Signal défaillant : réflexions sur l'usage des communications dans les milieux militants

anonyme

Juin 2019

une traduction de wtfspvm.
labeur PIPELINE PATRIARCAL
révision COPIEUSE CANNIBALE
couverture ADOLPH VON MENZEL, tiré du livre *Die Werke Friedrichs des Großen, vol.* 2, 1913
typesetté avec TEX & fonts IM FELL ENGLISH
Printemps 2024

wtfspvm.net

Article original

NOTE DE L'AUTEUR•E

Ce zine a été originalement publié en mai 2019. Signal mets à jour ses fonctionnalités de manière périodique. Pour être à jour sur les informations techniques, visitez *signal.org*, *community.signalusers.org*, et */r/signal* sur reddit.

Pour contacter l'auteur•e : signalfails@riseup.net

Signal est un service de messagerie crypté qui existe sous plusieurs formes depuis environ 10 ans. Depuis, c'est un logiciel qui a été largement adopté par les réseaux anarchistes à travers le Canada et les États-Unis. De plus en plus, pour le meilleur ou pour le pire, nos conversations interpersonnelles et de groupes ont migré sur la plateforme Signal, au point de devenir la manière de communiquer par excellence des anarchistes sur ce continent, avec très peu de débats publics par rapport aux implications de cette situation.

Le logiciel Signal est une application pour téléphone [1]. Ce changement d'habitudes de vie qui se produit est relié à une vie qui est de plus en plus médiée par les écrans de téléphones et les réseaux sociaux. Ça a seulement pris quelques années pour que les téléphones intelligents deviennent obligatoires pour quiconque qui veulent des ami•es ou qui auraient besoin d'un travail, à quelques exceptions près. Jusqu'à maintenant, les milieux anarchistes étaient une de ces exceptions ; on pouvait refuser de trimbaler un téléphone intelligent et quand même être capable d'exister socialement. Maintenant j'en suis moins sûr•e, et c'est crissement déprimant. Je vais donc faire ma tête de cochon et insister sur le fait qu'à travers ce texte ,qu'il n'y a aucune substitution aux relations en face à face dans le monde réel, avec toute la richesse et la complexité du langage non verbal, des émotions, du contexte physique, et qu'elles continuent

1. ndlt Une application pour ordinateur est disponible, mais il faut préalablement s'enregistrer au moyen d'un téléphone.

d'être la manière la plus sécuritaire d'avoir une conversation privée. *Please*, laissons nos téléphones à la maison, rencontrons-nous dans la rue ou dans la forêt, conspirons ensemble, faisons de la musique, construisons des affaires, détruisons en d'autres, et cultivons nos vies hors-ligne ensemble. Je pense que c'est plus important que de savoir utiliser Signal correctement.

L'idée de faire ce zine m'est survenue il y a environ un an, lorsque je visitais des ami•es dans une autre ville et que je blaguais à propos des manières que les conversations Signal par chez nous tournent en catastrophe. Ces blagues ont immédiatement fait écho chez mes ami•es, et c'est à ce moment que j'ai réalisé que cette conversation se produisait à plusieurs endroits. En tâtant le terrain, tout le monde avait des plaintes et des opinions, mais peu de pratiques communes en émergeaient. J'en suis venu à avoir une liste de questions que j'ai fait circuler dans mes réseaux. J'ai été surpris•e de recevoir une douzaine de réponses détaillées, et combinées à plusieurs conversations informelles, ce qui informe donc la majorité de ce texte [2].

Je suis pas un•e expert•e — je n'ai pas étudié en cryptographie et je ne sais pas coder [3]. Je suis un•e anarchiste avec un intérêt pour la sécurité avec une approche holistique, et un scepticisme envers la technologie. Mon but avec ce texte est de faire refléter la manière dont Signal est devenue tellement centrale

2. Un gros merci à tout le monde qui a soumis quelque chose ! J'ai volé beaucoup de vos idées.

3. NDLT Par contre la traduction oui.

pour la communication entre anarchistes [4] dans notre contexte, d'évaluer les implications de ce contexte pour notre sécurité collective et notre organisation sociale, et de proposer des pistes de solutions pour développer des pratiques communes.

