VIE PRIVÉE ET FACEBOOK: POURQUOI JE NE POSTE RIEN DE MES ENFANTS SUR LE WEB

Rien du tout. C'est le meilleur moyen de les défendre de la reconnaissance faciale, du profilage à la Facebook et de l'utilisation future de ses données personnelles.

Par [Slate.com](http://www.slate.fr/source/slatecom) | publié le 04/10/2013 à 10h23, mis à jour le 04/10/2013 à 10h25

Je ne poste jamais rien sur ma fille sur Facebook. Absolument rien. C’est le seul moyen de la défendre contre la reconnaissance faciale et autres prospections à but commercial.

Je me souviens très bien de ce post Facebook. On y voyait «Kate» (un pseudonyme), 5 ans, la fille d’une de mes amies, debout devant sa maison en bikini jaune vif, le panneau indiquant la rue clairement visible derrière elle sur la porte d’entrée. La légende disait: «*On part à la plage pour notre week-end annuel de la Fête du travail*» et dessous figuraient plus de 50 likes et commentaires de proches –y compris d’une flopée «d’amis» que la mère de Kate connaissait à peine.

La photo avait été téléchargée sur un album Facebook, où il y avait 114 clichés rien que de Kate: toute propre et emmaillotée le jour de sa naissance, en train d’embrasser son Labradoodle, de faire de la balançoire. Mais il y avait aussi des photos d’elle dans son bain et un moment dérangeant où elle posait vêtue du soutien-gorge rose de sa mère.

Je comprends parfaitement le désir de ses parents de capturer chaque minute de la vie quotidienne de Kate; la petite enfance est tellement éphémère. Mais je sais aussi que ces posts vont affecter la vie d’adulte de Kate, et j’ai conscience de l’impact à plus grande échelle de la création d’une génération d’enfants nés dans le péché numérique originel.

Fin août, Facebook [a de nouveau mis à jour](https://www.facebook.com/about/privacy/your-info) sa politique d’utilisation des données. On peut notamment y lire:

«*Nous pouvons suggérer à un ami de vous identifier dans une photo en scannant et en comparant les photos de votre ami à des informations que nous avons rassemblées à partir de votre photo de*[*profil*](http://www.slate.fr/life/78468/enfant-vie-privee-facebook)*et des autres photos dans lesquelles vous avez été identifié*.»

En gros, cela signifie qu’à chaque téléchargement de photo, les parents de Kate aident Facebook, sans le vouloir, à faire fusionner ses mondes réel et numérique. Des algorithmes vont analyser les gens autour de Kate, les références qui y sont faites dans des posts, et au fil du temps détermineront son cercle d’intime le plus probable.

Le problème, c’est que Facebook n’est qu’un site parmi d’autres. A chaque mise à jour de statut, vidéo YouTube et post de blog d’anniversaire, les parents de Kate la privent de tout espoir d’anonymat futur.

Cela présente quelques problèmes évidents pour la Kate de demain. La puberté est en soi une période déjà assez difficile à traverser. Pourquoi rendre accessibles à ses éventuels galants de fac des centaines de photos embarrassantes et faciles à trouver? Si la mère de Kate raconte une expérience négative qu’elle vit avec sa fille, cela sera-t-il susceptible d’affecter ses chances d’intégrer une bonne université? Chacun sait que les recruteurs des facs regardent les profils Facebook et une foule d’autres sites et de réseaux avant de prendre leur décision.

Un autre problème, plus insidieux, hantera Kate jusqu’à son âge adulte et au-delà. Une myriade d’applications, de sites Internet et de textiles intelligents s’appuient sur la reconnaissance faciale aujourd’hui, et l’ère de l’omniprésence de la biométrie ne fait que commencer. En 2011, un groupe de hackers a mis au point une application permettant de scanner un visage pour obtenir immédiatement le nom de la personne et les grandes lignes de sa biographie, directement sur votre téléphone.

Déjà, des développeurs ont élaboré une interface de programmation qui fonctionne pour Google Glass. Si Google a interdit les applications officielles de reconnaissance faciale, il ne peut empêcher le lancement d’applis non-officielles. Il y a beaucoup à gagner à obtenir un accès en temps réel à des informations détaillées sur les gens avec qui nous interagissons.

Le meilleur moyen de s’en sortir est de commencer par ne pas créer ce contenu numérique au départ, surtout pour des enfants. Les parents de Kate ne se sont pas contentés de télécharger une ou deux photos d’elle: ils ont créé une mine de renseignements qui vont permettre à des algorithmes d’en savoir toujours plus sur leur fille au fil du temps. Tout espoir de réel anonymat que Kate aurait pu caresser a été tué par un cours de danse classique diffusé sur YouTube.

Sachant à quel point les contenus et les données numériques sont catalogués, mon mari et moi avons fait un choix important avant la naissance de notre fille. Nous avons décidé que nous ne mettrions jamais en ligne aucune photo ou autre information personnelle qui puisse l’identifier. A la place, nous avons créé un *digital trust fund*[compte numérique en fiducie].

Cela a vraiment commencé pendant que nous cherchions son prénom. Nous avons réduit la liste à quelques choix, que nous avons soumis (avec leurs variantes) à des recherches de domaines et de mots-clés pour voir ce qui était encore disponible. Ensuite, nous avons écumé Google pour voir quel contenu avait été posté avec ces noms, et nous avons regardé si une adresse Gmail avait déjà été créée.

Nous nous sommes tournés vers [KnowEm.com](http://knowem.com/), un site que je consulte souvent pour chercher des noms d’utilisateur, même si à la base il sert à enregistrer des noms de marque. Certes, nous avions un prénom de prédilection pour notre fille, mais nous en aurions changé si KnowEm nous avait dit qu’il était peu disponible ou si nous avions trouvé des contenus négatifs associés à notre choix.

Une fois son prénom choisi, nous avons passé plusieurs heures à enregistrer son URL et à l’inscrire sur un vaste éventail de sites de médias sociaux, tous liés à un seul compte mail qui servirait de principale clé d’accès. Nous avons mis mon adresse mail permanente comme clé secondaire –tout comme vous rempliriez des papiers administratifs financiers pour ouvrir un compte à un mineur à la banque. Nous avons construit un système de gestion de mot de passe pour qu’elle puisse stocker toutes ses informations de connexion.

Le jour de sa naissance, notre fille avait déjà un compte Facebook, Twitter, Instagram et même Github. Et à ce jour, nous n’avons jamais posté le moindre contenu.

Tous ses comptes sont actifs mais privés. Nous fouillons aussi régulièrement les réseaux de nos amis et de notre famille pour enlever toutes les identifications. Ceux qui nous connaissent bien comprennent et respectent notre règle *«pas de post sur la petite».*

Quand nous estimerons qu’elle est suffisamment mûre (à ne surtout pas confondre avec le moment où elle sera assez grande techniquement), nous lui donnerons une enveloppe contenant son mot de passe. Elle pourra commencer à réaliser en partie son identité numérique, et nous nous assurerons qu’elle prendra toutes ses décisions en étant bien informée de ce qu’il convient de dévoiler d’elle-même, et à qui.

Notre fille ne pourra pas éviter de devenir un personnage public, car dans cette nouvelle ère numérique, nous le sommes tous. J’adore les parents de Kate, ils l’élèvent bien et elle deviendra sûrement une jeune femme épatante. Mais ils lui volent toute possibilité d’avoir, une fois adulte, une personnalité numérique libérée des préjugés et des partis-pris.

***Amy Webb***