

# Appli de tchat : pourquoi et comment passer de WhatsApp à Signal

## Que se passe-t-il au juste avec WhatsApp ?

Depuis quelques jours, on parle beaucoup du transfert des “boucles” WhatsApp vers les “groupes” Signal. C'est une discussion qui peut paraître technique, mais elle est aussi particulièrement importante pour les associations, les entreprises et les partis politiques, parce que toutes ces organisations utilisent bien volontiers les applis de tchat et que, au-delà des fonctionnalités des unes et des autres, se pose la question de leur sécurisation et de l'exploitation plus ou moins importante de leurs données personnelles.



Au sein d'EELV par exemple (le parti que je connais bien : ) ), les boucles WhatsApp se multiplient autant qu'à une époque, les listes de discussions par e-mail. Vous connaissez certainement déjà la blague : deux écolos pas d'accord entre eux, c'est trois listes de discussions créées ! C'est un peu la même chose ces dernières années avec WhatsApp...

WhatsApp est effectivement très pratique pour rassembler rapidement des dizaines, voire des centaines de personnes, et partager news, infos et actions avec toutes ces personnes. La puissance de ce genre d'outil n'est pas à minorer, c'est par exemple grâce aux rumeurs contre la gauche et les progressistes en général, partagées en un clic sur des centaines de groupes WhatsApp, que Bolsonaro a fait campagne au Brésil et qu'il a pu conquérir le pouvoir. WhatsApp a été une véritable “plate-forme de radicalisation à droite” lors de ces élections.<sup>1)</sup>

Or, il se trouve que la petite entreprise qu'est WhatsApp au départ, est rachetée en 2014 par le géant Facebook, parce que l'application commence à faire trop de concurrence au Messenger de Facebook comme outil de tchat en ligne. A l'époque, les fondateurs de WhatsApp incluent dans le deal que, pendant cinq ans, Facebook ne pourra pas exploiter les données personnelles des utilisateurs-trices à des fins publicitaires. Le rachat provoque quelques remous en internes, car au départ, la philosophie de WhatsApp était claire : pas d'exploitation des données des utilisateurs.<sup>2)</sup>

Et devinez quoi ? Les années ont passé, et de nouvelles Conditions Générales d'Utilisation (CGU) sont proposées en ce moment aux usagers de WhatsApp. En cas de refus, à partir du 8 février 2021 l'appli deviendra tout simplement inutilisable. Le souci c'est que ces nouvelles CGU autorisent beaucoup plus qu'auparavant la

collecte des données personnelles, et cette collecte va bénéficier à... Facebook, et non plus à WhatsApp seulement. En gros, WhatsApp sans Facebook qui regarde derrière votre épaule, ce ne sera plus possible. <sup>3)</sup>

## Mais de quelles données parle-t-on exactement ?

Alors, attention, parce que quand on parle des “données personnelles des utilisateurs”, on a tendance à imaginer à peu près tout. Mais en fait, non, on ne parle pas du **contenu** que l'on produit sur ces applications, on parle de toutes les **méta-données** susceptibles d'être captées lorsqu'on utilise ces applications. En bref : non, personne ne “voit” ce que vous partagez comme propos ou comme photos. En revanche, les organisation qui développent ses applications, généralement des sociétés privées à but lucratif, vous proposent leur service en échange de quelques informations vous concernant. Les métadonnées, ce sont toutes ces informations relatives à l'art et la manière dont vous émettez et recevez des messages, au contexte technique, parfois même géographique, dans lequel vous utilisez l'application. Par exemple, parmi les métadonnées les plus souvent aspirées : quel type de système d'exploitation vous utilisez, votre localisation grâce au GPS, quel moyen de paiement en ligne, vos achats récents, l'historique de votre navigation internet... Il y a des dizaines et des dizaines de méta-données potentiellement utiles pour alimenter des bases de données à visée commerciale.

Dans un récent article, des journalistes de Forbes ont répertorié quelles méta-données étaient récupérées par quatre applis de tchat parmi les plus populaires : le Messenger de Facebook, WhatsApp, iMessage d'Apple et Signal. Cet article a été beaucoup partagé ces derniers jours grâce au tableau qu'il propose, qu'on a vu tourner sur Twitter et Facebook. <sup>4)</sup>

