# Risques pour la vie privée liés aux personnes proches

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 juin 2020

https://www.bortzmeyer.org/privacy-intimate.html

---

De nombreux articles ont été écrits sur la vie privée, et sur sa défense dans le monde numérique. Beaucoup de techniques ont été développées pour faire face aux menaces contre la vie privée, notamment autour du chiffrement. Mais ces techniques, quoique indispensables pour vous protéger d'un attaquant extérieur à votre entourage, ne sont pas forcément efficaces face à un proche. Or, les attaques contre la vie privée peuvent parfaitement être le fait de personnes proches, par exemple dans le cas d'un espionnage d'une épouse par un mari jaloux. Dans un article en anglais publié dans le Journal of Cybersecurity <https://www.schneier.com/academic/paperfiles/Privacy_Threats_in_Intimate_Relationships.pdf>, Karen Levy et Bruce Schneier argumentent qu'il est urgent de traiter le cas des attaquants proches.

Un attaquant proche, cela peut être un ou une conjoint·e, les parents (ou les enfants !), un ou une colocataire. Beaucoup de mesures de sécurité sont fondées sur des suppositions sur l'attaquant, suppositions qui ne sont plus vraies dans le cas d'attaquants proches. Un exemple typique est celui des questions de sécurité « quel était le nom de jeune fille de votre mère », questions auxquelles un attaquant proche peut facilement répondre. Or, alors que la littérature technique et scientifique sur la sécurité informatique est pleine d'articles sur les attaquants, leurs motivations, leurs capacités, les meilleurs moyens de s'en protéger, il y a assez peu de publications sur la classe des attaquants proches ("*intimate threats*"). Mes lecteurs et lectrices orientés vers la technique peuvent se demander en quoi ces attaques par des proches sont si spéciales et si différentes des attaques plus connues. Patience, vous allez avoir des exemples.

Ces attaques par des proches sont difficiles à quantifier, mais semblent fréquentes : dans un sondage, 31 % des personnes interrogées ont admis avoir fouillé dans un ordiphone sans autorisation. (La grande majorité des exemples cités dans l'articles concernent les États-Unis, mais il n'y a pas de raison de penser que cela soit très différent ailleurs.) Parmi les gens hébergés dans des abris pour victimes de violences conjugales, les trois quarts ont été victimes de surveillance exercée par leur agresseur via des outils numériques. Et les attaques contre la vie privée sont souvent le préalable à des attaques plus dramatiques, par exemple des féminicides.

L'article classe dans les attaques de proches la surveillance exercée par les parents sur leurs enfants mineurs. Même si elle est bien intentionnée, elle n'est pas forcément une bonne idée, et elle contribue à banaliser la surveillance.

D'abord, les auteurs notent bien que la surveillance est inévitable dans une relation entre personnes proches. Quand on vit dans le même appartement, on sait quand l'autre rentre et sort, par exemple, une information typiquement considérée comme privée. On entend l'autre ou les autres parler au téléphone, on connait ses problèmes de santé, dans un couple, on a souvent un compte joint, on partage souvent le même PC, sans séparation entre plusieurs comptes sur la machine, etc (l'article donne plusieurs références d'études concernant le niveau de partage dans les couples). On pourrait en déduire qu'il n'y a pas de vie privée quand on vit ensemble mais ce n'est évidemment pas vrai. On ne veut pas que son conjoint, son colocataire, ou ses amis savent absolument tout de vous. Et c'est évidemment encore plus vrai si on a, par exemple, un conjoint violent. Mais le problème est compliqué : le partage d'informations n'est pas un mal en soi, et le niveau de partage dépend de goûts personnels et de normes sociales, tous les deux très variables. Et il peut être vu comme une preuve de confiance (« si on s'aime, on ne dissimule pas son mot de passe »).

Parfois, la question même de savoir si l'accès aux données des autres est légitime ou pas est compliquée. S'il n'y a aucun doute qu'on ne doit pas intercepter les messages échangés par un voisin dans le train, la question est moins claire dans le cas familial. Les parents doivent évidemment suivre ce qui arrive aux enfants mineurs (d'autant plus que certains problèmes, par exemple de harcèlement, ne seront pas toujours signalés spontanément). Et même entre adultes, chercher à savoir pourquoi son conjoint ou sa conjointe semble déprimé·e ou anxieu·x·se n'est-il pas souhaitable ? L'approche classique de la sécurité informatique, avec des règles simples (« dans une communication entre Alice et Bob, toute personne qui n'est pas Alice ou Bob est un attaquant »), ne marche pas forcément ici.

