité des utilisateurs en protégeant l'accès à différents éléments comme l'état du système du smartphone mais aussi et surtout aux données présentes sur l'appareil. Mais

en fonction dont l'application a été fabriquée, il est possible qu'un certain nombre de demandes d'autorisations puissent être automatisées par le simple fait d'accepter l'installation de l'application.

Workflow d'utilisation des autorisations

Si votre application propose une fonctionnalité qui peut nécessiter un accès à des données ou des actions restreintes, déterminez s'il vous est possible d'obtenir les informations ou d'effectuer les actions sans avoir à déclarer d'autorisations. Vous pouvez répondre à de nombreux cas d'utilisation dans votre application, tels que la prise de photos, la mise en pause de la lecture de contenus multimédias et l'affichage d'annonces pertinentes, sans avoir à déclarer d'autorisations.

Autorisations sur Android

Il convient donc de faire attention aux autorisations que l'on donne aux différentes applications installées sur notre appareil.

Tiens d'ailleurs, connaissez-vous les différentes autorisations que vous avez donné à une application comme WhatApp par exemple ?

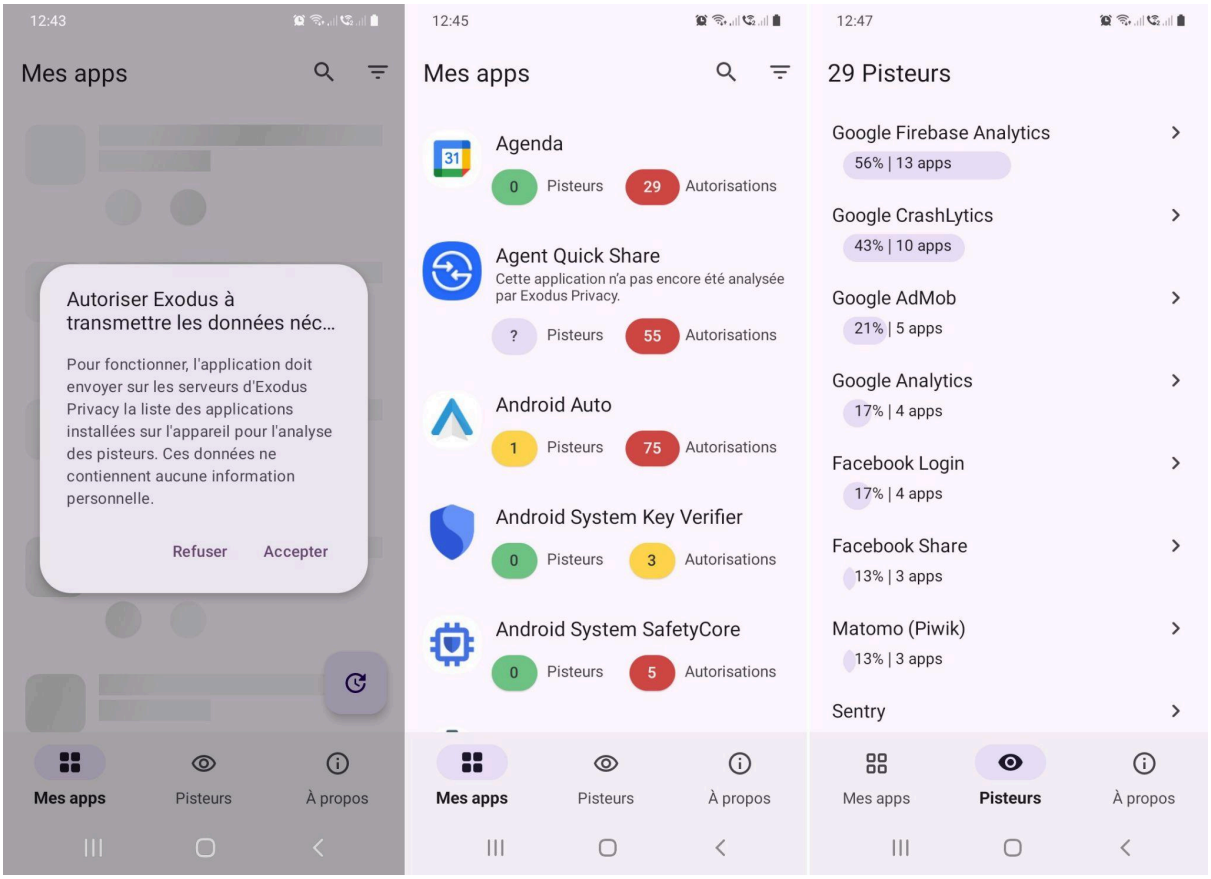
Sur la page de politique de confidentialité de WhatsApp (qui fait 79 pages si on voulait l'imprimer) on peut lire, entre autres, que l'application à accès à votre numéro de téléphone, au nom de votre profil, à vos messages et aux contenus multimédia au sein de vos messages et appels (avec stockage pendant 30 jours), mais aussi des informations de localisation précises, à vos contacts (que ceux ci utilisent ou non cette application), sur les groupes et communautés auxquels vous êtes inscrit, ainsi qu'à toutes les informations techniques de votre usage.