Signal 'Data Linked To You'	iMessage 'Data Linked To You'	WhatsApp 'Data Linked To You'	Facebook Messenger 'Data Linked To You'		
<ul style="list-style-type: none"><li>Contact Info<ul style="list-style-type: none"><li>Email Address</li><li>Phone Number</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>Device ID</li></ul></li></ul>	<ul style="list-style-type: none"><li>Contact Info<ul style="list-style-type: none"><li>Phone Number</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>Device ID</li></ul></li></ul>	<ul style="list-style-type: none"><li>Analytics<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Location<ul style="list-style-type: none"><li>Course Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Phone Number</li></ul></li><li>User Contact<ul style="list-style-type: none"><li>Other User Contact</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>Third-Party Advertising<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Physical Location</li><li>Course Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contact</li></ul></li><li>User Contact<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gateway Comment</li><li>Other User Contact</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>Product Personalisation<ul style="list-style-type: none"><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Physical Location</li><li>Course Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contact</li></ul></li><li>User Contact<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gateway Comment</li><li>Other User Contact</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Sensitive Info<ul style="list-style-type: none"><li>Sensitive Info</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>Health &amp; Fitness<ul style="list-style-type: none"><li>Health</li><li>Fitness</li></ul></li><li>Purchases<ul style="list-style-type: none"><li>Purchase History</li></ul></li><li>Financial Info<ul style="list-style-type: none"><li>Other Financial Info</li></ul></li><li>Location<ul style="list-style-type: none"><li>Physical Location</li><li>Course Location</li></ul></li><li>Contact Info<ul style="list-style-type: none"><li>Physical Address</li><li>Email Address</li><li>Phone Number</li><li>Other User Contact Info</li></ul></li><li>Contacts<ul style="list-style-type: none"><li>Contact</li></ul></li><li>User Contact<ul style="list-style-type: none"><li>Photos or Videos</li><li>Gateway Comment</li><li>Customer Support</li><li>Other User Contact</li></ul></li><li>Search History<ul style="list-style-type: none"><li>Search History</li></ul></li><li>Browsing History<ul style="list-style-type: none"><li>Browsing History</li></ul></li><li>Identifiers<ul style="list-style-type: none"><li>User ID</li><li>Device ID</li></ul></li><li>Usage Data<ul style="list-style-type: none"><li>Product Interaction</li><li>Advertising Data</li><li>Other Usage Data</li></ul></li><li>Sensitive Info<ul style="list-style-type: none"><li>Sensitive Info</li></ul></li><li>Diagnostics<ul style="list-style-type: none"><li>Crash Data</li><li>Performance Data</li><li>Other Diagnostic Data</li></ul></li><li>Other Data<ul style="list-style-type: none"><li>Other Data Types</li></ul></li></ul>

Pour faire simple :

- le **Messenger de Facebook** collecte pas moins d'une centaine de méta-données ! C'est vraiment beaucoup... Et ces informations incluent la liste de vos amis Facebook, la liste de vos contacts sur votre smartphone, l'historique de vos recherches dans le module de recherche de Facebook, l'historique de vos recherches dans votre navigateur Internet, votre localisation géographique, vos statistiques “fitness” si vous utilisez une appli de ce genre, les données d'usage de votre réseau mobile, ... Il y a même une catégorie de méta-données dénommée “sensitive info” (informations sensibles), sans plus de détail ! Bref, en utilisant Facebook et son Messenger, vous permettez à cette entreprise d'exploiter nombre de données personnelles au jour le jour. Encore une fois, pas pour connaître vos secrets les plus intimes,

mais pour établir votre profil de consommateur et savoir quelles publicités auront le plus de chances de vous intéresser, auxquelles vous serez tôt ou tard exposé. C'est le fameux *“si c'est gratuit, c'est vous le produit”*.

- **WhatsApp** collecte “seulement” 25 méta-données différentes. Ce qui n'a l'air de rien par rapport au Messenger de Facebook, mais désormais, avec les nouvelles CGU, ces données-là seront aussi exploitables par Facebook...
- **iMessage** d'Apple est beaucoup plus respectueux, avec seulement 4 méta-données récoltées...
- Et l'appli **Signal**, de son côté, ne récupère *aucune méta-donnée* de ses utilisateurs ! (La seule info qu'elle connaît de ses utilisateurs, c'est leur numéro de téléphone.)

Dans une mise à jour à la toute fin de l'article de Forbes, à propos des nouvelles CGU de WhatsApp, on apprend que *“clairement, exiger des usagers qu'ils acceptent ce partage de leurs données avec Facebook va constituer un “game changer” pour beaucoup d'entre eux. Même si les messages échangés resteront encryptés, cela va certainement générer une nouvelle inquiétude à propos de la valorisation des données personnelles par la machine Facebook.”* <sup>5)</sup>

A titre personnel, j'ai fait le choix de quitter Facebook, fin 2018, après dix années d'utilisation quasi-quotidienne de ce réseau social (j'ai trouvé [11 bonnes raisons pour supprimer définitivement mon compte](#)). En 2018, j'utilisais déjà beaucoup WhatsApp et je savais que cette entreprise collectait certaines données personnelles... Mais pourquoi pas, tant que le service fourni, gratuit et efficace, continuait à me convenir... Mais en ce début 2021, savoir que mes données personnelles récupérées par WhatsApp pourraient servir tôt ou tard à alimenter les bases de données de Facebook... comment dire... ça me donne l'impression d'avoir chassé Facebook par la porte, pour le voir revenir ensuite par la fenêtre. C'est agaçant, et je préfère vraiment que cette entreprise privée américaine ne sache rien de moi et que ça continue ainsi... !

Un bémol cependant (ou plutôt, une raison d'être rassuré) : en Europe, nous internautes, nous bénéficions du RGPD, le Règlement Général sur la Protection des Données, voté en 2016. <sup>6)</sup> Et grâce à ce règlement, les entreprises privées ne peuvent pas faire tout et n'importe quoi avec nos données personnelles. De ce fait, les données des usagers européens de WhatsApp ne peuvent pas, pour le moment, être utilisées par sa maison-mère, Facebook... En tout cas, c'est ce que prévoit ce texte. Il faut faire confiance à Facebook pour respecter ce règlement... Et de toute manière, cela ne supprime pas le souci pour tout le reste des internautes, hors d'Europe, c'est-à-dire tout le reste du monde ! Si vous avez un oncle ou un collègue en Asie ou aux Etats-Unis ou ailleurs, alors ses données ne seront pas aussi bien protégées qu'en Europe... et donc, en utilisant WhatsApp, ce correspondant se fera aspirer ses données personnelles, notamment sa liste de contacts et d'ami-e-s...