Cette difficulté à différencier ce qui est une communication normale et ce qui est de la surveillance est encore plus sérieuse sur le terrain juridique : porter plainte pour de l'espionnage par un proche est difficile, la justice pouvant hésiter à trancher la question de savoir ce qu'il est normal de partager au sein du couple. C'est encore plus compliqué dans les cas où la loi donne explicitement au mari le droit de surveiller sa femme, comme en Arabie saoudite, où l'État gère même un site Web permettant aux hommes de demander à être notifiés des déplacements de leur femme <https://www.nytimes.com/2019/01/11/world/middleeast/saudi-arabia-women-flee.html>.

Notez que, dans des pays supposés plus civilisés, on voit également des horreurs, comme des applications de surveillance qui disent explicitement dans leur publicité que le but est de fliquer sa femme <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessm>. Le pire étant sans doute cette société qui vend un matelas connecté permettant de détecter les mouvements suspects dans le lit <https://www.telegraph.co.uk/news/2016/04/15/smart-mattress-lets-yo>, en votre absence (mais l'article contient d'autres exemples affreux ; aux États-Unis, les sociétés commerciales n'hésitent pas à faire ouvertement de la publicité pour des usages amoraux ; en Europe, on est plus hypocrites). Même quand la publicité ne dit pas explicitement que le but est de surveiller, beaucoup des gadgets connectés permettent de le faire facilement, et sont souvent utilisés en ce sens.

Un cas bien plus compliqué que celui du macho fliquant sa femme est celui, déjà mentionné, des parents surveillant leurs enfants. « Surveillance » n'est pas forcément un terme négatif, ici. Évidemment que les parents doivent surveiller leurs enfants mineurs, pour éviter qu'ils ne se mettent en danger, ou mettent en danger les autres. Mais le marketing exagère les dangers, pour vendre du matériel et des applications de surveillance. Cela va jusqu'à des bracelets connectés, comme ceux imposés aux prisonniers. (L'URL donné dans l'article ne marche plus, quoique la société soit toujours là, peut-être a-t-elle eu honte de son produit.) Dans le cas particulier des États-Unis, notez qu'il existe une énorme pression sociale contre tout ce qui apparait comme une négligence par les parents dans ce domaine. Policiers et même simple voisins se sentent autorisés à harceler les parents qui laissent ne serait-ce qu'un tout petit peu de liberté à leurs enfants. D'où le mouvement Free-range, qui plaide pour qu'on desserre la surveillance des enfants. Notez que ce soupçon contre les parents, et cette pression pour qu'ils resserrent la vis, est surtout dirigée contre les parents des classes populaires <https://www.nytimes.com/2018/07/27/opinion/sunday/motherhood-in-the-age-of-fear.html>.

Quant à l'activité en ligne, aux États-Unis, la surveillance de l'activité des enfants par les parents est très répandue. (Et les parents qui ne le font pas ne sont pas forcément motivés par le désir de laisser de la liberté à leurs enfants, ils peuvent simplement être incompétents techniquement.) Le but n'est d'ailleurs pas uniquement d'assurer la sécurité de l'enfant, au moins une application <https://www.bark.us/> prévient les parents quand...l'enfant utilise des gros mots en ligne.

L'article note aussi que le problème peut être inverse : dans les familles où la personne la plus à l'aise avec les outils numériques est un des enfants, les enfants peuvent violer la vie privée de leurs parents, et accéder à de l'information personnelle. Même la biométrie ne les arrête pas : comme les enfants ressemblent à leurs parents, ils peuvent parfois tromper la reconnaissance faciale <https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/>.

Parmi les attaquants proches possibles, l'article note aussi le cas des personnes âgées. Comme pour le cas des enfants, une certaine surveillance peut être bien intentionnée. (Ce qui ne veut pas dire acceptable : les personnes âgées ne sont pas des mineures.) Le problème est que les visions de la personne âgée et de celle qui décide pour elle peuvent diverger, comme dans ce sondage du journal "*The gerontologist*" <https://academic.oup.com/gerontologist>, cité dans l'article, où les surveillés avaient systématiquement une moins bonne opinion de la surveillance que les surveillants.

Enfin, parmi les personnes proches qui peuvent poser des problèmes en matière de vie privée, il y a les amis qui, sans partager autant de choses avec vous qu'un conjoint ou un ascendant, connaissent quand même pas mal de choses. Le problème est particulièrement net pour les jeunes, où les relations d'amitié peuvent être de courte durée. Les secrets confiés pendant la période d'amitié peuvent être dangereux ensuite.

