DataRespect
Privacy As A Service

Présentation du Projet

Révision 14 Avril 2017

1 : Besoins soulevés par le problème

Les données, et notamment les **données personnelles des utilisateurs**, sont le **carburant de l'économie numérique**. Les données permettent de rendre des services plus innovants, plus pertinents et plus personnalisés. Ces données, comme toutes les matières premières, ont une valeur que tentent de convoiter les entreprises.
Les utilisateurs sont de plus en en plus informés sur **la valeur de leurs données**, 70 % d'entre eux[1] se disent même prêts à échanger leurs données personnelles contre de l'argent ou des bons de réductions.
Maîtriser, contrôler et certifier les données est donc indispensable pour les utilisateurs comme pour les entreprises, et a fortiori lorsqu'il s'agit de données personnelles (produites par un individu) ou nominatives (associées directement à un individu).
Cependant, les **utilisateurs sont réticents à partager leurs données** personnelles sans contrôle ni restriction, **92 %[2] d'entre eux se disent inquiets de potentielles fuites ou de mauvaises utilisations** de leurs données personnelles. Un frein majeur de l'adoption des objets connecté est le risque de la non-confidentialité des données personnelles : les acheteurs potentiels d'objets connectés se disent inquiets par l'usage qui sera fait des données personnelles collectées par ces objets, **42%[3] des usagers reportent leur achat d'objet connecté par crainte d'un mauvais usage de leurs données**.

La **confiance** entre les usagers et les fournisseurs de service est la clef d'une bonne relation commerciale. Pour respecter les attentes des utilisateurs, nous relevons 3 enjeux majeurs pour les entreprises :

- **Continuer à rendre des services** tout en respectant les choix des utilisateurs concernant la **confidentialité des données personnelles** ;
- **Permettre à l'utilisateur d'avoir une traçabilité sur l'usage de ses données** lorsque celui-ci souhaite les échanger contre de l'argent ou d'autres formes de rémunération (bons de réduction, avantages, etc.)
- **Empêcher le recoupement de données et la ré-identification de l'utilisateur** par des tiers, permettant, à partir de données simples, de déduire des informations personnelles, voire nominatives, potentiellement très sensibles : état de santé, solvabilité, tendances politiques, religion etc.

La confiance comme défi

L'enjeu pour les entreprises proposant des services ou des objets connectés est de **lever les réticences** des utilisateurs vis-à-vis de l'utilisation de leurs données personnelles. Amener plus d'utilisateur à partager plus de données se traduira pour les entreprises par :

- **L'augmentation du nombre d'utilisateurs**
- **L'augmentation du chiffre d'affaire**
- **Une meilleure personnalisation des services**
- L'amélioration globale des services
- La possibilité de soutenir de nouveaux modèles économiques

Un nouveau cadre réglementaire en Europe

Par ailleurs, le **cadre légal en Europe se renforce :** le Parlement européen a adopté le 14 avril 2016 un Règlement sur la protection des données **(GDPR).** Toutes les entreprises, même non Européennes manipulant les données de ressortissants Européens devront s'y conformer d'ici avril 2018[4].
Outre de d'apporter nouvelles exigences en terme d'organisation (Privacy by Design), de traitement, de contrôle, ou d'accès aux données par l'usager, le non-respect de ces dispositions peut conduire à

[1] Réf https://newsroom.intel.com/news-releases/intel-securitys-international-internet-of-things-smart-home-survey/
[2] Réf https://tresorit.com/blog/92-of-germans-concerned-about-their-data-security-welcome-new-eu-data-protection-laws/
[3] Réf Igniting Growth in Consumer Technology, 2016, Accenture
[4] Réf https://www.cnil.fr/fr/adoption-du-reglement-europeen-par-le-parlement-europeen-un-grand-pas-pour-la-protection-des-donnees

une pénalisation des contrevenants jusqu'à **4 % du chiffre d'affaires mondial de l'entreprise ou 20 millions d'euros** (maximum des deux). De plus, ce règlement institutionnalise des actions de classes qui elles ne sont pas plafonnées.