## Quel usage fait-on de ces applis de tchat, et pourquoi c'est potentiellement sensible ?

Mais pourquoi s'inquiéter comme ça ? Après tout, les applis de tchat, ce ne sont pas non plus des cellules d'écoute de la STASI ou du Pentagone... qui ont certainement d'autres choses à faire que de mater la dernière photo que vous avez envoyée à votre *crush* du moment pour réussir à enfin attirer son attention.

Oui mais voilà, ces applis de tchat ont pris énormément d'importance ces dernières années. Et pas seulement pour échanger avec sa tante ou organiser les achats du repas de Noël. Des entreprises, des associations, des partis politiques utilisent ces applis au jour le jour pour communiquer, mobiliser, lancer des actions, prendre des décisions, discuter des dossiers en cours, etc.

Le “grand public” utilise peut-être WhatsApp pour la liste de courses du jour, mais en parallèle, des “boucles” WhatsApp de plusieurs centaines de participants s'agitent chaque jour, sur des sujets plus ou moins confidentiels et sensibles. ET là, on a un problème : il est difficile de faire confiance aux Etats, y compris lorsqu'ils se prétendent tout à fait démocratiques et respectueux de la vie privée de leurs ressortissants...

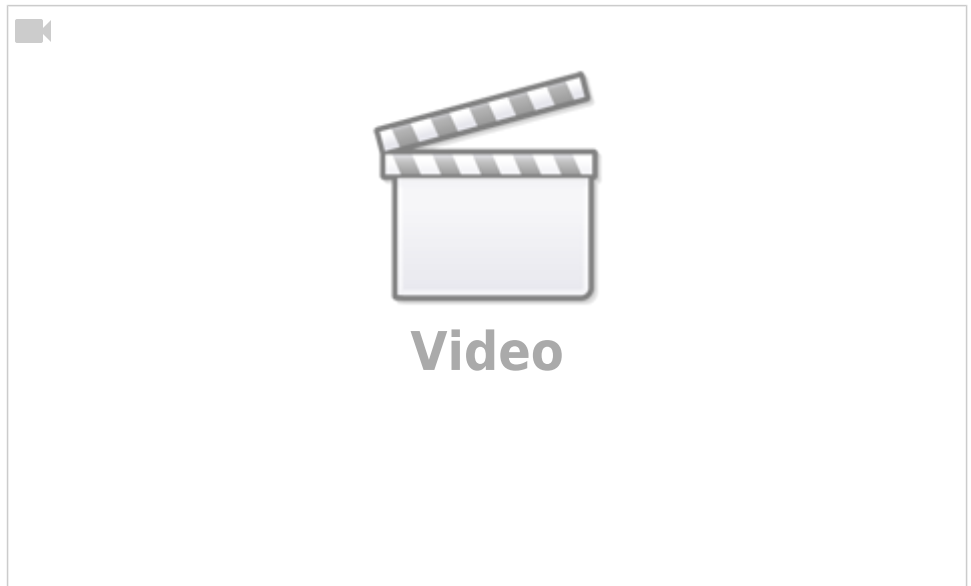
Aux Etats-Unis en 2001, la *“loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme”* a ouvert la voie à une écoute généralisée des internautes au nom de la sécurité nationale <sup>7)</sup>. En 2013, Edward Snowden rend publiques les programmes de surveillance des internautes par la

NSA américaine, sur la base des méta-données récupérables via les diverses applications de réseaux sociaux populaires <sup>8)</sup>. Je vous conseille d'ailleurs de regarder l'excellent documentaire [Meeting Snowden](#) de Flore Vasseur, sorti en 2017 et primé à plusieurs reprises. C'est édifiant.

En France, après les attentats terroristes de 2015, le gouvernement Hollande arrive à faire voter par l'Assemblée Nationale plusieurs lois qui, au prétexte, là aussi, d'améliorer la sécurité des honnêtes gens, permettent désormais aux services de renseignement de s'intéresser de beaucoup plus près à la vie numérique des citoyen-ne-s. <sup>9)</sup>

Qu'on ne s'y trompe pas, la menace d'un espionnage massif des entreprises et des partis politiques, en Europe, par certains Etats, au nom de leur "sécurité nationale", n'est pas seulement théorique, il y a eu des exemples depuis les révélations de Snowden. En 2012, les élections présidentielles françaises sont surveillées de très près par la NSA américaine <sup>10)</sup> ; en 2015 la chancelière Allemande, Angela Merkel, est écoutée jusque sur son smartphone, là encore par la NSA <sup>11)</sup>... De grands groupes peuvent aussi être tentés de surveiller leurs salariés syndiqués, comme ce fut le cas avec Ikea en 2012 <sup>12)</sup>, ou encore une entreprise détenue par un gouvernement qui aimerait bien récupérer quelques secrets industriels de ses concurrents étrangers. <sup>13)</sup>

On pourrait se dire que tout cela, ça ne nous concerne pas, nous "simples" usagers de WhatsApp. Le problème est quand même que, d'une part, quelle que soit l'application considérée, la sécurité est toujours plus ou moins aléatoire, par exemple les usagers de WhatsApp ont été inquiétés en 2019 par une faille de sécurité importante <sup>14)</sup>, et d'autre part, il faut se rendre compte d'une chose importante : en tant que simples citoyen-ne-s, nous ne savons pas exactement quelles sont les obligations auxquelles sont soumises toutes ces applications par les Etats. En janvier 2020, l'Etat américain a encore essayé de contraindre la société d'Apple de lui laisser accéder aux données personnelles de deux iPhones, dans le cadre d'une enquête du FBI... <sup>15)</sup>