Une brève histoire de Signal

Il y a de cela 25 ans, les optimistes technologiques parmi nous voyaient l'émergence d'internet comme un énorme potentiel pour devenir un outil libératoire. On se rappelle le vieux segment de la *CBC* qui faisait l'éloge « d'un réseau d'ordinateurs appelé internet » comme étant « l'anarchie modulée » ? Même s'il y a encore des manières efficaces de communiquer de manière sécuritaire, de se coordonner et de répandre des idées en ligne, il est clair que l'État et les entités corporatives capturent de plus en plus l'espace virtuel pour nous subjuguer en augmentant graduellement les formes de surveillance et contrôle social intense [5] Internet a toujours été une course à l'armement. En 1991, le cryptographe, activiste militant pour les droits civils pour la paix, Phil Zimmerman créa *Pretty Good Privacy* (*PGP*), qui est une application *open-source* pour cryp-

4. NDLT et autres groupes d'extrême gauche.

5. Les modes de gouvernance à l'ère d'internet vont varier d'un endroit à l'autre – les états autoritaires vont préférer utiliser le filtrage et la censure d'information, tandis que les états démocratiques vont produire un genre de « citoyenneté numérique » – mais la surveillance de masse et la guerre cybernétique deviennent la norme.

ter des fichiers et de chiffrage *end-to-end* de courriels [6] Bon, j'épargne à tout le monde les détails techniques, mais *basically*, l'importance du *end-to-end* est que l'on peut directement communiquer de manière sécuritaire avec une autre personne, et le service de courriel ne peut pas voir le message, que ce soit *Google* ou *Riseup*. À ce jour, du moins à ce que l'on sait, l'encryption *PGP* n'a jamais été brisée [7].

Pendant des années, les *geeks* de sécurité dans certains cercles – anarchistes, journalistes, criminels, etc. – ont essayé de répandre l'utilisation du *PGP* dans leurs réseaux en tant qu'infrastructure de communication sécurisée, et ce avec un certain succès. Comme avec tout, il y a des limitations. Ma plus grande crainte en termes de sécurité [8] Avec le *PGP* est le manque de

---

6. Ironiquement, le gouvernement des États-Unis essaiera plus tard d'inculper Zimmerman avec distribution de code source PGP, prétextant qu'il « exportait des armes ». Il publia donc le code source sous la forme d'un livre et en posta partout à travers la planète, le motif étant que l'exportation de livres est protégée en vertu de la Constitution des États-Unis.

7. Les procès contre les *Brigate Rosse* en Italie (2003) et les exploiteurs de pornographie juvénile aux États-Unis (2006) ont démontrés que les services de police fédérale ont échoués à briser les appareils et communications sécurisées avec *PGP*. À la place, les agents ont mis sous écoute les appareils, passé une législation qui nous oblige à divulguer nos mots de passe, et bien sûr, d'utiliser des indics et des opérations d'infiltration.

8. Jusqu'à très récemment, *PGP* n'encryptait pas les métadonnées (tel qui envoie un courriel à qui, sur quels serveurs, à quel moment), ce qui était un gros problème. Un avocat de la *NSA* a déjà dit, « si j'ai assez de métadonnées, je n'ai pas vraiment besoin du contenu ».

Forward Secrecy, ce qui signifie que si une clé d'encryption privée [ce qui, dans ce contexte, sert à décrypter les messages et n'est jamais divulgué à qui que ce soit] est compromise à un certain moment, tous les courriels qui ont déjà été envoyés avec cette clé peuvent être décryptés par un assaillant. C'est une vraie préoccupation, en prenant en considération que la *NSA* (*National Security Agency*) a sûrement stockée tous les courriels encryptés quelque part, et un jour les ordinateurs quantiques seront capables de briser l'encryption *PGP*. Me demandez pas d'expliquer comment les ordinateurs quantiques fonctionnent – du mieux de mes connaissances, *it's evil fucking magic*.

Le grand problème social avec *PGP*, et celui qui a grandement informé le projet Signal, est le fait ça n'a jamais été vraiment adopté en dehors des groupes niches. Selon mon expérience, c'était aussi difficile d'embarquer les anarchistes avec *PGP* et de l'utiliser correctement. Il y a eu des ateliers, plusieurs personnes l'ont mis en place, mais du moment que leur ordinateur *crashait* ou que leur mot de passe était perdu, on revenait à la case départ. Ça n'est juste pas resté.

Aux alentours de 2010, les téléphones intelligents ont commencé à être populaires et tout changea. L'omniprésence des réseaux sociaux, la messagerie instantanée en permanence, et la capacité aux compagnies de télécommunications (et donc le gouvernement) de traquer chaque geste des utilisateur•ices [9]

9. Envie de lire quelque chose d'effrayant ? Fait des recherches à propos du *Sensorvault* de *Google*.

a complètement transformé le modèle de risque. Tout le travail des personnes investi•es dans la sécurité informatique a été retardé de plusieurs décennies : les téléphones intelligents se basent sur une architecture complètement différente des ordinateurs, résultant en un moins grand contrôle du côté utilisateur, et l'avènement des permissions d'applications qui sont complètement illimitées ont rendu la vie privée sur un téléphone intelligent une vrai *joke*.