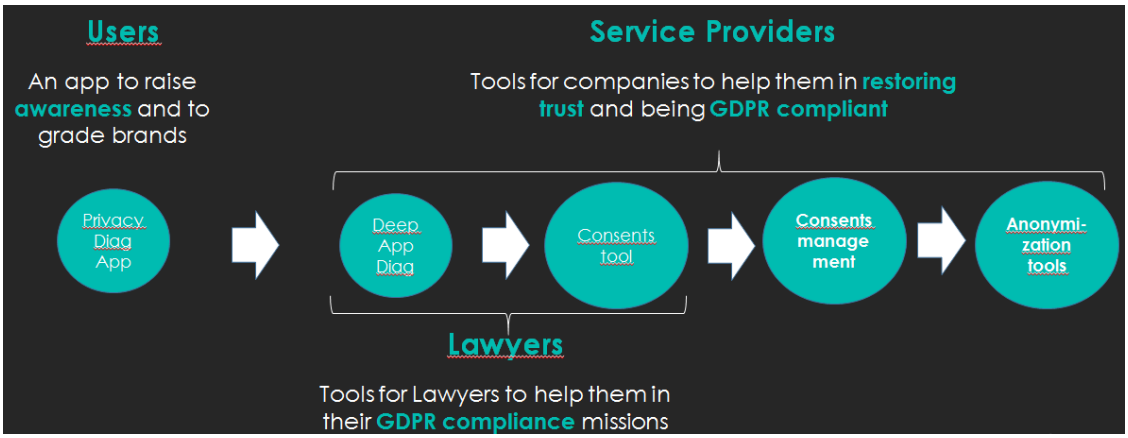
DataRespect, le tiers de confiance des données personnelles

Parce que **la confiance de l'utilisateur est au cœur de l'enjeu**, **DataRespect** offre aux entreprises une solution pour développer des services (cloud ou mobile) garantissant à l'utilisateur un **contrôle total sur ses données personnelles et sur l'usage** qui en est fait.

DataRespect est une solution de « **Privacy as a Service** » permettant de mettre en place facilement des politiques de gestion des données personnelles. **DataRespect** est une plateforme d'intermédiation entre l'environnement de l'utilisateur (smartphone, objets connectés, maison connectée, voiture, etc.) et les fournisseurs de services. Les différents outils de **DataRespect** permettent la mise en place tous les moyens nécessaires pour respecter les choix de l'utilisateur en matière de **protection de son identité**, de **précision de l'information** transmise et de la **traçabilité de ses données.**

Une gamme de produits

Nous avons développé un ensemble de produits permettant de répondre aux différentes attentes des entreprises et des usagers.



- Une application grand public gratuite permettant à l'usager de découvrir quelles données sont collectées par chacune des Apps de son smartphone, et surtout lui permettant de noter son niveau de confiance pour chacune de ses Apps.
- Pour les entreprises des outils de diagnostiques profonds des applications mobiles ou des objets connectés afin de valider que l'application ne communique pas avec d'autres serveurs que ceux décrits dans les Conditions Générales de l'usager. Ces diagnostiques nous permettent d'attribuer des labels éthiques aux applications testées et respectueuses.
- Un outil de gestion des consentements des usagers qui va archiver d'une manière opposable la signature du contrat régissant l'usage des données de l'usager par l'entreprise (via blockchain).
- Un outil de modélisation et d'anonymisation des données à la volée permettant à l'entreprise de ne travailler que sur des données anonymisées.

2 : Cartographie des acteurs présents

Une solution innovante et unique

Les exigences imposées par la GDPR ont considérablement activé ce marché. Toutefois, **DataRespect** a un caractère unique à plusieurs titres :

- C'est le premier gestionnaire de consentements authentifié par blockchain
- C'est une solution unique de traitement de données de flux permettant d'assurer le niveau de confidentialité souhaité par l'utilisateur, propriétaire de ses données.