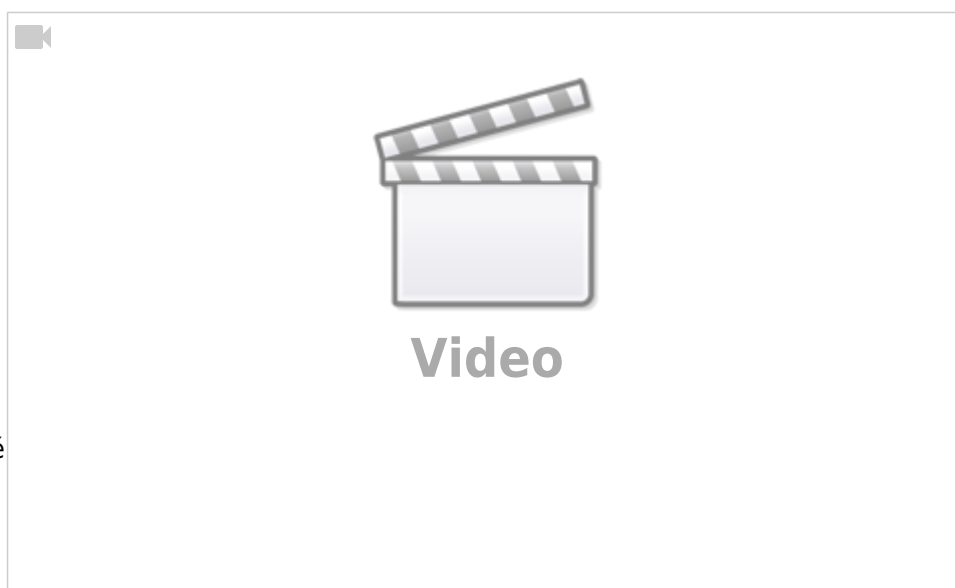


## Signal : une alternative complète et respectueuse de la vie privée de ses usagers

Or donc, si l'on veut se passer de WhatsApp et de ses assez grandes oreilles, quelle alternative utiliser ? Comme beaucoup d'autres, je me suis penché sur [Signal](#). C'est une des applis que je teste régulièrement depuis un an au moins. Car il existe beaucoup d'applications qui rêvent de détrôner WhatsApp, et certaines d'entre elles sont des applications *opensource*, c'est-à-dire que leur code source est récupérable, qu'on peut le scruter et l'étudier à loisir, voire même le modifier pour proposer une nouvelle appli. Généralement, ces applis *opensource* sont supportées par une fondation ou une association, à but non lucratif, et c'est bien le cas de Signal.

Une autre appli est aussi assez connue désormais, [Telegram Messenger](#), mais j'avoue avoir une légère préférence pour les fonctionnalités proposées par Signal. Et le fait qu'une bonne partie des Trumpistes réactionnaires, racistes et complotistes se réfugie depuis peu sur Telegram ne fait que me conforter dans l'idée qu'on est mieux sur Signal <sup>16)</sup>. A suivre aussi, l'appli française [Olvid](#), qui n'est pas encore *opensource*, mais son équipe prétend [vouloir l'ouvrir tôt ou tard](#). (D'autres applications sont citées plus loin dans cet article.)

Signal *“met l'accent sur la confidentialité et la protection des données personnelles”*. Concrètement, cela signifie que l'appli en connaît le moins possible sur vous en tant qu'utilisateur, en n'utilisant que votre numéro de téléphone pour vous identifier. C'est la seule méta-donnée qu'utilisera l'application pour gérer votre compte. Tout le reste est *“chiffré de bout en bout”*. Sans entrer dans des détails techniques compliqués, voilà le principe : les messages émis sont codés via une clé de chiffrement au moment de leur envoi, ils sont reçus par le destinataire de manière codée et sont décodés au dernière moment, une fois sur l'écran du destinataire. De plus, avec Signal, votre photo de profil, votre nom et prénom, vos contacts sur Signal avec qui vous discutez, tout cela est aussi chiffré de bout en bout, et à aucun moment l'équipe de développeurs de l'application ne peut y avoir accès *“en clair”*.



Le *“chiffrement de bout en bout”* est un principe de sécurisation assez simple en théorie, mais qui peut vite devenir complexe à appréhender. Je vous conseille l'excellente vidéo du *“youtubeur”* français Mr Bidouille ci-joint si vous voulez mieux comprendre.

Et ce n'est pas un détail, cette politique de confidentialité fait de Signal l'une des applications les plus plébiscitées ces dernières années, et par des personnalités très différentes : le lanceur d'alerte Edward Snowden, le milliardaire chef d'entreprise Elon Musk, même l'Union Européenne a encouragé ses fonctionnaires

à utiliser Signal, notamment dans le cadre d'échanges avec des personnes extérieures à cette administration, afin de garantir la confidentialité des données transmises<sup>17)</sup>. Pour les plus curieux, il faut lire la [page Wikipédia présentant l'histoire de Signal](#) et bien entendu suivre [le blog officiel de Signal](#) qui réagit rapidement à l'actualité ainsi que [le compte Twitter de l'application](#), source d'informations sur ses mises à jour régulières.

