Contrôler ses ordiphone et tablette

Niveau : Intermédiaire
Prérequis : Être l'aise avec l'usage des ordiphones et tablettes, comprendre les enjeux de la surveillance généralisée.

Conférence : Nos empreintes numériques

Résumé : Ces appareils sont devenus des interfaces pour de nombreux usages du quotidien. Pourtant, ces couteaux suisses numériques constituent souvent une faille importante pour la protection des données personnelles. Des méthodes simples permettent néanmoins de limiter ces dégâts. Découvrez comment vous protéger sur des systèmes type Android.

Si vous êtes soucieux de votre vie privée numérique, cet atelier est fait pour vous !

Préambule : Pourquoi Android

S'agissant d'un atelier spécifiquement dédié au thème de la vie privé, il peut sembler étrange de baser celui-ci sur un système type Andoid plutôt qu'une alternative, sachant que l'éditeur, la société Google, est représenté comme étant le mal absolu dans le domaine.

Il faut garder à l'esprit qu'Android, le système commercial de Google vendu avec les appareils, fonctionne à l'aide d'un noyau GNU/Linux modifié, nommé Android, ce qui est du logiciel libre. Par-dessus, une couche de logiciels prioritaires est ajouté par l'éditeur, implémentant une collection de système de surveillances. C'est cette surcouche qui pose problème. Finalement, rien ne nous empêche de profiter du noyau Android tout en supprimant ou bloquant les surcouches Google.

Parallèlement, les alternatives tels que Sailfish OS, bien qu'intéressantes, restent à ce jour des marchés de niche, proposant une offre d'applications réduite.

Acte 1 : Les applications

Exodus Privacy

Le but du jeu dans notre exercice, est d'éviter au maximum d'utiliser des applications intrusives et qui ajoute des algorithmes d'espionnages.

Une association française, Exodus Privacy, œuvre quant au référencement de la potentielle curiosité des applications disponible pour Android via le gestionnaire proposé par Google. Pour vous donner un aperçu de ce qui est possible de trouver comme information, rendez-vous sur la page web https://reports.exodus-privacy.eu.org et recherchez « Torche ».

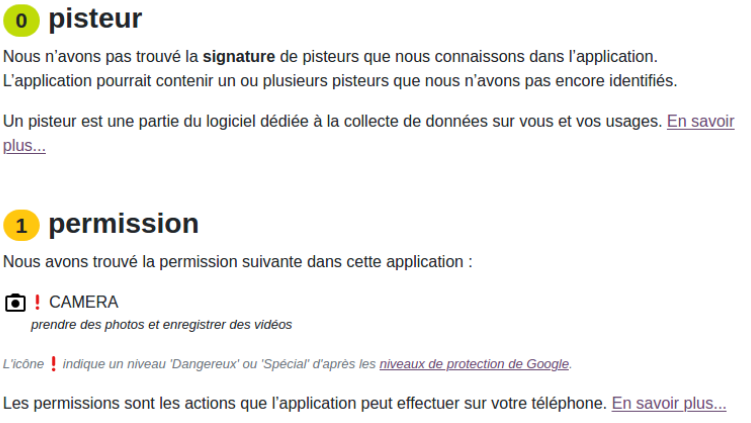
Vous verrez alors apparaître une liste d'application de torche, dont le but est de simplement allumer le flash de la caméra de votre ordiphone en cas de besoin.
Dans la liste, vous avez à disposition deux exemples intéressant, les deux opposés !

L'un intégrant 16 pisteurs, c'est-à-dire 16 algorithmes qui envoient des informations vers Facebook, Google, Twitter et 6 autres services inconnus.

8 permissions, notamment l'accès à votre réseau Internet.

En face, la seconde application ne contient aucun pisteur connu et n'a accès qu'à la caméra pour activer le flash.

Elle ne fait que ce dont on a besoin, allumer la torche !



On retrouve des exemples intéressants tels que l'application Météo France, avec ses 26 pisteurs et 13 permissions !

Ainsi, ces rapports donnent de bons indicateurs quant aux choix d'une application pour un usage précis.