Nous avons identifié plusieurs concurrents internationaux et deux français positionnés de manière très marquée sur le sujet de la confidentialité des données personnelles des utilisateurs :

Compétiteur	Date de création	Size	Offre	Forces et faiblesses
TRUSTe	1997	150+	Approche Holistique; Analyse consulting, certification ; Spécialiste de la gestion de cookies Web	Positionné sur la chaine complète de décision de l'analyse à l'intégration technologique
FORGEROCK	2010	150+	Fournit une plateforme complète pour développer des services spécialisés basés sur de l'identity management	Possède des clients captifs pour l'identity management, Forgerock peut légitimement proposer étendre ses solutions vers la privacy. Néanmoins, l'identité signifie « qui vous êtes », l'anonymisation est le contraire.
Cozy Cloud	2012	10, levée €5M	Crée un cloud personnel pour chacun	Des premiers clients, mais avec un modèle très différent des SI des entreprises actuelles et fragile en terme de QoS
NEURA	2013	20	Propose des services personnalisés aux usagers, basés sur la confiance	Afin d'assurer la confidentialité, Neura propose des blocks préfabriqués pour créer des services intelligents : Reconnaissance de comportement, gestion du temps
PrivacyCheq	2013	20	Privacycheq crée de la confiance en synchronisant les exigences des utilisateurs d'IOT avec les entreprises	En grande partie déclarative, assez simple à mettre en œuvre pour les entreprises mais ne peut assurer le "Privacy by design".
MatchUpBox	2014	20, levée €400k	Protection des données personnelles	POC réalisé pour une assurance, fragilité financière, en cours de pivot
OneTrust	2016	82 en 18mois	OneTrust automatise la réalisation des PIA et réalise un mapping des données sensibles des différentes bases de l'entreprise	Onetrust s'est construit par rachat d'entreprises en particulier Optanon
BigID	2016	5, levée $2,6M	Aide les entreprises à protéger d'identité des usagers ; Scanne toutes les bases de données pour localiser les données sensibles	Entreprise récente premiers POCs vendus
Privacy Labs	2016	5, levée $4M	Protège la confidentialité des donnée personnelles	Très peu d'information disponible. Pas encore de produit ni de clients

La plupart de ces concurrents traitent des données « à plat », c'est-à-dire des données issues de fichiers situés dans des bases de données, et pas de gestion des consentements.

3 : Présentation de l'équipe

Philippe MICHEL – Président

50 ans, serial entrepreneur, 25 ans d'expériences dans le domaine de l'IT et des objets connectés Management, business development.

Ingénieur électronique de formation, il a débuté ses travaux sur l'interopérabilité et la maison connectée dès 1999. Il a créé en 2001 Digital Home Concept une entreprise qui a conçu et déployé des solutions de domotique IP (précurseur de ce qui est aujourd'hui appelé objets connectés). Digital Home Concept a créé le logiciel ExDomus lancé par Microsoft et dans tous ses Média-centers. Digital Home Concept a fait la R&D de Legrand, Schneider, EDF, et a commercialisé ses solutions en Europe.
Il a vendu en 2007 la société au groupe Hager, et l'équipe de Digital Home Concept est devenue le laboratoire de recherche logiciel de Hager.
Depuis 2009, il intervient comme consultant pour de grandes entreprises (Leroy Merlin, Syntec Numérique …) pour ajouter des services digitaux à la ville ou à la maison. Spécialiste de l'innovation et de l'IOT, membre de la LoRa alliance, il intervient dans de nombreux congrès et accompagne de nombreuses entreprises innovantes.

Richard THIBERT – Directeur Technique services en ligne

48 ans, entrepreneur, 20 ans dans le développement logiciel de bases de données, spécialiste de systèmes de sécurité bancaires.

En 1984 Richard réalise à 16 ans le premier éditeur assembleur wysiwyg pour Apple II, édité par Version Soft, au catalogue d'Apple France. Parallèlement à ses études il devient le plus jeune développeur Macintosh enregistré par Apple France. Ingénieur en électronique, diplômé de ESSEC et docteur en informatique de l'Université d'Orsay il rejoint KPMG pour mener des projets système d'information pour de grandes entreprises. Puis il rejoint le groupe Banque Populaire pour participer à la transformation numérique des processus et créé en 1999 une entreprise offrant des services en mode SAAS pour les Banques et les Assurances en assurance la sécurité et la confidentialité des données manipulées.