Ce respect de la confidentialité des échanges a aussi une conséquence : comme l'appli Signal, sur votre smartphone, n'a aucune information lui permettant de savoir que vous êtes bien vous-même derrière l'écran (ni localisation, ni détails techniques sur le terminal utilisé, etc.), elle doit passer par une autre méthode d'identification pour continuer à assurer la confidentialités de vos échanges. Et cela se fait via un code secret à 4 chiffres, le NIP, que l'application vous demande de décider et de retenir de mémoire. Ce NIP n'est stocké nulle part sur votre smartphone, et du coup, lors des premières semaines d'utilisation, l'application va vous le demander à plusieurs reprises. Après quelques temps, ces demandes de resaisir votre NIP deviendront de moins en moins fréquentes.



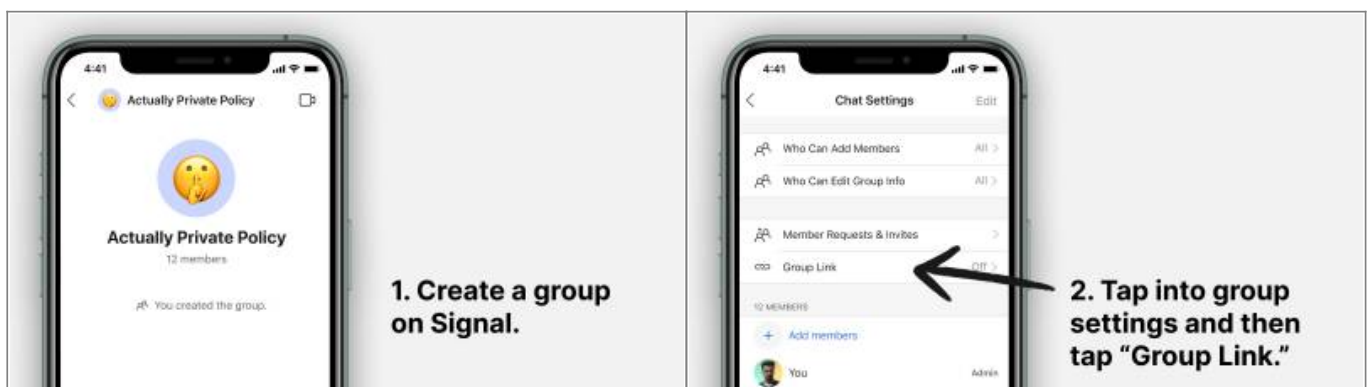
Autre point motivant pour passer à Signal, il existe aussi un [Signal Desktop](#) disponible pour Windows, Mac et Linux, qui permet de gérer ses conversations et ses groupes depuis l'écran de l'ordinateur plutôt que depuis le smartphone. C'est l'équivalent de la web app de WhatsApp, mais avec un détail qui change tout : le client Signal sur ordinateur est indépendant de celui sur smartphone, ce qui signifie qu'il n'est pas nécessaire d'avoir son smartphone connecté pour l'utiliser. Voilà qui peut être fort pratique si l'on n'a pas son smartphone sous la main ou que sa batterie est épuisée ! Concrètement, il vous faudra "synchroniser" une seule et unique fois les deux applis (pour que l'appli Desktop sache qui vous êtes), et ensuite elles pourront vivre leur vie, indépendamment.

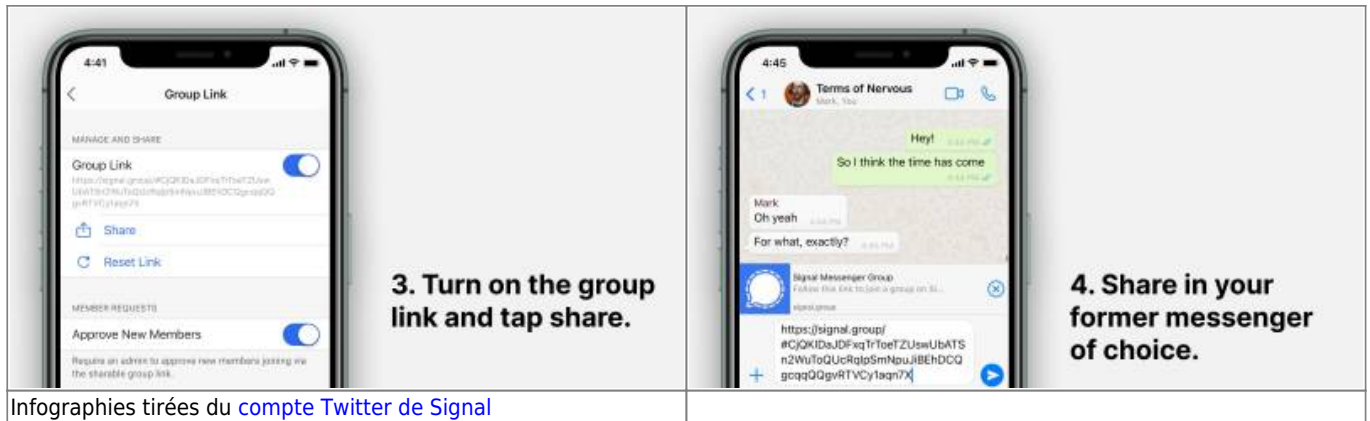
## Réussir la migration de boucles WhatsApp vers des groupes Signal

La procédure pour migrer une "boucle" WhatsApp vers un "groupe" Signal est très simple, techniquement parlant. Elle est un peu plus délicate, socialement parlant.