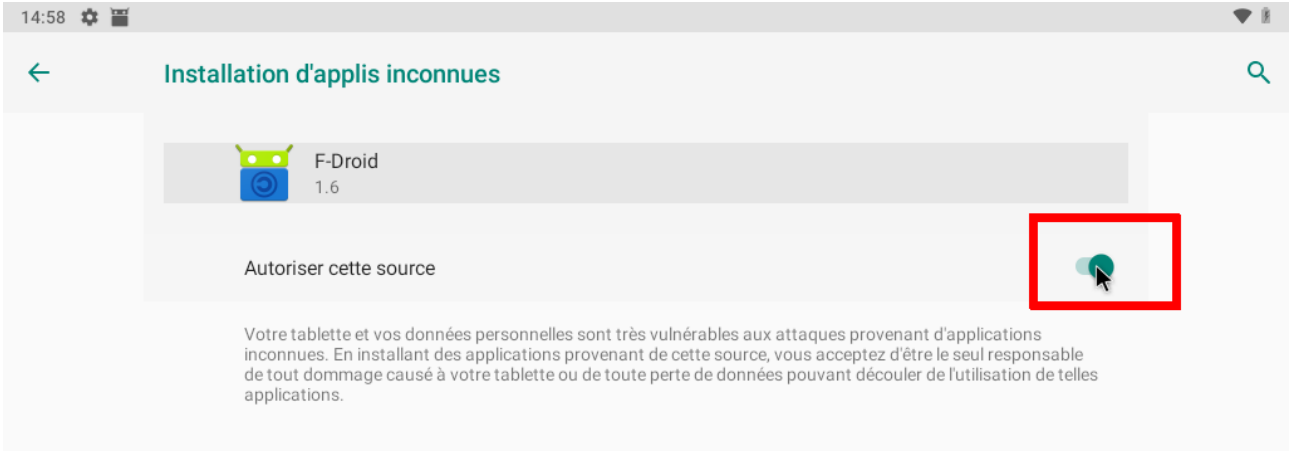
Applications alternatives

Installer F-Droid

Alternative à Google Play, F-Droid est un gestionnaire d'applications exclusivement libres, compilés par les mainteneurs permettant de s'assurer de la non-présence de traceurs. Pour faire simple, c'est une application de confiance qui propose d'autres applications et mises à jour de confiance.

Pour la rechercher et l'installer sur votre appareil, rendez-vous sur https://f-droid.org et sélectionnez **Télécharger F-Droid**.

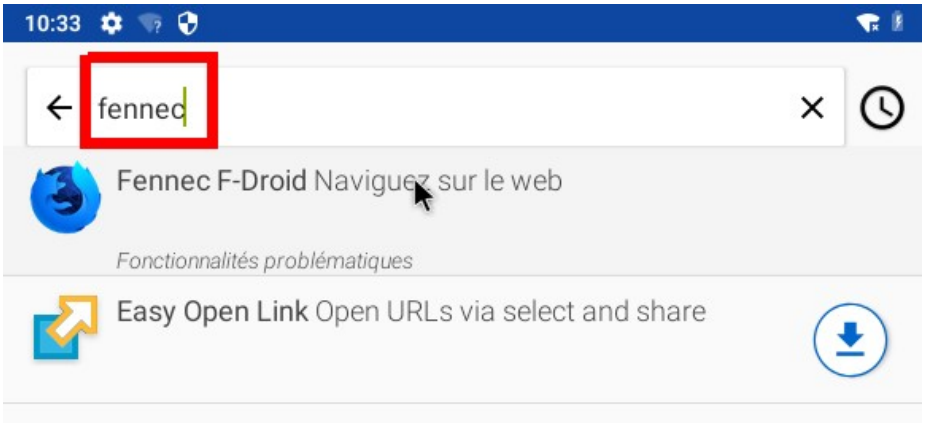
Pour l'installer, si ce n'est pas déjà fait, vous devrez activer dans les réglages de votre appareil la possibilité d'installer des applications depuis une source « **inconnue** ».