Benjamin BERTRAN – Directeur Technique services mobiles et objets / Export USA

33 ans, 10 ans de développement logiciel en centre de recherche, spécialiste de l'IOT, développement logiciel et data management.

Diplômé Ingénieur en informatique en 2006, Benjamin a commencé à travailler pour Digital Home Concept pour contribuer au développement de l'IHM logicielle d'Ex-Domus. De 2008 à 2011, il a dirigé le développement du projet de recherche DiaSuite à l'INRIA Bordeaux. Ce projet visait à créer une plate-forme IOT complète couvrant l'interopérabilité des protocoles, l'agrégation des données, la conception des services et l'exécution des applications. De 2012 à 2015, il a conseillé des laboratoires de recherche, des PME et des grandes entreprises pour construire des projets de R & D en dirigeant Elopsys (cluster en électronique et technologies numériques).

4 : Le marché et notre solution

Big Data et monétisation des données

Le **Big Data** permet d'extraire des informations extrêmement riches à partir des données simples et très nombreuses. Selon IDC[5], les dépenses annuelles des entreprises liées au Big Data devraient approcher les **$50 milliards d'ici 2019**. La valorisation de ces données et leur monétisation sont des enjeux économiques majeurs pour les entreprises. Plus les utilisateurs seront enclins à partager leurs données, pour bénéficier des services plus qualitatifs ou en échange d'argent ou d'autres récompenses (bons de réduction, etc.), plus les informations déduites seront précises et augmenteront en valeur.

IoT / objets connectés

Le marché des objets connectés est estimé à plus de **7000 milliards de dollars d'ici 2020**[6]. Cependant, selon différentes études[7], entre 20% et 30 % des acheteurs potentiels voient les problématiques de l'utilisation légale des données personnelles comme un frein à leur adoption massive (42%[8] des usagers n'ont pas acquis ou ont cessés d'utiliser des produits connectés par manque de confiance sur l'usage de leurs données). La protection des données personnelles représente donc **un enjeu commercial pour le monde de l'IoT de plusieurs centaines de milliards de dollars**.

Un marché naissant mais essentiel aux services numériques

La confidentialité est un des trois défis du web, selon son inventeur[9]
Deux éléments essentiels animent notre marché :

- La prise de conscience des usagers sur l'importance de maintenir la confidentialité de leurs données personnelles
- La pression dans les entreprises pour une mise en place rapide de la GDPR

Ce marché est anxiogène, à la fois pour les entreprises et les usagers. Nos éléments de langage sont donc les suivants :

Confiance de l'usager pour la marque (la base du commerce)

Bienveillance de l'entreprise pour son client et de DataRespect pour l'entreprise (beaucoup plus porteur de valeur qu'une transparence qui reste passive)

Acceptabilité de la solution par l'usager (capacité de l'usager à donner son/ses **Consentements**)

Anonymisation (permet de rendre un service sur des données « détachées » de l'identité de l'usager)

Stratégie produits

Une prise de conscience de plus en plus vive

Les usagers sont de plus en plus au courant de l'usage intensif de leurs données. Seulement 37% sont confiant dans l'usage d'internet (-3% en 2016)[10].
Nous devons accompagner la prise de conscience des usagers et leur permettre de distinguer les applications éthiques des autres.

DataRespect grand Public est une application gratuite permettant à l'usager de découvrir quelles données sont collectées par chaque application présente sur son Smartphone. Organisée comme un jeu lui permettant d'améliorer son score, elle apprend à l'usager à se protéger des pilleurs de

[5] IDC, oct. 2015, http://www.cio.com/article/3004512/big-data/idc-predicts-big-data-spending-to-reach-48-6-billion-in-2019.html
[6] IDC, The Internet of Things Moves Beyong the Buzz, 2014
[7] Markess, Top 10 des freins liés au marché des objets connectés, 2015
[8] Igniting Growth in Consumer Technology, 2016, Accenture
[9] http://webfoundation.org/2017/03/web-turns-28-letter/
[10] http://www.caissedesdepots.fr/sites/default/files/medias/barometre_de_la_confiance_des_francais_dans_le_numerique_0.pdf

données et à distinguer les bons des mauvais. Un bouton « Faites-moi peur » permet de prendre conscience de la quantité d'application qui peut enregistrer images, son, sms, contacts sans le demander à l'usager.