Techniquement, il suffit de :

1. Créer un groupe sur Signal (Paramètres > Nouveau groupe), y ajouter au moins une personne en plus de vous-même, et lui donner un nom ;
2. Aller dans les Paramètres de ce groupe et activer l'option "Lien de groupe"
3. Une fois dans la page Lien de groupe (qu'on vient d'activer), choisir de "partager" le lien (Partager > Copier le lien) ;
4. Vous rendre sur la boucle WhatsApp, y coller le lien et inviter tout le monde à vous rejoindre.





L'opération de création d'un groupe et de partage de son lien ne prend que quelques secondes. Mais c'est là que les freins arrivent. Depuis une semaine environ je me suis lancé dans le transfert de plusieurs boucles WhatsApp auxquelles je participe dans le cadre de mes activités militantes à EELV. Je ne tiens pas un compte précis des différentes boucles, mais je suis inscrit au moins sur une dizaine de ces boucles, et encore, je ne pense pas être parmi les plus investis !

Depuis une semaine donc, voilà ce que j'ai pu constater dans cet effort de migration :

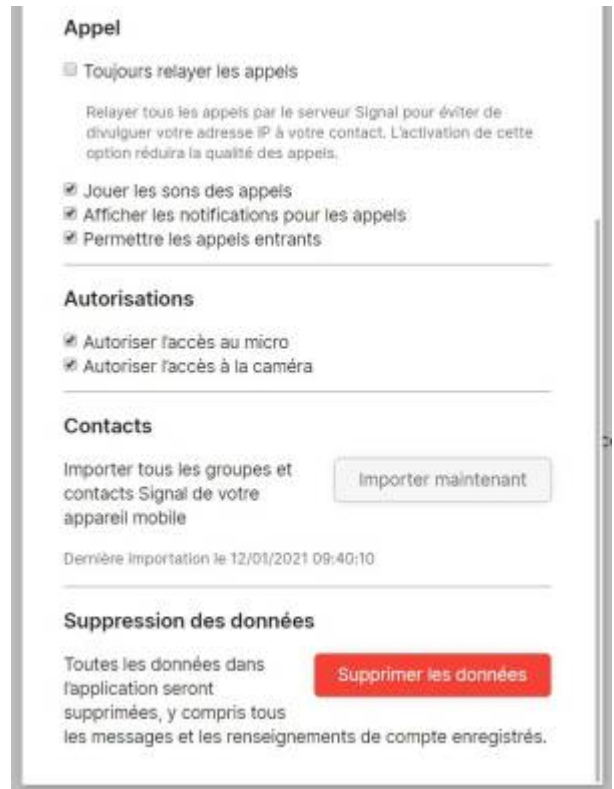
1. Première étape, il faut **expliquer pourquoi** ce serait peut-être une bonne idée de migrer. C'est un préalable nécessaire (et c'est bien pour ça que je rédige l'article que vous êtes en train de lire :) ) ;
2. Ensuite, il faut **savoir prendre son temps**, la migration d'un groupe de plus de 30 personnes se réalisera rarement en une seule journée, il faudra peut-être une bonne semaine pour que tout le monde fasse le pas ;
3. Pendant cette période de transition, la **hiérarchie des deux groupes** doit être très claires : le groupe officiel reste le groupe WhatsApp, le groupe Signal est encore en gestation et ne doit pas servir à lancer des discussions parallèles, sinon ce sera vite le bordel et on accusera vite l'initiative de migration d'avoir sapé la dynamique qui était en cours sur WhatsApp... ;
4. **Quand supprimer le groupe WhatsApp ?** C'est seulement une fois que quasiment toutes les personnes inscrites se sont décidées à adhérer au groupe Signal, qu'on peut prendre la décision de supprimer le groupes WhatsApp d'origine. Je dis quasiment parce que, si dans un groupe de 80 personnes par exemple, une seule personne dit *"non, je n'utiliserai pas Signal !"*, est-ce bien raisonnable de conserver le groupe WhatsApp pour autant ?

Mon expérience depuis une semaine de tentatives de migration (déjà 5 ou 6 groupes "basculés", entre 5 personnes et 70 personnes) me fait dire que lorsqu'on propose le lien, entre 15 % et 25 % des membres vont cliquer sur le lien et donc arriver sur Signal en quelques minutes. Et puis... ça ralentit énormément... Pour motiver les autres à ne pas trop tarder, je n'ai pas trouvé d'autre solution que de rappeler, une ou deux fois par jour, combien de personnes sont déjà inscrites sur le groupe Signal, mais sans trop insister non plus : *"Nous sommes déjà 25 sur le groupe Signal !", "ça y est plus de la moitié des inscrits à ce groupe ont basculé sur Signal, j'en profite pour vous rappeler le lien pour y adhérer à votre tour"*.

Il m'est même arrivé de faire une capture d'écran du groupe Signal avec toutes ses mentions *"intel vient d'adhérer au groupe"*, les unes à la suite des autres, et de la balancer sur le groupe WhatsApp correspondant, histoire de donner envie aux autres de franchir le pas.

## Aller plus loin avec Signal

Dans l'ensemble, les fonctionnalités de Signal sont tout à fait comparables à celles de WhatsApp, vous vous y retrouverez très facilement, notamment grâce au [Signal Desktop](#) mentionné plus haut. Les paramètres des groupes mettent en avant plusieurs actions qui peuvent s'avérer très utiles, et l'application est mise à jour régulièrement (au moins une fois par mois).



