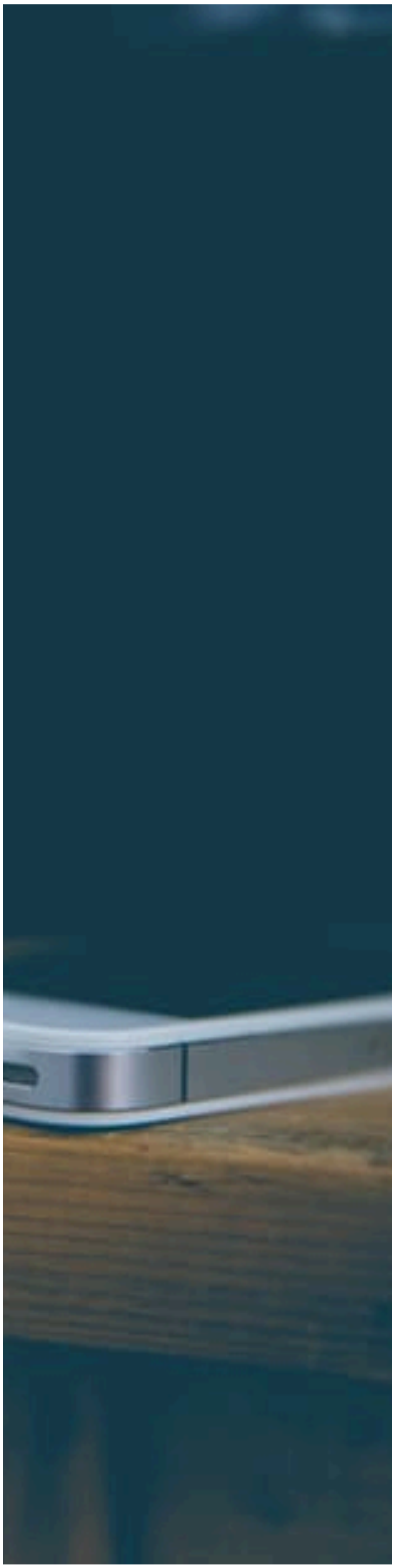


Living Things

Privacy by design : pour un IoT respectueux des données personnelles

Compte-rendu. Evénement du 3 avril 2018

Les données personnelles sont devenues l'alpha et l'oméga de l'IoT, de la personnalisation et de l'intelligence des services numériques. Dans le même temps, la confiance dans le numérique décline. Le flou autour du consentement et de l'utilisation de nos données personnelles fait partie des coupables. De plus, l'utilisation des technologies à des fins surveillance et de contrôle des individus fait l'objet de réflexions et de risques pointés par les prospectivistes.

Le RGPD qui entre en vigueur cette année oblige entre autres à solliciter le consentement explicite des utilisateurs et la mise à disposition des données dans un format lisible par machine.

Quelles sont les promesses de la « privacy by design » pour les utilisateurs? Est-ce une garantie suffisante face aux enjeux de nos usages du numérique ? Comment le marché répond-il aux nouvelles attentes ? Quelle proportion des intentions se traduit en achat de produits conçus en "privacy by design" ? Les GAFA peuvent-ils être bousculés par de nouveaux acteurs ayant une approche plus transparente (« privacy by design », voire « ethic by design ») ?

Retrouvez dans les pages qui suivent les interventions de nos invités :

- Jacques-François Marchandise, Délégué général de la FING
- Rand Hindi, CEO et fondateur de Snips
- Léonie Williamson, Product manager chez Kolibree
- Mathilde Maître, designer chez Fabernovel
- Chloé Beaumont, Hub manager à la MAIF
- Jean-Laurent Schaub, co-fondateur de Ween

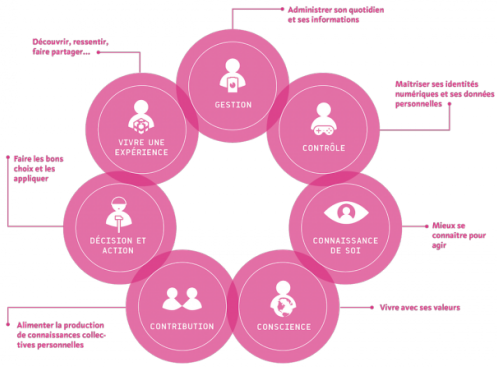
cap-digital Paris Region

Systematic Paris Region Digital Ecosystem

Introduction

Par **Jacques-François Marchandise**, Co-fondateur et délégué général de la FING

Le projet MesInfos explore ce qui se passe si on rend aux usagers le contrôle de leurs données. La CNIL la MAIF, des banques, des acteurs de l'énergie,... font partie du projet qui a donné naissance à My data.
L'utilisateur aura un usage fort de ses données et cela permet de trouver une alternative à la captation des données par les plateformes.