C'est le contexte duquel Signal a émergé. L'anarchiste *cypherpunk* Moxie Marlinspike commença à travailler sur un logiciel qui amènerait l'encryption *end-to-end* aux téléphones intelligents, avec du *Forward Secrecy*, travaillant sur l'idée que la surveillance de masse devrait être contrée avec de l'encryption de masse. Signal a été conçu pour être facile d'usage, *cute* et sécurisé. Moxie accepta de faire équipe avec des géants technologiques tels *WhatsApp, Facebook, Google et Skype* pour également implémenter l'encryption du protocole Signal sur leur plateforme.

> « La grande victoire pour nous est lorsqu'un milliard de personnes utilisent WhatsApp et ne savent même pas que c'est encrypté » — Moxie Marlinspike

De manière très compréhensible, les anarchistes auront tendance à faire confiance à Signal — un *nonprofit* géré par un anarchiste — pour leurs communications [10] que de faire confiance

10. ndlt Depuis janvier 2022, Moxie n'est plus impliqué dans Signal de

à GAFAM, dont le modèle d'affaires est de récolter et de revendre les données utilisateur. Signal à d'autres avantages par rapport à ces plateformes : c'est *open-source* (et donc sujet à revue entre pairs), ça encrypte la plupart des métadonnées, ça stocke le moins de données utilisateur possible, et ça offre des caractéristiques très utiles tels les messages éphémères et la vérification de numéro de sécurité pour se protéger des interceptions.

Signal a eu des éloges quasi universels de la part d'expert•es en sécurité informatique, incluant des mentions du lanceur d'alerte de la *NSA* Edward Snowden et des scores records de la très respectée *Electronic Frontier Foundation*. En 2014, des documents divulgués depuis la *NSA* décrivaient Signal comme une « menace importante » a sa mission (de savoir tout à propos de n'importe qui). Personnellement, je fais confiance à l'encryption.

Mais Signal ne protège vraiment que d'une seule chose, c'est la communication qui voyage de ton appareil à un autre appareil. C'est très bien, mais c'est seulement un morceau d'une stratégie de sécurité. C'est pourquoi c'est important, lorsqu'on parle de sécurité, de commencer avec un modèle de risque. La première question pour n'importe quelle stratégie de sécurité est de savoir qui est ton adversaire anticipé, ce qu'il essaie de capturer, et comment il est probable qu'il parvienne à l'avoir. L'idée de base est que les choses et les pratiques sont seulement

---

quelconque manière.

sécuritaires ou non sécuritaire relativement au genre d'attaque que tu t'attends à te défendre contre. Par exemple, tu peux avoir tes données protégées avec une encryption *de la muerte* et le meilleur des mots de passe, mais si ton assaillant•e est prêt•e à te torturer jusqu'à tant que tu donnes cesdites données, ça n'a pas plus vraiment d'importance.

Pour les besoins de ce texte, je proposerais de travailler un modèle de risque qui concerne principalement deux types d'adversaires. Le premier type est les services de renseignement au niveau mondiaux ou les puissants *hackers* qui font de la surveillance de masse et qui interceptent les communications. Le second type est les services de police qui font de la surveillance ciblée d'anarchistes, opérant sur le territoire contrôlé par le gouvernement canadien ou américain. En ce qui a trait la police, les techniques d'enquêtes de base incluent la surveillance de listes courriel et les réseaux sociaux, envoyer des agents infiltrés à des événements, et des indics à l'occasion. Ils auront à certains moments plus de ressources, ou nos réseaux deviendront une plus grande priorité pour eux, ils escaladeront alors à des techniques plus avancées incluant l'infiltration à long terme, la surveillance physique fréquente ou continue (incluant des tentatives de capturer des mots de passe), la mise sous écoute des appareils, l'interception des communications, et les descentes de police où des appareils seront saisis et sujettes à une analyse judiciaire.