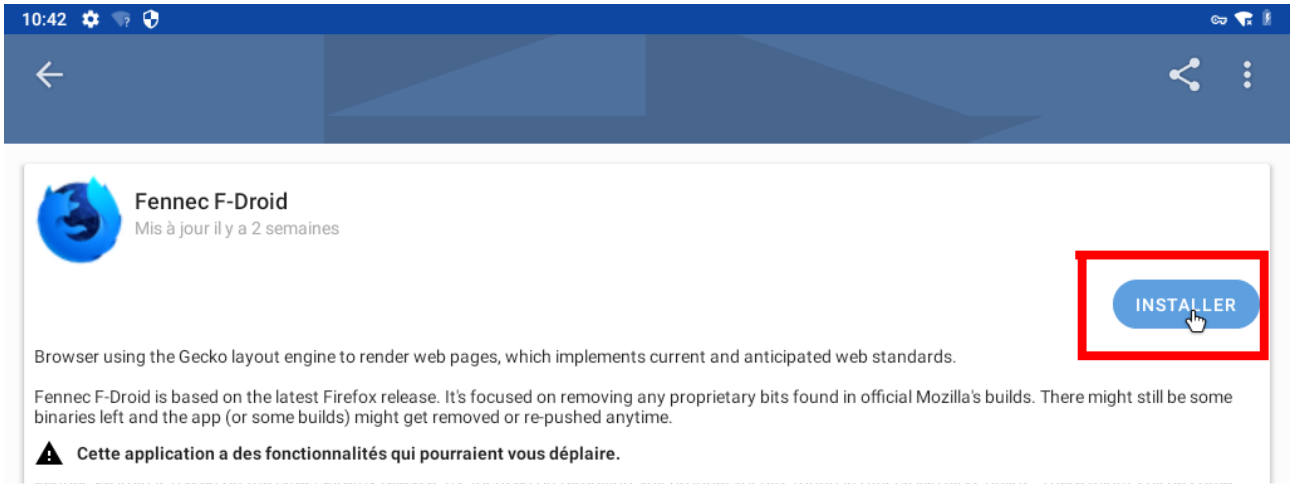
Installer depuis F-Droid

Maintenant, en utilisant l'application F-Droid précédemment installé, il est possible d'ajouter diverses autres applications selon les besoins. Pour l'exemple, sera installé le navigateur web **Fennec F-Droid**, utilisé dans le chapitre suivant.

À l'aide de la fonctionnalité de recherche intégré dans F-Droid, écrivez fennec, vous sera proposé des résultats dont celui recherché.



Sélectionnez-le, et cliquez sur **Installer**.