Quels sont les points communs aux attaques contre la vie privée menées par des personnes proches, points qui méritent d'être pris en considération dans la recherche de solutions de protection ? D'abord, les auteurs notent que les attaquants ne sont pas toujours rationnels. Dans une attaque traditionnelle, le défenseur compte sur la rationalité de l'attaquant. Si celui-ci vise un gain financier, il ne dépensera pas d'avantage d'argent pour l'attaque que celle-ci lui aurait rapporté. Ce calcul devient faux dans le cas d'atteintes à la vie privée menées par des personnes proches, qui peuvent être motivées par des émotions irrationnelles comme la jalousie. L'un des auteurs se souvient d'avoir, enfant, occupé une journée d'oisiveté à essayer les 10 000 combinaisons possibles d'un cadenas, sans espoir d'un gain particulier, juste parce qu'il s'ennuyait. Un cambrioleur classique n'aurait pas fait cela.

Ensuite, les attaquants proches habitent souvent dans la même maison que les victimes. Cette coprésence complique sérieusement les questions de sécurité informatique où, souvent, le concepteur des solutions suppose que les différentes parties en cause sont physiquement séparées. Par exemple, regarder par dessus l'épaule pour apprendre un mot de passe est bien plus facile quand on vit ensemble. Même chose pour l'installation d'un logiciel malveillant sur l'ordinateur ou l'ordiphone de sa cible. Ou encore les systèmes d'exploitation d'ordiphone qui affichent tout ou partie d'un message entrant, même quand le téléphone est verrouillé. Un exemple plus amusant est celui de cette femme jalouse qui avait déverrouillé l'ordiphone de son mari en profitant d'une sieste <https://www.theguardian.com/world/2017/nov/08/qatar-airways-plane-forced-to-land-after-wife-discovers-husbands-affair-midflight> pour placer son doigt sur le lecteur d'empreintes digitales.

Moins amusant, mais hélas fréquent dans le cas d'attaques par un proche, le risque de menaces ou de violences physiques. Le meilleur mot de passe du monde ne sert à rien si un mari violent menace de tabasser sa femme pour avoir accès à son ordinateur. Ce risque de pression physique est rarement pris en compte dans les analyses de sécurité.

---

Dans les analyses de sécurité classiques, on suppose que l'attaquant est un étranger complet, qui n'a pas de pouvoir particulier sur la victime. Dans les cas des attaques par les proches, ce n'est plus le cas : même sans menace physique explicite, l'attaquant peut exercer un certain pouvoir, par exemple dans les cas où la femme est (légalement, ou "*de facto*") soumise au mari. Cette autorité (qui peut être en place pour d'excellentes raisons, cf. l'autorité des parents sur les enfants) complique encore les choses. Il y a également une « autorité implicite » : dans le foyer, il y a en général une personne qui pilote le système informatique et qui, via ses compétences techniques et sa mainmise sur ledit système, a un pouvoir supérieur. Et cette autorité implicite est souvent genrée : dans le couple, c'est souvent l'homme qui est l'administrateur système.

Enfin, les proches connaissent évidemment beaucoup de choses sur vous, ce qui est normal, mais peut rendre certaines attaques plus faciles.

Bon, ce n'est pas tout de décrire le problème. Et les solutions ? Évidemment, il n'est pas question d'arrêter de vivre en couple, ou d'avoir des amis, de même qu'on ne cesse pas d'avoir des relations sexuelles parce que les MST existent. La première étape est que les concepteurs de systèmes de sécurité devraient reconnaitre le problème des attaques par les proches, problème qui semble sous-estimé aujourd'hui. (J'ai écrit « les concepteurs », comme s'ils étaient tous des hommes, mais ce n'est pas parce que je ne connais pas l'écriture inclusive. L'auteure et l'auteur de l'article font remarquer que les victimes des attaques par les proches sont plus souvent des femmes, alors que les concepteurs des systèmes de sécurité sont plus souvent des hommes, et que cela peut expliquer le retard dans la prise en compte de ces attaques par les proches.)

Déjà, il n'y a pas que des solutions techniques. Il est par exemple anormal que les entreprises qui vendent des solutions de harcèlement restent impunies. La justice devrait les poursuivre <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-t>, les antivirus devraient les détecter et les bloquer <https://www.wired.com/story/eva-galperin-stalker>. Pour les systèmes à usages multiples, et qui ne sont donc pas de purs systèmes d'espionnage, c'est plus compliqué, mais l'article fournit plusieurs pistes. (L'article ne mentionne pas une autre piste de solution, celle de changements sociaux, par exemple de changement des relations entre hommes et femmes, avec moins d'indulgence pour la violence conjugale. Ces changements sont également une approche importante.)

Déjà, comme indiqué plus haut, il est temps de reconnaitre que le problème existe, et aussi d'admettre qu'il n'a pas de solution simple (personne ne propose une étanchéité complète dans les relations personnelles).