En retour, la **notation de confiance** que l'usager donne à chacune de ses apps nous fournit un moyen de pression sur les marques.
Nous avons intégré dans cette application une notion de **label** que DataRespect peut fournir aux applications respectueuses.

Des données pas nécessairement bien maitrisées

Nous avons aussi constaté que fréquemment, les applications pour Smartphone développées par les entreprises ou leur prestataire avaient des **« fuites de données ».** Ceci est principalement dut à la multiplication des services en SaaS utilisés par les développeurs qui se connectent à des serveurs autres que ceux de l'entreprise. Chaque service et chaque librairie logicielle utilisé acquiert les même droits que l'application, et par exemple un simple fournisseur de police de caractère a la possibilité d'avoir accès (malhonnêtement bien sûr) au micro du smartphone, si celui-ci est autorisé pour l'app.

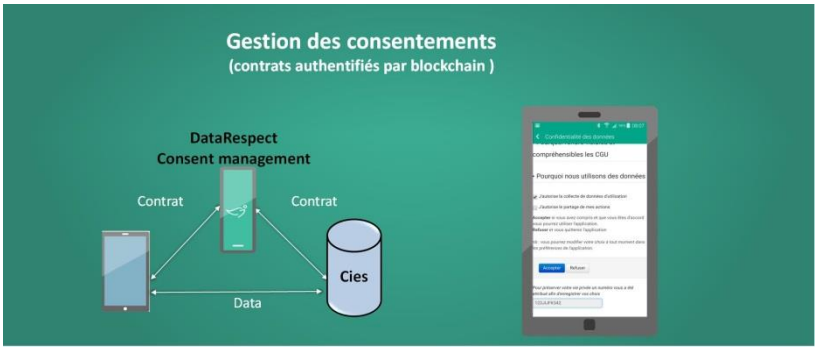
PrivacyDiag
Privacy As A Service

Nous avons donc créé un **outil de diagnostic profond « Privacy Diag »** basé sur un **banc de test**, pour les apps et les objets connectés afin de relever toutes les traces IP qui en sont issues. Ces traces et leur destination sont analysées, si elles ne sont pas cryptées, des patterns sont relevés. Ceci nous permet de délivrer un rapport à l'entreprise lui permettant d'avoir un premier aperçu de situation.
Ce premier produit nous permet d'avoir un premier contact avec l'entreprise, avec un produit à bas prix peu engageant, mais riche pour nous sur l'environnement IT du futur client SaaS.
Il nous permet aussi de fournir le **label de confiance** présent dans l'application grand public.

Gérer les consentements des usagers

La première chose à faire pour respecter les données de l'usager, est de l'informer sur ce qui est fait de ses données, et de lui demander son accord. Ses **consentements** doivent selon la règlementation être **éclairés,** c'est-à-dire pris en pleine connaissance de cause. Quand ces consentements sont perdus au milieu de cinq ou six pages de conditions générales ils ne sont pas lus.
D'autre part, l'entreprise n'a aujourd'hui quasiment aucun moyen, plusieurs années plus tard, de prouver que l'usager a bien donné ses consentements.
Notre offre **« Consent manager »** permet de simplifier pour l'entreprise tous les échanges avec l'usager concernant la confidentialité de ses données et permet **d'authentifier**, de **dater** et de **rendre opposable** toute signature d'accord relative à ces données.

Un contrat est établi entre l'usager et l'entreprise, et ce contrat est signé par une blockchain privée.