Cela comprend l'heure à laquelle vous utilisez l'application, la durée de vos appels mais aussi sur quel appareil vous utilisez l'application, des informations sur le navigateur que vous utilisez ainsi que sur l'opérateur mobile ou le fournisseur d'accès à Internet et le WIFI.

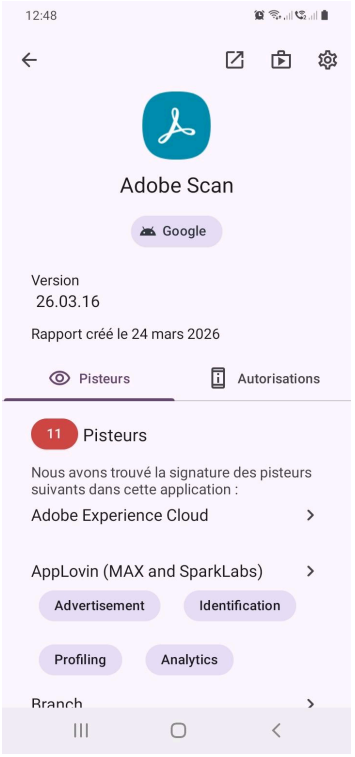
Même si vous décidez de ne pas utiliser les fonctionnalités de localisation précises de l'application WhatsApp utilise les adresses IP et d'autres informations, comme les indicatifs des numéros de téléphone, afin d'estimer votre localisation générale (par exemple, le pays/la région).

Quels pisteurs sont installés sur mon smartphone ?

Il est enfin temps de regarder dans nos appareils pour en savoir un peu plus ! Il y a 2 façons de regarder cela, la plus simple étant d'installer l'application Exodus sur son appareil et de lancer l'analyse des applications présentes :



Après l'installation de l'application il faut autoriser la transmission des données afin que la liste des applications installées sur votre appareil puissent être comparée avec les données présentes sur le site d'Exodus.



Vous obtenez alors un listing alphabétique de vos applications avec le détail des pisteurs et autorisations accordées à chaque application.

Quelle est l'application qui a le plus de pisteurs sur votre smartphone ?

Pour moi c'est l'application **Adobe Scan** avec **11 pisteurs** et plus précisément les pisteurs suivants :

Advertissement
Identification
Profiling
Analytics
Crash reporting

Pour une application qui sert à scanner des documents !

Alors que l'application Drive qui fait la même chose emporte avec lui zéro pisteur ! Je sais ce qu'il me reste à faire : le ménage et trouver des applications plus respectueuses de mes données personnelles !

Et cela pourrait être l'objet d'un prochain atelier !

Pistes à creuser

Quand vous souhaitez installer une application ou quand une application vous demande des éléments personnels, posez-vous les questions suivantes :

- combien contient-elle de pisteurs et quelles autorisations sont demandées ?
- ai-je envie ou besoin de l'installer ?
- ai-je envie ou besoin de lui donner ce qu'elle me demande ?

C'est à vous de décider, mais en réfléchissant ainsi à vos usages au quotidien, vous pouvez avoir une meilleure maîtrise de notre identité numérique.

En fonction des retours vous allez peut-être devoir organiser des ateliers pour faire le ménage et pour remplacer les outils trop "pollués" par les pisteurs.

Les principaux problèmes d'installation de l'application Exodus Privacy
• Les iPhones et les Windows phones ne peuvent installer l'application, uniquement disponible sur Android
• Seules les applications issues du Google Play store sont analysées, donc si une personne a des applications d'une autre source (notamment les applications pré-installées par le fabricant), elles ne seront pas analysées.

Source d'inspiration pour cet atelier : Kit Exodus Privacy, un kit smartphones et vie privée pour animer un atelier. Merci à mes collègues conseillers numériques (Laura, Sylvain, Thomas, Stéphane, Mikael, Loick et Constance) qui m'ont apporté leurs points de vue et leurs idées dans la création du jeu **A qui est ce smartphone ?**

Ressource : La collecte de données personnelles (tiré du parcours d'accompagnement à la découverte de services numériques éthiques - Webinaire 6 - Framasoft et Hubikoop - 2023).