Au moment où je rédige cet article, je note ces quelques fonctionnalités qui sont à portée de main, dans les paramètres :

- On peut choisir de rendre l'adhésion à un groupe automatique ou au contraire la **soumettre à validation préalable** de son administrateur-trice ;
- On peut (on doit !) **désactiver le "lien de groupe"**, pour éviter que ce lien ne puisse servir ensuite à quelque intru qui voudrait aller voir de quoi on y cause. Ce n'est pas anodin : la mésaventure était arrivée à WhatsApp en février dernier <sup>18)</sup> ;
- On peut permettre les **messages éphémères dans un groupe**, c'est-à-dire des messages qui vont disparaître après leur lecture et qui n'apparaîtront plus ensuite dans l'historique ;
- Comme sur WhatsApp, Signal permet de **retrouver facilement les médias et documents échangés** dans le groupe (Menu > Tous les médias). Les fichiers sont classés par type : Médias, Fichiers, Sons, Tout. Très pratique pour retrouver ce PDF de compte rendu de réunion qui date d'il y a six mois...
- Enfin, depuis quelques jours, Signal propose un service de **visioconférence de groupe**, à concurrence, pour le moment, de huit participants en même temps. Mais les développeurs annoncent vouloir rapidement augmenter le nombre de participants.

Un dernier point : comme la plupart des applis de tchat, Signal peut aussi **prendre en charge vos SMS**. Sur mon terminal, j'utilise donc désormais Signal pour les deux fonctions, groupes de discussion et SMS... Et de fait, je compte bien supprimer au final deux applications appartenant aux GAFAM : l'appli Messages de Google que j'utilisais jusqu'ici pour les SMS, et l'appli WhatsApp de Facebook... Mais attention, à l'usage, je me suis aperçu d'un détail potentiellement gênant : le Signal Desktop n'a pas connaissance des SMS échangés sur le smartphone, et donc vous n'y verrez apparaître que vos échanges avec les autres utilisateurs de Signal qui ont créé un compte Signal. Si votre correspondant utilise un autre logiciel de SMS et n'a pas de compte Signal, alors vous ne pourrez lui répondre que depuis votre smartphone, et la discussion en question ne sera pas visible depuis le Signal Desktop.

## En guise de conclusion

Nous sommes peut-être au tout début d'un mouvement de fond, avec une meilleure visibilité sur toutes les données personnelles récupérées par les réseaux sociaux et les applications qu'on nous "offre" plus ou moins gratuitement sur nos smartphones et nos ordinateurs. Ou bien, peut-être, comme beaucoup d'autres, Signal va retourner aux marges face à l'indéboulonnable domination de WhatsApp de Facebook... Difficile à dire aujourd'hui, mais en tout cas, les mois qui vont suivre vont être intéressants à surveiller.

Pas plus tard qu'aujourd'hui, au moment où j'achevais ce long article (environ 10 pages si vous l'imprimez en PDF), j'ai découvert un nouveau site qui se propose de référencer très en détail une liste assez impressionnante d'applis de tchat, dont Signal bien entendu, et beaucoup d'autres, dont le Messages de Google (ah, enfin !), Viber ou Riot.

En tout, une douzaine d'applications sont comparées, sur des considérations très détaillées comme l'origine des financements reçus par l'entreprise ou la fondation qui propose l'application, le fait qu'un audit de sécurité ait été réalisé ou pas sur la solution proposées, la qualité de la documentation pour en comprendre le code source, la possibilité ou pas de créer un compte de manière tout à fait anonyme, etc.

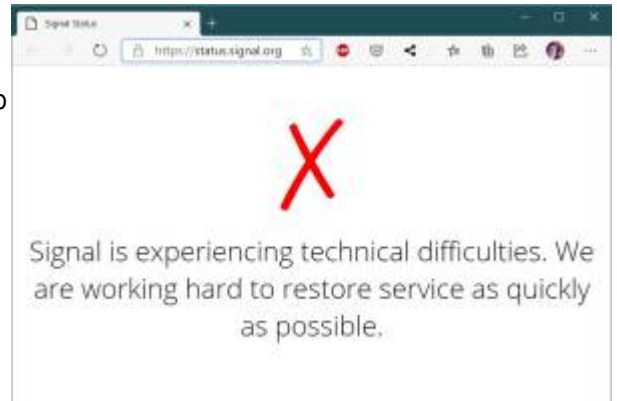
Et trois seulement de ces applis sont considérées comme vraiment sûres du point de vue des données personnelles et du respect de la vie privée : Signal, mais aussi [Threema](#) et [Wire](#).

C'est par ici : <https://www.securemessagingapps.com/>

	Google Messages	Apple iMessage	Facebook Messenger	Element / Riot	Signal	Microsoft Skype	Telegram	Threema	Viber	Facebook Whatsapp	Wickr Me	Wire
TL:DR: Does the app secure my messages and attachments?	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes
Company jurisdiction	USA	USA	USA	UK	USA	USA	USA / UK / Belize / UAE	Switzerland	Luxembourg / Japan	USA	USA	Switzerland
Infrastructure jurisdiction	Worldwide (rollout ongoing, unsure of exact locations, most likely Google Cloud regions)	USA (Ireland and Denmark planned); iMessage runs on AWS and Google Cloud	USA, Sweden (Ireland planned)	UK (and potentially all jurisdictions, given it's a decentralised messaging platform)	USA	USA, the Netherlands, Australia, Brazil, China, Ireland, Hong Kong, and Japan	UK, Singapore, USA, and Finland	Switzerland	USA	USA (unsure of other locations)	USA (unsure of other locations)	EU
Implicated in giving customers' data to intelligence agencies?	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	No
Surveillance capability built into the app?	No	No	No	No	No	Yes	No	No	No	No	No	No
Does the company provide a transparency report?	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Company's general stance on customers' privacy	Poor	Poor	Poor	Good	Good	Poor	Poor	Good	Poor	Poor	Good	Good
Funding	Google	Apple	Facebook	New Vector Limited	Freedom of the Press Foundation / the Knight Foundation / the Shuttleworth Foundation / the Open Technology Fund / Signal Foundation (Brian Acton)	Microsoft	Pavel Durov	User pays / AFinum Management AG	Rakuten / friends and family of Talmon Marco (it's very unclear)	Facebook	Gilman Louie / Juniper Networks / the Knight Foundation / Breyer Capital / CME Group / Wargaming	Janus Friis / Iconical / Zeta Holdings Luxembourg