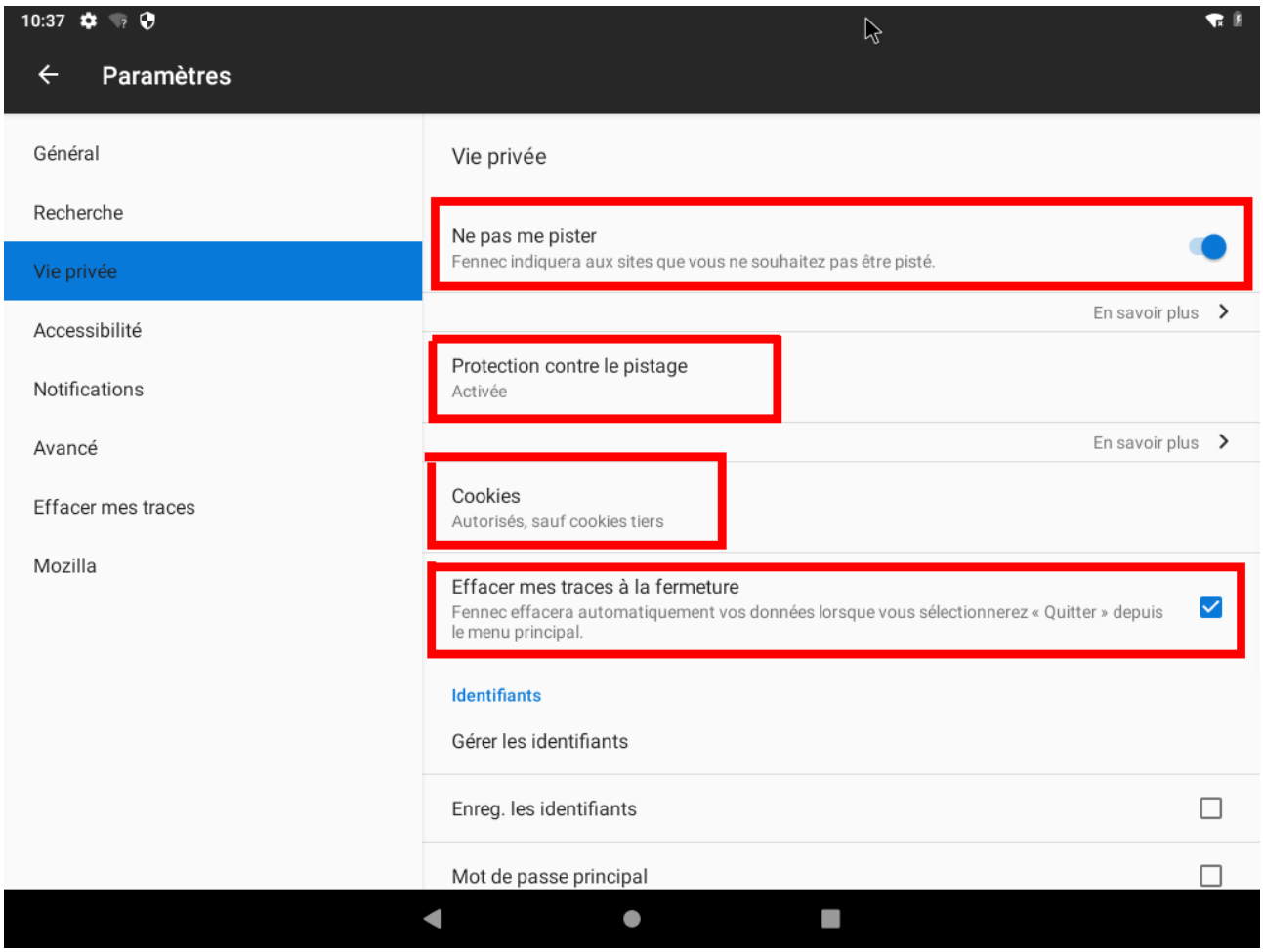
Navigateur web

Il existe donc pléthores d'applications répondant à divers besoins. Certaines sont réellement pratiques, d'autres sont discutables, car, sont souvent des équivalences à des offres proposées via un simple navigateur web.
Ce qu'il faut garder à l'esprit, c'est qu'il est en général bien plus simple de contrôler les flux d'informations transitant via des navigateurs de confiances, plutôt que des « applis officielles ».

Dans ce cadre, l'exemple pratique est le service Météo France : Vous pouvez consulter la météo sur meteofrance.com !

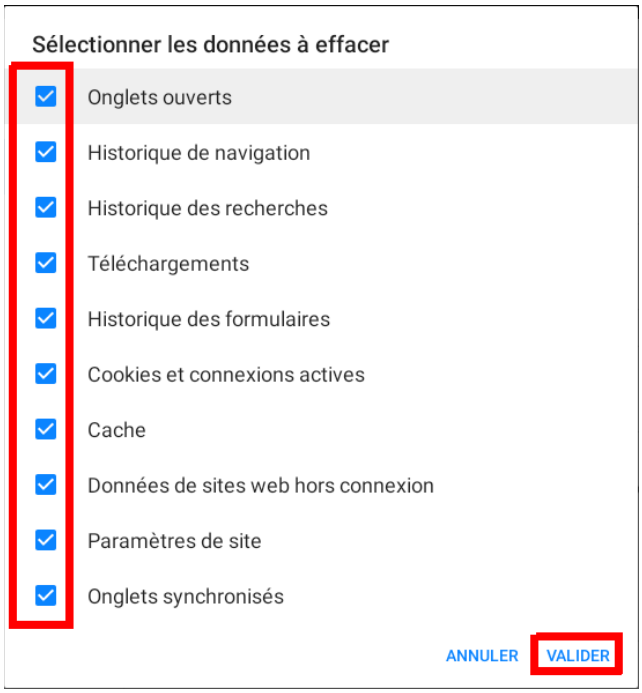
Fennec F-Droid est une fourche du navigateur Firefox. L'intérêt de son utilisation plutôt que l'original est d'éviter l'introduction de pisteurs lors de sa compilation. De la même manière que pour l'atelier « Naviguer protégé sur le web », est proposé sa configuration pour limiter le pistage.