Il est à noter que plusieurs juridictions européennes implé-

mentent ou ont implémenté des lois (*key disclosure laws*) obligeant légalement les individus à donner leurs mots de passe aux autorités sous certaines conditions au risque de faire face à une peine d'emprisonnement [11]. Ce n'est peut-être qu'une question de temps, mais pour Canada et les États-Unis, nous ne sommes pas légalement obligé•es de dévoiler nos mots de passe aux autorités, du moins tant que nous ne traversons pas les frontières [12].

Si ton appareil est compromis avec un *keylogger* ou tout autre logiciel malveillant, ça sert à rien de communiquer par voie sécurisée. Si tu *chill* avec un *snitch* ou un flic, ça sert pas à grande chose d'enlever la batterie de ton téléphone pour aller prendre une marche dans le parc. La sécurité d'un appareil et la culture de sécurité sont deux concepts qui ne sont pas couverts par ce texte mais qui doivent être pris en considération lorsqu'on veut se protéger se protéger de ces menaces réelles. J'ai inclus quelques suggestions dans la section *Pour en lire davantage sur le sujet*.

Il faut mentionner que Signal n'est pas conçu pour l'anonymat. Ton compte Signal est enregistré avec un numéro de

11. Le déni plausible, le *forward secrecy* et la destruction des données sécurisées sont intégrées dans des outils de protection de vie privée pour essayer de contrer cette menace ou du moins à minimiser son dommage.

12. Les empreintes (et autres données biométriques) ne sont pas considérés des mots de passe dans plusieurs juridictions, ce qui signifie que les écrans verrouillés avec une empreinte ne sont pas sujet aux mêmes protections légales.

téléphone, à moins que tu l'aies enregistré avec un *burner phone* payé *cash*, tu n'es pas anonyme. Si tu n'es plus en possession du numéro de téléphone utilisé pour enregistrer ton compte, on pourrait *hijacker* ton compte. C'est pourquoi il est super important, si tu utilises un numéro anonyme pour enregistrer ton compte [13], que tu actives la fonctionnalité « Blocage de l'inscription [14] ».

En grande partie en raison de la sécurité, Signal est devenu la norme en termes de communication dans les milieux anarchistes au cours des dernières années, éclipsant tout le reste. Mais tout comme « LE MESSAGE, C'EST LE MÉDIUM [15] », Signal influence profondément comment les anarchistes s'agencent et s'organisent ensemble.

La sociabilité de Signal

> « Signal est utile dans la mesure que ça remplace des formes de communications moins sécuritaires, mais ça devient dangereux ... lorsque ça remplace la communication en face à face. [16] » — anonyme

13. NDLT Depuis février 2024, on n'est plus obligé de divulguer notre numéro de téléphone sur Signal (au moyen d'un *username*). Mais la pratique d'avoir un numéro anonyme est encore fortement encouragé.

14. NDLT C'est pas expliqué dans le texte, mais la fonctionnalité « Blocage de l'inscription » (*Registration Lock*), oblige à rentrer le NIP Signal pour se réinscrire avec le numéro de téléphone.

15. NDLT *« the medium is the message »*

16. NDLT *« Signal is useful to the extent that it replaces less secure forms of electronic communication, but it becomes harmful ... when it replaces face-to-face communication*

Les majeures implications sociales de Signal ne sont pas spécifiquement par rapport à l'application. On parle ici des implications de graduellement transférer nos communications, expression personnelle, efforts organisés, et tout le reste sur des plateformes virtuelles et de les médier avec des écrans. Mais j'ai rapidement compris quand je passais à travers les réponses de questionnaire qu'avant Signal, je connaissais plusieurs personnes qui rejetaient en bloc les téléphones intelligents pour des raisons de sécurité et des raisons sociales. Lorsque Signal est arrivé avec des réponses à la majorité des préoccupations de sécurité, la position de méfiance a rapidement été érodée. Aujourd'hui, la plupart des récalcitrant•es ont des téléphones intelligents, soit parce que ces personnes ont été convaincu•es d'utiliser Signal ou que c'est devenu obligatoire de l'utiliser si tu voulais resté impliqué•e. Signal a fonctionné comme point d'entrée à utiliser des téléphones intelligents pour certain•es anarchistes.