## Quelques suites

Le vendredi 15 janvier à 16h, heure française, les serveurs de Signal sont “tombés”, à cause de l'afflux massif de nouveaux utilisateurs depuis quelques jours.<sup>19)</sup> L'interruption de service dure encore lundi soir vers 23h. Le compte Twitter @signalapp précisait deux jours avant que le nombre d'installations de l'application depuis le Play Store de Google était passé de 10 millions à 50 millions en l'espace d'une seule journée ! Il y aurait en moyenne presque 4 000 nouveaux comptes créés chaque minute sur Signal depuis quelques jours...



Le même jour, WhatsApp annonce sa décision de repousser ses nouveaux CGU, obligatoires pour continuer à utiliser l'application, au 15 mai, au lieu du 8 février, en arguant du fait qu'il y a trop de “confusion” et “d'informations erronées” sur ces nouvelles règles.<sup>20)</sup> En parallèle, un article du magazine anglais Wired d'avril 2020 réapparaît sur les réseaux sociaux<sup>21)</sup>, et liste les raisons d'abandonner WhatsApp pour Signal, avec notamment cet argument : “Peut-être que la raison la plus convaincante pour utiliser Signal est la longue histoire du manque de respect de Facebook envers la vie privée de ses utilisateurs”<sup>22)</sup>

1)

[WhatsApp radicalise la droite dans le Brésil de Bolsonaro - 25 août 2019 - Huffington Post](#)

2)

[Coup bas en pagaille: les dessous du rachat de WhatsApp par Facebook - 27 septembre 2018 - 01Net](#)

3)

[WhatsApp now requires you to share data with Facebook — or stop using the app - 7 janvier 2021 - iMore](#)

4)

[WhatsApp Beaten By Apple's New iMessage Privacy Update - 3 janvier 2021 - Forbes](#)

5)

Extrait d'origine en anglais : “Clearly, mandating user acceptance of this data sharing with Facebook will be a game changer for many users. While messages remain encrypted, this will raise further concerns around the monetization of user data by the Facebook machine.

6)

[Voir l'article Wikipédia en français sur le RGPD](#)

7)

[voir l'article Wikipédia français USA Patriot Act](#)

8)

[Voir l'article Wikipédia français Edward Snowden](#)

9)

A l'époque, j'avais rédigé plusieurs articles à ce sujet, en tant que co-responsable de la commission nationale thématiques Partage 2.0 / Libertés numériques, voir notamment [2015 : Les trois dérives du nouveau projet de loi sur le renseignement](#) et [La Neutralité du Net](#), pourquoi c'est important, et pourquoi le Parlement Européen doit la défendre

10)

[En 2012, la CIA a espionné l'élection présidentielle en France - 17 février 2017 - L'Express](#)

11)

[Espionnage : Merkel, arroseuse arrosée - 1er mai 2015 - Libération](#)

12)

[Espionnage de salariés : Ikea et plusieurs ex-dirigeants renvoyés en correctionnelle - 14 mai 2020 - 20 Minutes \(AFP\)](#)

13)

[6 questions pour comprendre les accusations d'espionnage contre Huawei - 22 mai 2019 - Le Monde](#)

14)

[Comment WhatsApp permet à des inconnus de vous espionner à votre insu - Avril 2019 - 01.Net](#)

15)

[Les Etats-Unis Lancent Une Nouvelle Attaque Contre Le “Cryptage De Données” d'Apple - 9 janvier 2020 - Forbes.com](#)

16)

Trump supporters flock to messaging app Telegram after Parler goes offline - 11 janvier 2021 - The Telegraph

17)

Tout comprendre à Signal, la messagerie préconisée par Edward Snowden - 8 janvier 2021 - Numérama

18)

WhatsApp : vos groupes privés et vos numéros sont peut-être accessibles sur Internet - 22 février 2020 - Le Parisien

19)

Signal down after getting flooded with new users - 15 janvier 2021 - Bleeping Computer

20)

Plus de temps pour notre récente mise à jour - 15 janvier 2021 - Blog officiel de WhatsApp

21)

Why everyone should be using Signal instead of WhatsApp - 15 avril 2020 - Wired

22)

Version originale : *"Perhaps the most compelling reason to use Signal is Facebook's long-standing lack of respect for its users' privacy."*

From:

<https://www.gregorygutierrez.com/> - Travailler avec le sérieux d'un enfant qui s'amuse

Permanent link:

<https://www.gregorygutierrez.com/doku.php/linux/pourquoi-et-comment-passer-de-whatsapp-a-signal?rev=1610793363>

Last update: **2021/01/16 11:36**