Rentrez dans les options via le pictogramme ⋮ Sélectionnez **Paramètres**.



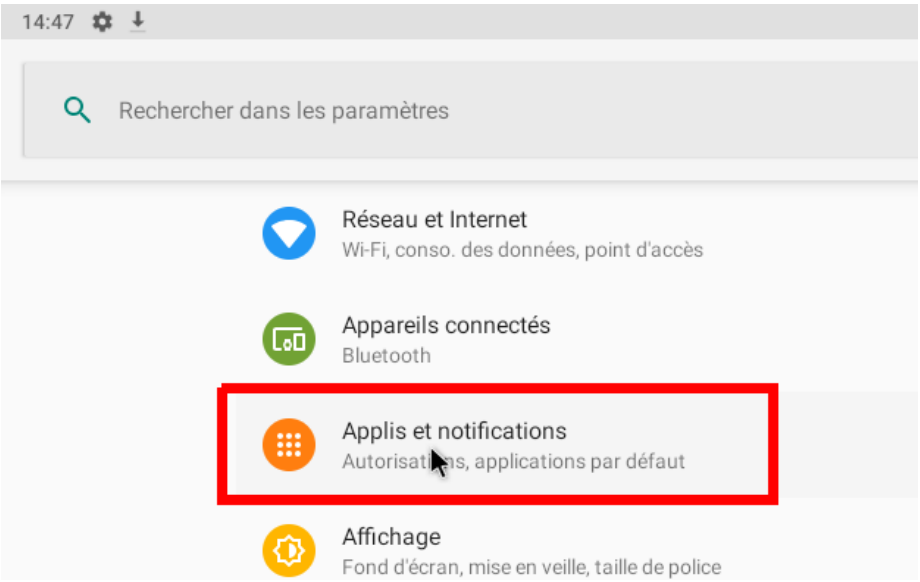
Dans la rubrique **Vie privée**, réalisez ces modifications :

- Cochez l'option **Ne pas me pister**,
- Activez (**Activée**) la **Protection contre le pistage**,
- Autorisez uniquement les cookies légitimes (**Autorisés, sauf cookies tiers**)
- Cochez le maximum d'options dans le menu **Effacer mes traces à la fermeture**.



Acte 2 : le système

Nettoyer

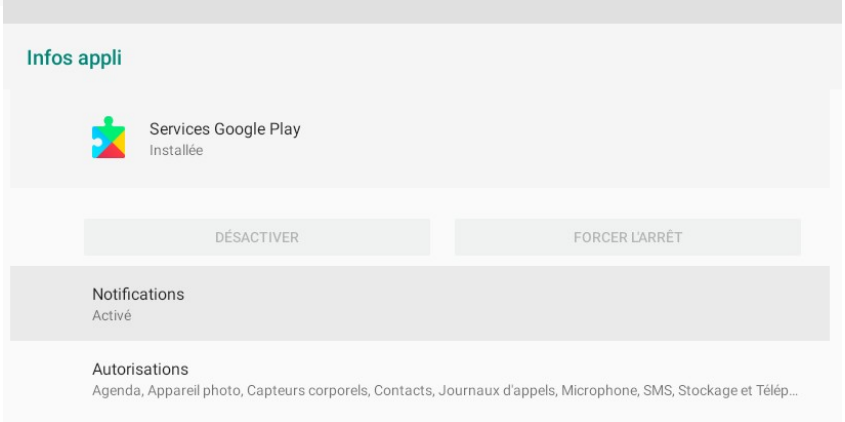


Accédez aux préférences de votre système, généralement accessibles depuis un pictogramme en forme de rouage, puis rendez-vous dans le menu permettant de gérer vos applications.

Vous avez précédemment installé le navigateur web Fennec, ainsi celui proposé par Google, Chrome, n'a plus d'utilité. Si vous tenez à votre vie privée, il est fortement recommandé de le supprimer !