D'un autre côté, si l'on considère Signal comme du *harm reduction* pour ceux•ses qui sont déjà pris dans le piège des *smartphones*, c'est une bonne chose. Je suis réjoui•e d'apprendre que le monde qui socialisait et s'organisait sur des canaux qui ne sont pas cryptés comme Facebook a fait le *switch* à Signal. Dans mon entourage, les discussions de groupe ont remplacé la « petite liste courriel [17] et c'est vraiment utile pour planifier des

---

»

17. NDLT On s'entend que y'a rien que je regarde moins que les messages

activités, partager des liens ou s'envoyer des *memes*. Dans les réponses que j'ai collectées, les groupes Signal qui sont le plus utiles aux personnes interrogées, ou peut-être simplement les groupes les moins gossants sont ceux qui sont petits, *focus* et pragmatique. Signal peut aussi être un outil puissant pour passer le mot rapidement et de manière sécuritaire sur un enjeu qui requiert une réponse dans l'immédiat. Si le fait de s'organiser sur Facebook à amener plusieurs anarchistes à croire que l'organisation avec un élément de surprise est impossible, Signal à partiellement récupéré cette idée, et j'en suis reconnaissant•e.

Signal défaillant

J'ai premièrement imaginé ce projet comme une courte série de *comics* que je voulais appeler *Signal Fails*, librement basé sur le livre *Come Hell or High Water : A Handbook on Collective Process Gone Awry* [18] Ça l'adonne que c'est difficile dessiner des images représentant des fils de discussion et que je suis poche en dessin. Je suis désolé à tout le monde à qui j'ai promis cette idée, peux être dans la seconde édition... Dans tous les cas, je veux quand même inclure quelque idées de *Signal Fails*, comme moyen de rire de nous (je m'inclus là-dedans !) et de peut être gentiment pousser tout le monde à arrêter d'être *fucking* gossant.

Bond, James Bond — Avoir Signal ne te rend pas impénétrable. Donne un peu d'encryption au monde, et ceux•ses-ci vont

d'une liste courriel... ».

18. NDLT Publié chez *AK Press*.

immédiatement exposer tous leurs contacts aux trucs les plus *sketchs*. Ton téléphone est encore un appareil qui te traque, et la confiance est encore un élément à acquérir. Parlez aux camarades des choses dont tu es confortable de parler au téléphone, et des choses dont tu n'es pas à l'aise.

Le silence n'est pas consentement — Es-tu déjà allé à une rencontre, fait des plans avec des camarades, établi un conversation Signal pour coordonner la logistique, pour finalement avoir une ou deux personnes qui changent rapidement le plan décidé de manière collective par une série de textos rapide que personne n'a vraiment le temps de répondre à? Pas cool. [19].

L'enfer c'est un meeting éternel [20] — Un groupe Signal n'est pas un *meeting* perpétuel. Je suis déjà trop sur mon téléphone, je n'aime pas quand une conversation s'active sur mon téléphone pour n'être finalement qu'une longue conversation entre deux personnes ou le fil de pensée d'une personne qui n'est pas du tout relié au propos du groupe. J'apprécie lorsque les conversations ont des débuts et des fins.

It Wants to Feed — Je méprise particulièrement celui-là. Probablement en raison des réseaux sociaux, certain•es d'entre nous est habituée à recevoir de l'information via une pla-

19. NDLT Tsé quand on parle de centraliser le pouvoir, ceci est un bon exemple.

20. NDLT La traduction ne rend pas justice à la phrase originale, *« Hell is an endless meeting »*.

teforme. Mais Signal n'est pas un réseau social, *thank fuck*. C'est pour cela que lorsqu'un gros groupe Signal commence à devenir *THE FEED*, t'es dans le trouble. Ça veut dire que si tu n'es pas assez attentif•ve, tu vas manquer toute sorte d'informations importantes, que ce soit des événements qui s'en viennent, des gens qui changent leurs pronoms, ou des guerres de mots qui mène à du conflit social. Les gens oublient que tu existes, et éventuellement, tu disparais littéralement. *Kill THE FEED* [21].

Crier au loup — aka le problème du bouton panique. Tu *chilles* dans un grand groupe Signal avec tous tes ami•es *cool et branché•es* et leur vrai numéro de téléphone, lorsqu'une personne se fait arrêter pour vol dans une épicerie *(ou whatever else)* et *surprise* son téléphone n'est pas encrypté ! Tout le monde capote et abandonne le navire, mais il est trop tard, parce que si les flics étaient en train de passer à travers le téléphone en ce moment, ils auraient pu voir tout le monde en train de quitter le groupe et le *mapping* social aurait été complété. *Womp Womp*.

Dériver de la mission — Une personne créer un groupe Signal pour la coordination d'un événement d'un temps limité.

21. NDLT Dans une perspective d'occupation, notamment pour la palestine, mes relations sont plus authentiques et fiables lorsque je ne regarde pas les conversations des groupes de coordination. Je sais déjà tout ce qui se passe car je suis physiquement sur place ! *Muter* les conversations est alors une très bonne pratique.