On prédisait il y a quelques années qu'on était dans une destruction massive de la confiance (2010-2011) et qu'on aurait à se prémunir des abus en matière de données

Peut-on faire autrement, pour apporter un service personnalisé à l'usager, que de capter massivement ses données ?

L'IoT parle de nos données personnelles. Il entre dans nos maisons, nos salles de bain, et permet d'en savoir beaucoup sur nous, les usagers. Autour d'enjeux de santé, sportifs, d'énergie, la problématique est toujours plus large... L'IoT va charrier toujours plus de données personnelles.

Concernant le RGPD, on peu s'y prendre de deux manières : cela peut être un processus lourd de mise en conformité. Mais dans ce cas on risquerait de perdre de vue la création de valeur qu'il propose. Car il peut créer de l'innovation.

L'IoT est une chance.

On va avoir un changement de relation à nos propres objets. On suppose des objets associés à des services. Leur cycle de vie va être nouveau et va poser plus largement la question de la responsabilité des concepteurs.

De façon générale dans le champ de l'économie de la donnée, il reste peu d'espace pour les concepteurs qui veulent se frotter aux GAFA. Mais dans le domaine de l'IoT, le champ des services possibles est vaste et assez dense, et il y a une valeur forte sur les efforts de conception des objets.

Les assistants vocaux en privacy by design

Par **Rand Hindi**, co-fondateur et CEO de Snips

D'ici à 2021 on va pouvoir parler à 2-3 milliards d'objets.

Amazon Echo, Google Home : l'assistant vocal était l'objet le plus vendu à Noël toutes catégories confondues sur Amazon. Plus de 50 millions d'américains en ont un chez eux. Leur adoption est plus rapide que le smartphone. On met des assistants vocaux dans tous les objets. Les TV, les voitures, ... sont des objets de plus en plus compliqués à utiliser. L'assistant vocal va permettre de parler aux objets et faciliter leur usage. Les assistants vocaux vont se démocratiser.

Tous les micros sont connectés sur internet.

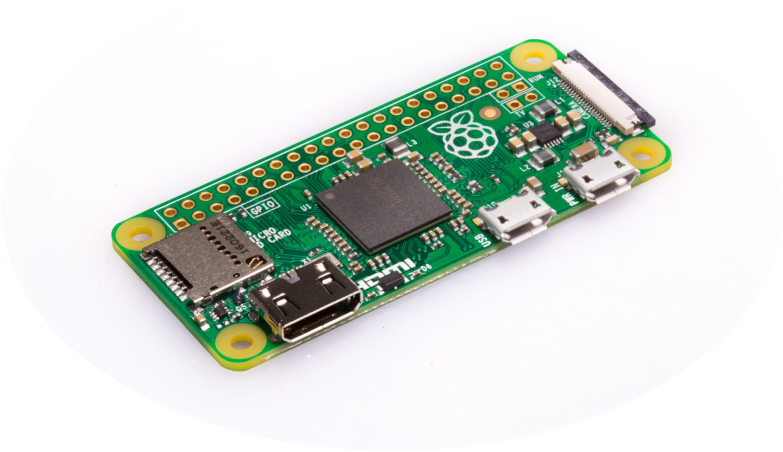
Avec les fuites de données comme on en voit dans l'actualité, on peut anticiper les problèmes auxquels on risque de faire face. Amazon est l'entreprise la moins transparente sur la privacy. De son côté, l'assistant Google Home a eu un bug dans le hardware au début : l'objet « pensait » qu'on lui parlait en permanence et enregistrait 24 heures sur 24.

Il suffit qu'un seul objet ait un problème pour que toute votre vie se retrouve sur internet.
Si on veut appliquer le privacy by design à l'assistant vocal il ne faut pas envoyer les données sur le cloud. C'est la seule solution. Tous les autres arguments, notamment un crédit de confiance, ne donnent aucune garantie de privacy ni d'intégrité. La voix est une donnée biométrique, il n'est pas possible de garantir qu'il n'y a pas d'identification de la personne. De plus il faudrait prévenir les gens qu'on invite chez soi qu'on a un assistant vocal et leur demander leur consentement. Si bien qu'il est même conseillé de le débrancher quand on ne s'en sert pas.

L'alternative pour les assistants vocaux : analyser directement dans l'ordinateur (edge computing). On va donc analyser la donnée au plus près de là où elle est produite.

Cette technologie consomme 1000 fois moins de ressources.

Ceux qui analysent la donnée dans le cloud ne se sont jamais posé la question de la performance. Snips est capable de faire tourner un assistant vocal sur un raspberry pi et est 100% compliant avec le RGPD. Pour Snips le fait que le traitement et la donnée ne sortent pas de l'objet est capital.



Snips propose une plateforme opendev et repose sur une communauté de développeurs.