Dans la pratique, c'est un peu plus compliqué puisque qu'il n'est en général pas possible de désinstaller les applications proposées par défaut. On peut cependant généralement les désactiver.

Vous rencontrerez aussi la problématique que certains services, en général les plus curieux, ne peuvent être ni désinstallés, ni désactivés ! C'est le cas de Google Play.

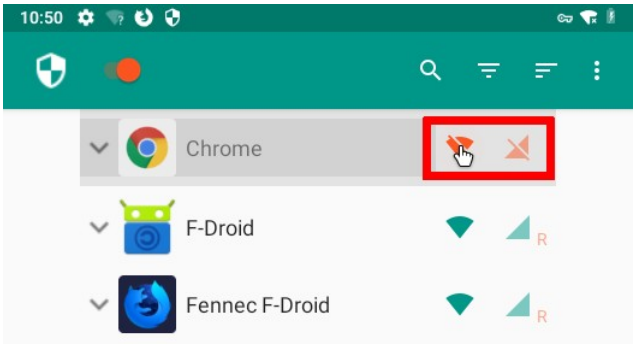


Filtrer

Comme vu précédemment, certaines applications installées par défaut ne peuvent être désinstallées ni même désactivées. Pour éviter les fuites de données personnelles, il est possible d'ajouter l'application Netguard qui bloque les flux avec les extérieurs. En soit, si une application problématique récupère des informations sur vous, elle ne pourra pas les expédier via Internet.

De la même façon que pour le navigateur Fennec, installez l'application **Netguard** via F-Droid.

Dans l'interface, vous êtes dans la capacité de bloquer les interactions avec l'extérieur, en cliquant sur les réseaux wifis et mobiles, pour chacune des applications qui ne sont pas de confiance.



Pour la démonstration, voici un exemple concret de ce que peut bloquer Netguard sur une application non désactivable et non utilisée dans la pratique (c'est-à-dire tourne en tache de fond inutilement). Dans le cas présent, il s'agit de Google Play Store sur Android 4.1.

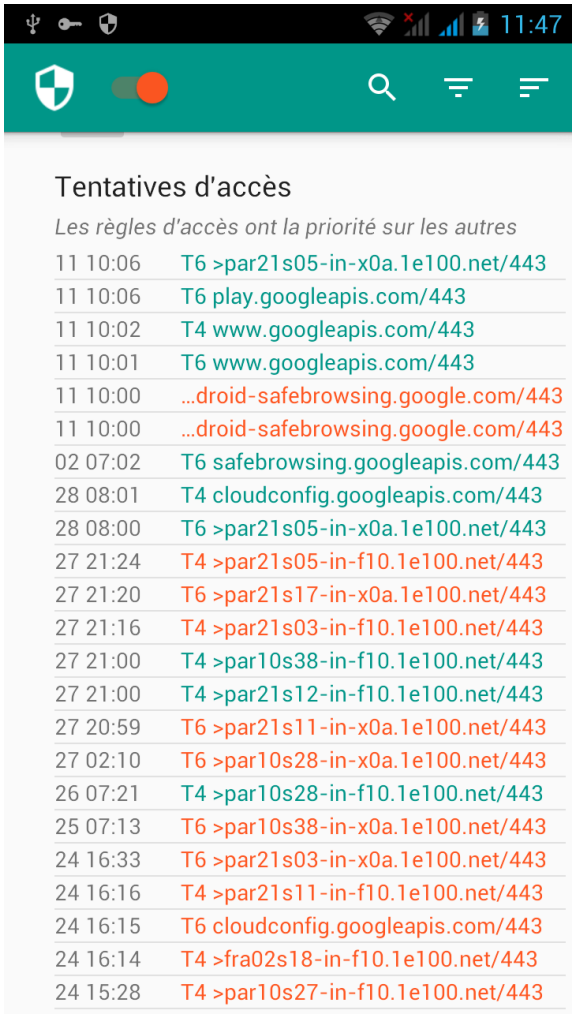


Figure 1: Blocages de données issues de l'application Google Play Store, par Netguard.