Des outils simples pour les développeurs (librairie + API) permettent de mettre en place rapidement une solution efficace de gestion des consentements.
D'autres fonctionnalités sont ajoutées à cet outil :

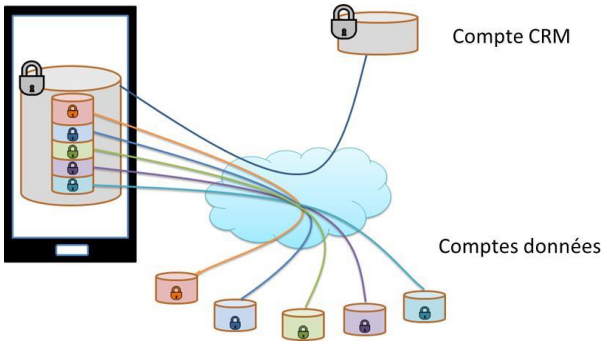
- Séparation CGU / données utilisées et visualisation graphique (pour faciliter le consentement éclairé de l'usager)
- Possibilité d'intégration des fonctions de demande de droit à l'oubli et de portabilité dans le formulaire de consentement
- Possibilité de signature de contrat pseudonymisé afin de garantir un pseudo-anonymat de l'usager qui installe une application
- Gestion des durées de conservation des données

Permettre un usage anonyme des services

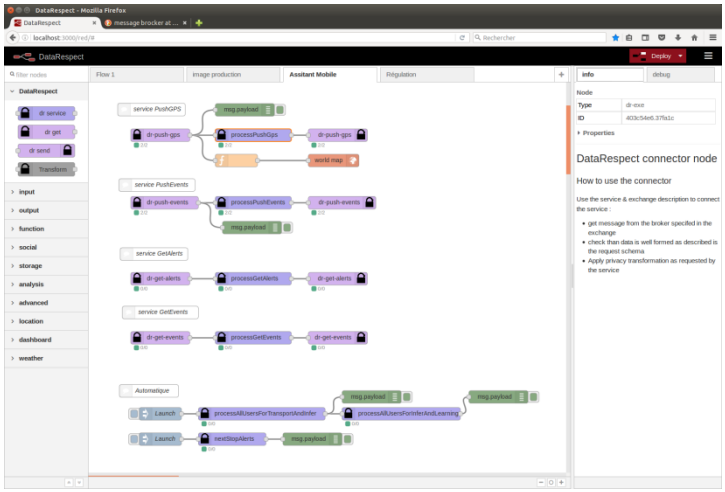
L'outil le plus sophistiqué que nous avons développé est un outil de modélisation et d'anonymisation des flux de données. Si le modèle de l'entreprise est adapté, il permet de fournir le service en ne manipulant que des données anonymes ne permettant pas une ré-identification de l'usager, ce qui permet à l'entreprise de **sortir intégralement du champs d'application de la GDPR**.

Des données correctement anonymisées ne relèvent plus du champ d'application de la réglementation sur la protection des données

Notre outil sépare le compte client CRM de l'usager du (des comptes données) afin d'éviter tout lien entre les données « utiles » permettant de rendre le service et les données identifiantes.



Les données de l'usager sont cryptées et lui seul peut les relier à son compte identifiant.
Nous fournissons un tableau de bord de gestion permettant facilement de modéliser les trafics de données et fournissant des outils d'anonymisation et de floutage des données usagers.



Les données transitent par nos serveurs qui anonymisent ou floutent la donnée comme le fait partiellement un proxi. Pour rester compatible avec les systèmes d'information existants dans les entreprises, nos interfaces d'entrée et de sortie sont sous la forme d'API standard. Les technologies utilisées sont NodeJS, MongoDB, et NodeRed.

Concrètement, **DataRespect permet de garantir la maîtrise des données personnelles par construction** (correspondant au Privacy by Design). Cela signifie que les données nécessaires pour rendre un service seront maîtrisées de bout-en-bout, des objets connectés ou smartphones jusqu'aux services, tout en respectant les choix de l'utilisateur en matière de filtrage, de floutage et d'anonymisation de ses données.