C'est fini, mais personne ne veut lâcher prise. *Somehow*, ce regroupement ad hoc est maintenant L'ORGANISATION PERMANENTE qui se charge de tout décider à propos de tout – indéfiniment.

Vers des pratiques communes

Si tu penses que ce guide est à propos des meilleures pratiques sur Signal ou sur avoir une bonne étiquette de messagerie instantanée, je suis désolé•e que tu te sois rendu jusqu'ici avant de réaliser que ce n'était pas le cas. C'est plus un genre *d'intervention à propos de notre* buddy *Signal*. Je crois en développer des pratiques communes dans des contextes sociaux spécifiques, et je recommande qu'on commence à en parler de manière explicite dans nos réseaux. Et pour y parvenir, j'ai quelques pistes de solution.

Il y a quelques obstacles à avoir des pratiques communes. Y'a du monde qui n'ont pas *Signal*. Si c'est parce que ces personnes construisent leurs relations sans téléphone intelligent, je n'ai que du respect pour ça. Si c'est parce que ces personnes passent leur journée sur *Facebook* mais que Signal est *trop difficile*, je n'y crois pas. À tout le moins, Signal est facile à installer et à utiliser pour toute personne possédant un téléphone intelligent et une connexion internet.

Je suis aussi en désaccord avec la perspective owerlienne-fataliste qui voit l'encryption comme un truc inutile : « Les flics savent déjà tout anyways ! » C'est une manière très *disempowering* de comprendre comment le gouvernement interagit

avec les groupes d'extrême gauche, et heureusement une perception erronée de la chose – la résistance n'est pas encore futile. La *NSA* et la *CST* (Centre de la sécurité des télécommunications) ont des capacités cauchemardesques, incluant certaines que nous ne sommes même pas encore au courant. Néanmoins, il y a beaucoup de preuves indiquant que l'encryption frustre les enquêtes policières, d'où la raison pourquoi les gouvernements essaient de passer des lois contrecarrant ces outils.

Sans doute que le plus gros obstacle des pratiques communes est un manque général du *nous* – à quel point sommes-nous redevables à qui que ce soit, et si oui, à qui ? Comment faisons pour construire de manière éthique des normes sociales communes ? La plupart des anarchistes s'entendent que c'est mal de *snitch*, par exemple, mais comment en sommes-nous arrivés là ? Je pense certainement qu'il y a un individualisme libéral vulgaire qui influence l'anarchisme et qui rend la question des *attentes* presque trop tabou à discuter. Mais c'est un *take* à aborder pour une autre journée.

Quelques propositions pour de meilleures pratiques

Garder ça IRL – Comme une personne participant au sondage mentionnait, « La communication n'est pas juste par rapport à partager de l'information ». La communication en face à face construit des relations entières, incluant la confiance, et continue d'être la manière la plus sécuritaire

de communiquer.

Laisser son cell ou son laptop chez soi — au moins de temps en temps ? Surtout si tu traverses la frontière, où on peut te forcer à décrypter tes données. Si tu as besoin d'un téléphone quand tu voyages, achète un téléphone de voyage avec tes ami•es qui ne contient aucune information sensible, incluant ta liste de contact.

Sécuriser ses appareils — La plupart des appareils (téléphones et ordinateurs) ont maintenant l'option d'encrypter entièrement le disque dur. L'encryption est seulement aussi efficace que ton mot de passe et protège tes données *at rest*, c'est-à-dire lorsque l'appareil est à *OFF* ou lorsque les données ne sont pas utilisées par une application. Ton écran de verrouillage te donne la même protection lorsque ton appareil est à *ON*, mais peut tout de même être *bypassé* par un•e assaillant•e sophistiqué•e. quelques systèmes d'exploitation obligent d'utiliser le même mot de passe que l'écran de verrouillage, ce qui est navrant car ce n'est pas pratique de taper un long mot de passe 25 fois par jour (et ce parfois avec la présence d'yeux indiscrets [22] ou des

22. NDLT Il y a d'autre manière de sécuriser son téléphone contre les oué-reux•ses, notamment avec des mesures biométriques. Certain•es diront que ce n'est pas sécuritaire dans un contexte de manif, car ce serait facile pour la police d'ouvrir le téléphone avec force (ce qui est absolument vrai), mais qui peut être très utile dans une situation de violence conjugale.

caméras de surveillance [23]).