L'autre défi à laquelle la société a dû faire face : récupérer la data pour entraîner l'IA. La technologie a été entraînée avec de la fausse donnée. C'est du machine learning assisté par des opérateurs humains. La performance est même meilleure qu'avec de la vraie data.

Le modèle économique de Snips est le suivant : la technologie est vendue en marque blanche aux industriels, et on facture une licence par objet (modèle classique).

La conception technique, l'expérience usager et le marché du privacy by design

Table-ronde avec **Léonie Williamson**, Product manager chez Kolibree, **Mathilde Maître**, designer chez Fabernovel, **Chloé Beaumont**, Hub manager à la MAIF, **Jean-Laurent Schaub**, co-fondateur de Ween

CareOs et Kolibree sont deux sociétés qui font partie du groupe Baracoda : CareOS propose un écosystème intelligent de la salle de bain. Kolibree commercialise une brosse à dent connectée qui permet d'avoir une meilleure connaissance des brossages. Tous les algorithmes sont embarqués dans la brosse à dent : cela donne une garantie de privacy car tout se passe dans le manche de la brosse à dent et on ne récupère aucune donnée. Il y a tout de même une question de mise en conformité RGPD. Kolibree doit analyser la conformité de l'application.

Faire le choix de ne pas collecter de données sur les clients était difficile à faire d'un point de vue marketing : pas d'informations sur les utilisateurs, pas de mailing list,... Mais on a décidé de sauter le pas.

Care OS propose de connecter tous les objets dans la salle de bain. CareOS peut par exemple analyser un grain de beauté donc cela nécessite de prendre des photos. C'est un coffre fort dans lequel toutes les données personnelles sont stockées. C'est l'utilisateur qui choisira avec qui partager ces données. On peut lui proposer de les partager avec un dermatologue si on voit que son grain de beauté a changé de forme.

Ween a été créé en partant du constat que piloter soi-même les objets du quotidien va devenir trop contraignant, surtout avec leur multiplication.

Il y a 4 ans a été créée une application qui gère les objets connectés présents dans les lieux de vie. Il y a souvent un rite immuable : on arrive dans un lieu de vie, on y reste un certain temps, et on repart. Ces patterns ont été intégrés dans la prise de décision des objets. 90% des objets réagissent de manière différente selon que vous êtes dans la maison ou non, grace au géopilotage par le smartphone.

Ça a amené un challenge technique : utiliser la localisation des smartphones sans décharger la batterie.

L'autre contrainte était de protéger des volumes de données importants stockés sur serveur car cela engendre des coûts importants. Donc il valait mieux ne pas stocker de données.

Ween prédit toutes les 10 minutes dans combien de temps la personne va rentrer chez elle. Ca n'est pas de l'IA de haut niveau mais les algorithmes font cette première couche de calcul. On arrive à le faire aujourd'hui en consommant moins de 3% des

batteries des téléphones. La solution fonctionne sans google maps.

Fabernovel travaille pour des grands groupes dans la conception de nouveaux services. Les designers se posent la question de la privacy car les utilisateurs sont au cœur de l'expérience. En 2015 nous avons travaillé à la conception d'un immeuble connecté dans le 18ème. On a imaginé des services connectés dans les appartements et dans les parties communes en partant des usages : pilotage du chauffage, de l'électricité à distance. Quelles données capter ? Comment sensibiliser l'utilisateur ? Et comment être clair sur pourquoi on lui demande des informations, et surtout qu'est-ce qu'il aura en retour ?

Cela s'inscrit dans le design de l'attention, davantage d'actualité aujourd'hui qu'il y a trois ans. En tant que designer, il faut toujours inventer et en même temps toujours protéger l'utilisateur.

Le RGPD ressemble d'abord à une contrainte. On a beaucoup travaillé pour en faire une opportunité, c'est-à-dire protéger l'utilisateur, en faisant attention à ce qu'on va mettre entre ses mains. Le risque est de faire des boites noires. L'enjeu n'est pas seulement de partager une partie de ces données mais de partager en toute connaissance de cause et de l'impliquer et de lui donner le choix.

Certains clients demandent à « avoir plus de données » pour vendre plus, ou pour mieux accompagner l'utilisateur au quotidien, pour le réassurer. Il faut donc travailler avec eux et aussi éviter les failles de sécurité dans la conception.

La MAIF ne produit pas d'objets connectés mais le développement de ces objets a un impact. Le métier d'assureur est aujourd'hui sur un pivot. Plus on récupère de la donnée plus on peut faire de la prévention. Il devrait y avoir de moins en moins de sinistres et moins de prime de risque.

Donc pour la MAIF il s'agit d'accompagner les gens à mieux gérer leurs objets.