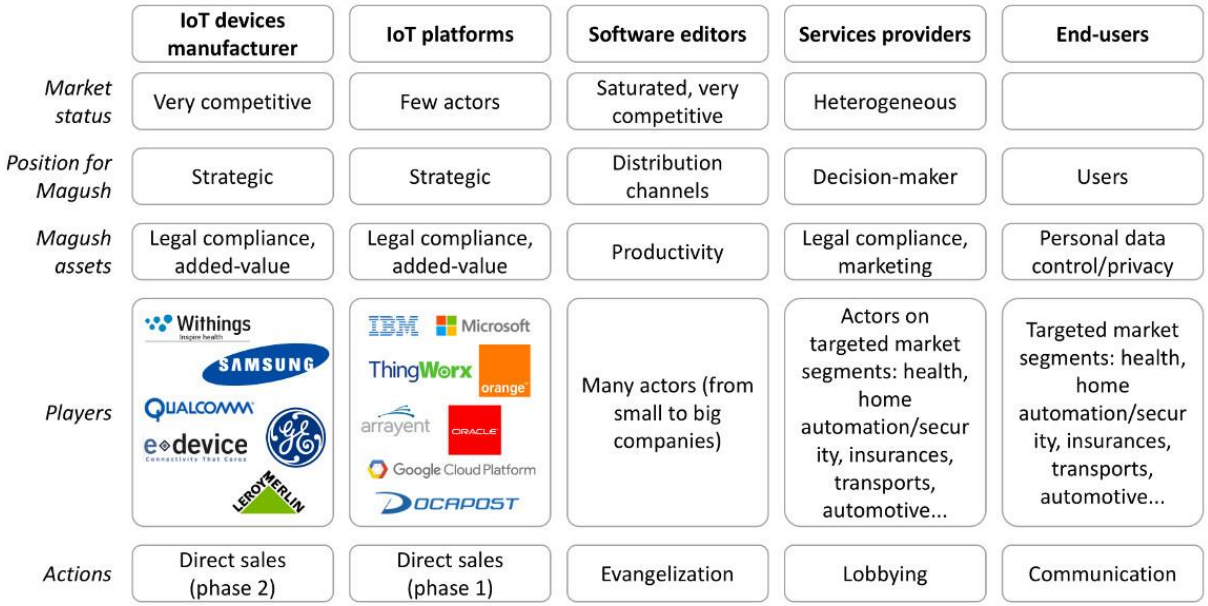
Les services de DataRespect peuvent être hébergés sur nos serveurs ou en frontal des serveurs de l'entreprise.

Structuration des acteurs

Notre positionnement se situe à l'intersection de la cyber-sécurité, du Big Data, des objets connectés, et de la monétisation des données. On peut décomposer la chaîne de valeur par typologie d'acteurs comme suit :

- Les fabricants de puces pour objets connectés
- Les fabricants d'objets connectés
- Les opérateurs/agrégateurs de données et les plateformes d'IoT
- Les éditeurs logiciels et intégrateurs développant les services pour le compte de donneurs d'ordres (les fournisseurs de services)
- Les fournisseurs de services
- Les utilisateurs finaux

Ci-dessous, les acteurs du domaine positionnés dans la chaine de valeur, des objets aux utilisateurs finaux.



Quelques marchés applicatifs/verticaux

Nous avons identifié des marchés verticaux qui sont en train de se développer et/ou de se réinventer grâce au Big Data et aux objets connectés. Dans ces marchés, la confidentialité des données personnelles prend d'autant plus de sens que les données collectées ou leur interprétation sont sensibles. Au travers d'actions de prospection, de lobbying et de sensibilisation, nous ciblerons notamment les marchés de la grande distribution, de la santé, de la maison connectée, des assurances et des transports.

Stratégie commerciale

Nos objectifs sont de cibler en priorité **:**

- les porteurs d'application grand public manipulant potentiellement des données sensibles ou fortement exposés à la GDPR (grande distribution, banque/asssurance, …)
- les agrégateurs de données/de services et les plateformes d'IoT : Orange/Docapost/OverKiz en France, Arrayent/PTC/AVNET aux USA et STREAM au UK.
- Les fabricants d'objets connectés associés à une application mobile (voiture connectée, domotique, Wearable…)

L'objectif est d'acquérir au plus vite une position de leader sur ce segment en nous positionnant comme tiers de confiance indépendant.
L'approche internationale est nécessaire afin d'éviter de voir apparaitre un leader dans deux ans qui préempte le marché. La réglementation Européenne est la même sur toute l'Europe en particulier en Allemagne où la sensibilité à la vie privée est forte, ainsi qu'aux USA fournisseur de services pour l'Europe, nécessitant une stratégie spécifique.