Éteindre ses apparelis — Si tu laisses ton appareil sans surveillance, ou que tu vas faire dodo, ferme-le. Achète-toi un réveil matin *cheap*. Si ta maison se fait *raid* en plein milieu de la nuit, tu seras *ben*content•e de l'avoir acheté. Si ton appareil est fermé et encrypté avec un mot de passe puissant au moment de sa saisie, les flics auront beaucoup de mal à réussir à rentrer dedans. Si tu veux être *next level*, achète-toi un coffre-fort décent et verrouille tes appareils à l'intérieur lorsque tu les utilises, ce qui réduit le risque qu'ils soient physiquement compromis à ton insu [24].

Établir des limites — Nous avons tous•tes une définition différente de ce qu'on trouve sécuritaire de parler sur nos téléphones et ce qui ne l'est pas. Discutons et développons ces limites collectivement, et aussi l'où nous ne sommes pas d'accord. Respecte les limites des autres même si tu penses que c'est sécuritaire selon toi.

Se mettre d'accord sur un système de vouching — Si tu es dans un groupe qui discute de trucs sensibles, développez collectivement une compréhension explicite de ce qui constitue un *vouch* lorsqu'une nouvelle personne vous joint. Dans

23. NDLT Un écran de protection *anti-spy* peut être une solution

24. NDLT Cette suggestion est optionnelle, une pratique de sécurité trop compliquée à plus de chances d'entraver sa propre efficacité que d'être *actually* sécuritaire. Un bon modèle de risque prend en considération l'accessibilité des méthodes implémentée.

une époque où les anarchistes reçoivent des accusations de conspirations, la mauvaise communication peut faire en sorte que des camarades se retrouvent en prison.

Demande le consentement d'abord — Si tu es pour ajouter une personne dans une conversation, et dévoiler son numéro de téléphone / identité au groupe en entier, demande leur consentement en premier.

Minimiser les prises de décisions — Considère laisser les décisions qui ne se répondent pas par un oui ou par un non aux *meetings* en personne, si possible. Selon mon expérience, Signal appauvrit le processus de prise de décisions.

Un objectif clair et défini — Idéalement, un groupe Signal a un but spécifique. Chaque nouvelle personne ajoutée au groupe devrait avoir ce but clairement expliqué. Si l'objectif est accompli, quitte le groupe et supprime-le.

Messages éphémères — Très pratique pour garder ça *spic & span*. Variant entre 5 secondes et 4 semaines, les messages éphémères peuvent être réglés en sélectionnant la partie supérieure de la conversation. Plusieurs personnes utilisent le temps de disparation standard d'une semaine pour tous leurs messages, que la conversation soit de nature sensible ou non. Choisis un temps d'expiration basé sur ton modèle de risque. Ça peut aussi être utile lorsqu'on communique avec une personne qui a des pratiques de sécurité de piètre qualité.

Vérifier les numéros de sécurité — Ceci est le meilleur moyen de se protéger d'une attaque *man-in-the-middle*. C'est facile à faire et encore plus facile en personne — ouvre ta conversation avec la personne avec qui tu veux vérifier et navigues à Réglages de la conversation > afficher le numéro de sécurité et scanne le code QR (ou compare les nombres). La plupart des répondant•es ont dit « Je devrais le faire, mais je ne le fais pas. ». Prenez avantage des *partys* et des grands rassemblements pour vérifier tes contacts. C'est *OK* d'être *nerd* !

Activer le verrou d'écran — Cette option peut être activée en sélectionnant la photo de profil en haut à gauche > Paramètres > Compte. Si, de quelconque manière, une personne parvenait à *hacker* ton numéro de téléphone utilisé pour enregistrer ton compte, il leur faudrait quand même ton *NIP* pour usurper ton identité. Cette fonctionnalité est particulièrement importante pour les comptes Signal [25] anonymes, parce qu'il est presque certain que ce numéro sera utilisé à nouveau.

Cacher le contenu des notifications — Empêcher les messages d'apparaître sur l'écran de verrouillage. Sur mon appareil, j'ai dû configurer ce paramètre dans les paramètres de l'appareil (et non les paramètres de Signal) sous Écran de verrouillage greater Notifications de contenu sensible.

25. ndlt Est-ce qu'on dit des Signaux ou des Signals ?

Supprimer les vieux messages — Faut faire le ménage de temps en temps. Soit en activant les messages éphémères ou en supprimant manuellement les conversations terminées, ne garde pas les messages qui ne te servent plus.