Plus concrètement, il faut que les concepteurs de systèmes informatiques cessent de considérer que l'attaquant est forcément lointain et fassent, entre autres, attention à ce qu'un système informatique affiche : l'attaquant peut être en train de regarder. C'est bien pour cela qu'on remplace les caractères d'un mot de passe par des puces, mais il faut pousser le raisonnement plus loin par exemple en se méfiant des notifications spontanées (« Vous avez reçu un message de Paul » « C'est qui, ce Paul qui t'écrit ? »). D'autre part, certaines indications visuelles peuvent poser problème. Firefox a un mode « navigation privée » (en général très mal compris et dont il y a beaucoup à dire mais ce n'est pas le sujet) et, au début, il était signalé par une barre violette très visible. Cette indication pouvait facilement être vue et attirer la suspicion (« pourquoi tu es en navigation privée ? Tu ne me fais pas confiance ? Tu as quelque chose à cacher ? ») Elle est depuis devenue plus discrète.

Ce cas contre-intuitif se rencontre également avec certaines options de sécurité bien intentionnées mais qui préviennent l'attaquant potentiel qu'on se méfie de lui. Par exemple, iOS affiche explicitement « Unetelle a cessé de partager sa localisation physique avec vous », ce qui est certainement un bon moyen de provoquer des réactions agressives chez un conjoint jaloux. Les auteurs de l'article estiment

qu'il serait préférable de pouvoir « faire semblant », en évitant de montrer un téléphone vide ou un « vous n'avez pas l'autorisation de voir ces messages », qui risque au contraire de susciter des suspicions.

Les options sélectionnées par défaut sont toujours une question cruciale en informatique, car beaucoup d'utilisateurs ne les changent pas. Ils ne savent pas comment les changer, ou n'osent même pas imaginer que cela soit possible. Mais cette importance des choix par défaut est encore plus vraie dans le cas des attaques par les proches, car une fois que le mal est fait, il peut être difficile à rattraper (je ne vous donne pas l'URL vers l'article de TechCrunch en raison de la scandaleuse interface d'acceptation du fliquage du groupe Verizon Media/Oath ; c'est d'ailleurs intéressant de voir un média qui donne des leçons aux autres en matière de vie privée se comporter ainsi ; bref, vous avez l'URL dans l'article).

Autre problème lié aux attaques par les proches : les relations évoluent. À un moment, tout va bien, on se fait une confiance totale et aveugle, puis les choses changent et on doit commencer à prendre des précautions. Il est donc important que les systèmes informatiques prennent en compte ce caractère dynamique. Un exemple ? Il faudrait que le système vous rappelle de temps en temps vos réglages et vous demande s'ils sont toujours d'actualité (« Machin est autorisé à voir vos messages privés. Souhaitez-vous continuer ? »)

Dernier point sur les pistes de solutions, mais très important : arrêter de considérer que le foyer est forcément une unité où tout le monde partage tout. L'acheteur d'un produit n'est pas forcément son seul utilisateur (même s'il est la seule personne qui compte, pour les entreprises du numérique) et il est important de permettre que les utilisateurs aient chacun leur « espace ». Si Netflix permet plusieurs profils pour un compte, ils ne bénéficient d'aucune vie privée, chacun peut voir ce que les autres ont regardé. (YouTube TV est mieux fait de ce point de vue.) Idem avec les machines partagées : si vous avez un iPhone à vous, et qu'il y a un iPad partagé dans la maison, la synchronisation des données risque de montrer à tout utilisateur de l'iPad ce qu'a reçu l'iPhone.

Au minimum, les accès des autres personnes de la maison à vos données ne devraient pas être discrets mais au contraire, il est important que chacun soit prévenu. Dans le monde physique, la surveillance est à la fois très commune (comme je l'avais signalé au début, les personnes qui habitent avec vous savent forcément plein de choses sur vous, et ce n'est pas un problème) et très visible. Tout le monde, sans être un expert en sécurité, sait ce que les proches savent de nous. Le monde numérique est différent : beaucoup de personnes ne se rendent pas compte de ce que ces systèmes informatiques permettent de connaitre, d'autant plus que la littératie numérique est très loin d'être équitablement partagée (par exemple entre hommes et femmes). Une fois n'est pas commune, je vais dire du bien de Facebook : leur système interne permet à des collègues d'accéder à des informations sur vous, mais vous en êtes prévenu·e, par une alerte spirituellement nommée Sauron.

En conclusion, les auteurs de l'article (en anglais) <https://www.schneier.com/academic/paperfiles/Privacy_Threats_in_Intimate_Relationships.pdf> nous préviennent que le problème va malheureusement sans doute s'aggraver dans le futur, avec la prolifération de gadgets connectés. Quelques efforts de protection de la vie privée sont faits, mais pas encore intégrés dans une vision globale de ce risque d'attaque par les proches.

Pour des conseils pratiques dans le cas du couple, je vous recommande l'article d'Éric, « Chacun ses comptes <https://n.survol.fr/n/chacun-ses-comptes> ».