Nous avons mis en place l'observatoire « mes data et moi ». La MAIF se positionne pour accompagner les usagers dans leur rapport à la donnée personnelle tout en mettant en place une éthique des données personnelles. Quand la question du big data est arrivée, on a fait du self data. Dans le cadre du self data on a fait le choix de ne pas aller vers les boites noires mais de restituer les données aux utilisateurs. Le droit à la portabilité permet de créer de nouveaux services ; Cozy cloud permet de croiser des données qui normalement ne se croiseraient pas.

On parle des objets connectés et le pic d'équipement arrive : il va y avoir de nouvelles applications à mettre en place. L'innovation n'est pas une problématique qui concerne le seul pôle numérique. C'est tout le propos de « la charte éthique pour un monde numérique plus humain » : elle signifie que par exemple, dans une offre habitat connecté, tous les services qu'on va agréger, et donc tous les partenaires de l'écosystème

respectent la charte. Les engagements d'investissement (SNIPS, cozy) ont vocation à déboucher vers de nouveaux services pour les sociétaires.

Y'A-T-IL UN MARCHE POUR L'IOT PRIVACY BY DESIGN ?

Il y a tout intérêt à faire attention lorsqu'on manipule des données médicales. On considère que c'est en étant transparent sur la manière dont on partage ces données, que l'on va attirer des clients (Kolibree).

Le privacy by design renforce la proposition de valeur initiale. L'assureur doit assurer le patrimoine numérique. (Maif)

Care OS essaie d'être LA plateforme en étant *designée* pour respecter la vie privée. Le défi va reposer sur la capacité d'imposer ce standard dans la salle de bain avant que Google ne le fasse.

On a également tous intérêt à ce que nos solutions soient intéropérables.

Il y aura de la place pour la privacy mais ça sera peut être comme le bio : pour ceux qui peuvent se le payer, ceux qui s'y intéressent.

COMMENT ASSOCIER/DISSOCIER LES UTILISATEURS DES OBJETS ?

Kolibree propose des opt in pour des programmes spécifiques comme des polices d'assurances. Le serveur identifie un paquet et sait qu'il doit l'envoyer directement dans la maison.

La meilleure façon de sensibiliser les utilisateurs est sans doute de leur poser la question de leur consentement, mais comment s'y prendre reste une question. Pour l'instant peu d'entreprises n'ont d'intérêt pour le privacy by design et donc elles ne sont pas fortement incitées à s'en soucier.

Les utilisateurs voient le service qu'on leur apporte. Ils aimeraient mieux contrôler et consentir « en pleine conscience ». En général, ils ne comprennent pas tout, et acceptent de partager leurs données parce qu'ils y sont obligés (ou le ressentent comme tel), pour avoir accès au service.

La question qui les inquiète le plus c'est l'espionnage par les pairs : le conjoint, les proches... peuvent en savoir un peu trop. Ainsi, s'il y a peu de gens qui s'impliquent dans les mouvements citoyens pour obtenir davantage de protection des données et de la privacy, il existe tout de même une question culturelle profonde de privacy. Comment transformer une angoisse en culture de protection de la privacy, et en demande sur le marché?

Les gens ont du mal à mettre des mots sur la peur qu'ils ont par rapport à l'usage de leurs données : une étude avec TNS a été menée. Il y a beaucoup de fantasme. Donc il faut beaucoup de pédagogie, et ne pas noyer les utilisateurs sous l'information. L'expérience utilisateur est très importante et la place du design va être clé.

Le stockage local des données a permis de prendre en compte une partie des préoccupations du grand public. Cet exemple montre qu'il faut

trouver les bons mots et parler simplement, quitte à simplifier.

L'une des questions qui rend la problématique complexe : est-ce que je sais avec mon smartphone de qui je suis l'usager ?

Avec cette première question on se rend compte qu'on sait très rarement à qui demander des comptes. Et est-ce que l'auteur de l'OS et de la machine prélèvent des données sans que je le sache ?

A l'inverse, est-ce les entreprises ayant des comportement vertueux et lisibles par rapport aux données personnelles en tireront une forte valorisation ?

Le design de l'attention fait des progrès vers l'éthique. La CNIL pourrait amener son label.

CONCLUSION

Le privacy by design n'est pas simplement une démarche éthique (« pour être gentil »), c'est aussi parce qu'on est prudent sur le coût de la protection des données, parce qu'on sent la monté de ces enjeux et de la notion de culture de la protection de la privacy au sein des organisations.

Ce qui vient de se dire doit encourager la CNIL et les pôles à publier les bonnes pratiques dans un endroit commun, avec des règles opposables pour favoriser leur adoption. Il y a quelque chose à faire de très stimulant pour l'innovation.

FABERNOVEL

Kolibree

MAIF
ASSUREUR MILITANT.

ween.ai
make objects autonomous

CES INNOVATION AWARDS 2018 HONOREE