Conclusion

J'ai embarqué dans ce projet pour avoir du *feedback* et refléter sur l'impact que Signal a eu sur les réseaux anarchistes aux États-Unis et au Canada, autant d'un point de vue de sécurité que d'organisation sociale. Avec cette démarche, je crois que j'ai mis le doigt sur des frustrations communes que les gens avaient, particulièrement avec les groupes Signal larges, et j'ai rassemblé les pistes de solutions offertes pour les faire circuler le plus largement possible. Je continue d'insister sur le fait que les téléphones intelligents font plus de mal que de bien à nos vies et dans nos luttes, et parce que c'est important pour moi de le faire. Nous avons besoin de préserver et construire d'autre manière de nous organiser, particulièrement hors-ligne, que ce soit notre qualité de vie ou la sécurité du mouvement. Au-delà des enjeux soulevés dans ce texte en lien avec l'usage des téléphones, la centralisation de nos communications est dangereuse. Si les serveurs de Signal se faisaient *shutdown* du jour au lendemain, ou Riseup.net, ou Protonmail, imagine comment cela serait dévastateur pour nos réseaux. Lorsque les anarchistes [26] deviennent une réelle menace pour l'ordre établi,

26. NDLT et tous autre groupes organisés de la gauche radicale.

ils s'en prennent à nous et à nos infrastructures sans aucune pitié, incluant la suspension de la « protection légale » que nous dépendons peut-être de [27]. Pour le meilleur et pour le pire, je crois que ce scénario a bien des chances de se réaliser au cours de nos vies, et nous devons nous organiser dans une perspective de résilience.

Les technophiles et *cyberwitches* parmi nous continuent d'expérimenter avec d'autres protocoles, logiciels et systèmes d'exploitation [28], et les partagent lorsqu'ils se prouvent utiles. Les récalcitrant•es devraient continuer à être récalcitrant•es, et trouver des manières de s'épanouir hors-ligne. Pour les autres, minimisons le degré auquel nous sommes aspiré•es par nos téléphones. Parallèlement à notre capacité de lutter, nous devons construire des vies qui valent la peine d'être vécues, avec des relations de qualité que nos ami•es potentiels et nos co-conspirationnistes trouveront irrésistiblement attrayantes. C'est peut-être le seul espoir que nous avons.

---

27. NDLT La loi 78 lors de la grève étudiante de 2012 au Québec et le règlement P6 à Montréal sont de bons exemples de suspension de droits humains

28. J'ai récemment remplacé sur mon téléphone Android par LineageOS, qui est un système d'exploitation *dégooglé* orienté sur la préservation de la vie privée dont le code est basé sur Android. C'est bien, mais c'est seulement compatible avec certains appareils, tu perds ta garantie et il y a définitivement une courbe d'apprentissage pour être en mesure de le configurer, de le garder à jour et de faire la transition aux logiciels *open-source*.

Pour en lire davantage

Your Phone is a Cop (It's Going Down)

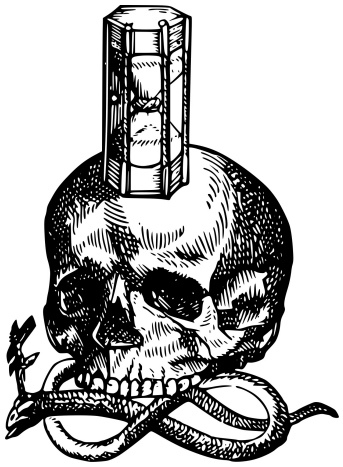
Choosing the Proper Tool for the Task(CrimethInc.)

EFF Tool Guides for Surveillance Self-Defense (incluant Signal) (EFF)

Towards a Collective Security Culture (CrimethInc.)

Toronto G20 Main Conspiracy Group : The Charges And How They Came To Be (North Shore)

POLÉMIQUE • INVENTIVE • DESTRUCTRICE



wtfspvm. EST UN COLLECTIF *anarchiste, queer et nihiliste*. Basé à Tiohtiá:ke, au soi-disant Québec, nous travaillons principalement à la traduction et la diffusion de textes dans une perspective *anticolonialiste, transféministe, anticapitaliste et nihiliste*. wtfspvm n'est pas intéressé par les guerres de clans et d'idées, mais souhaite plutôt participer à la diffusion de textes de diverses tendances en français. En effet, la majeure partie de la littérature anarchiste, libertaire, queer ou anticoloniale diffusée sur l'île de la tortue est uniquement disponible en anglais, ce qui contribue selon nous à maintenir une distance entre les milieux anglophones et francophones.