Forces de Porter du segment

Pouvoir de négociation des clients :

Les clients ont une marge de négociation faible. La seule possibilité pour eux serait d'effectuer ce développement en interne, et la barrière à l'entrée est assez importante (expertise, structuration…). La preuve des consentements doit être fournie par un tiers.

Pouvoir de négociation des fournisseurs :

Les fournisseurs des services de privatisation sont dans une situation assez forte vis-à-vis des entreprises qui sont de plus en plus contraintes (par le marché et l'évolution des règlementations) de mettre en place des solutions destinées à protéger la confidentialité des données personnelles.

Menace des produits ou services de substitution :

Une alternative pour les entreprises est d'étendre les termes des Conditions Générales de fourniture de Service qui représente un fort investissement juridique, potentiellement négatif au niveau marketing, et potentiellement non conforme (consentement éclairé).

Menace d'entrants potentiels sur le marché :

Les acteurs historiques de la sécurité peuvent entrer sur le segment de la confidentialité des données personnelles. Leur plus grand marché est pour l'instant le Web et très peu ont adressé le marché des applications mobiles, les objets connectés et plus généralement les données de flux.

Intensité de la rivalité entre les concurrents :

Peu de concurrence directe aujourd'hui car le marché est en train de se mettre en place. Mais le marché bouge rapidement (des nouveaux acteurs apparaissent en particulier aux USA). Les acteurs historiques de la sécurité et de l'authentification sont en train de travailler sur des nouvelles offres.

5 : Positionnement face à la concurrence

Notre positionnement est différent de nos concurrents car nous sommes centrés sur la gestion des consentements, et des données mobiles qui remontent en **flux**. De plus, nous fournissons un cadre de structuration des paramètres de confidentialité des données qui permet à l'entreprise le respect d'une organisation « Privacy by Design » donc conforme à la nouvelle réglementation.

6 : SWOT

Forces	Faiblesses
Equipe expérimentée Déjà des clients et études grands comptes Premier arrivant sur la niche	Taille critique pour traiter avec des grands groupes Couverture Internationale

Opportunités	Risques
Time to market Nouvelle réglementation européenne 2018 Solution smart-contract consentements blockchain bankable	Etre sorti du marché par un gros acteur Ne pas avoir assez de moyens financier pour se développer rapidement

7 : Retours Clients/Utilisateurs

A ce jour, un contrat a été signé avec la RATP pour la réalisation d'un premier POC livré en octobre 2016. D'autres devis avec des grands comptes (dont des grands opérateurs) sont en cours de négociation. L'intérêt porté à notre solution est marqué par chacun de nos prospects, et les différents salons que nous avons effectué aux USA (Santa Clara, Boston) ou en Europe (Dublin, Munich) ont été de francs succès. Les salons aux USA nous ont permis de valider l'appétence du marché américain pour notre solution.

La CNIL a aussi marqué son intérêt et peut être pour nous un grand vecteur de promotion, tout comme le PICOM (Pôle de compétitivité des industries du commerce rassemble les principaux acteurs français des domaines de la distribution, du commerce électronique et de la relation client).

Partenariats stratégiques

RATP, une référence dans le transport

Avec la RATP, nous avons établi un premier contrat de collaboration afin de développer et d'expérimenter des services hyper-personnalisés, nécessitant de collecter des données personnelles, tout en respectant le choix des utilisateurs en matière de partage de données et garantissant « by Design » un contrôle de ces données personnelles.

Implication dans la Chaire Identité Numérique

La Chaire « Valeurs et Politiques des Informations Personnelles » portée par l'Institut Mines Telecom et coordonnée par Claire Levallois-Barth. Cette chaire adresse de manière très large les problématiques des informations personnelles dans la société numérique, que ce soit sur des aspects juridiques, sociétaux, technologiques ou philosophiques.

Accélérateur Scale d'Euratechnologies à Lille et Village by CA

Nous avons été sélectionnés par l'accélérateurs SCALE d'Euratechnologies ainsi que par le Village by CA, qui nous accompagnent dans notre croissance et nous fournit un coaching de grande qualité. L'environnement du Campus d'Euratechnologies nous permet de côtoyer l'ensemble de l'écosystème digital et d'être mis en relation avec les partenaires de ces institutions.