Santé Connectée, Big Data et Internet des Objets dans le contexte des crises émergentes.

- enjeux de la santé connectée
- sécurité des données
- exploitation des données
- impact des technologies 3.0 sur l'environnement

Nicelab, Laboratoire Ouvert de Nice, Hackerspace, depuis 2011

Jean-Noël Montagné | Hackerspace de Nice | Nicelab.eu | 25 nov 2017

- enjeux de la santé connectée

Enjeux de santé publique

contre

Enjeux commerciaux

Équipements embarqués, équipements implantés, équipements du domicile, de l'espace public ou du centre de soin, applications pour smartphones, assistants personnels, robots d'assistance ou de soin, etc...

LE MARCHÉ DE L'E-SANTÉ ATTEINDRA 400 MILLIARDS DE DOLLARS EN 2022

Arthur L 27 mai 2016 Business, E-Santé Ecrire un commentaire

Pourquoi et comment les géants pharmaceutiques accélèrent dans le big data

Par **Jean-Yves Paillé** | 07/02/2016, 10:30 | 1158 mots

Santé connectée : « Sanofi est à l'avant-garde de cette révolution »

Par **Propos recueillis par Florence Pinaud** | 21/04/2015, 14:50 | 485 mots

Sanofi et Google envisagent *"des méthodes plus proactives et efficaces de contrôle du diabète"*

Cette alliance va associer le savoir-faire du laboratoire pharmaceutique français, dans le domaine des traitements et des dispositifs médicaux dans le diabète, à l'expertise du géant d'Internet en matière d'analyse de données, d'électronique miniaturisée et de puces de faible puissance. Andy Conrad, le

Après Novartis et Sanofi, Verily Life Science (Google) se rapproche de GSK

CHARLES FOUCAULT | SANTÉ, ALPHABET, INNOVATION |
PUBLIÉ LE 01 AOÛT 2016 À 16H38

Internet en vogue chez les enfants. Quatre-vingt-quatre pour cent de ces publicités faisaient la promotion de produits riches en graisses, sucre et/ou sel alors même que les industries alimentaires considéraient que les trois quarts de ces publicités correspondaient à des choix alimentaires sains pouvant faire l'objet de publicité en direction des enfants (Ustjanauskas, Harris et al. 2013).

Santé publique France

M Économie

ÉCONOMIE | Les données du « Monde » | Économie mondiale | Économie française

Les chiffres clés du diabète, un gigantesque marché pour les laboratoires

Conséquence de la pandémie d'obésité, 425 millions d'adultes sont diabétiques. Problème de santé publique, cette maladie

M Économie

ÉCONOMIE | Les données du « Monde » | Économie mondiale | Économie française

ÉDITION ABONNÉS

Diabète : la santé KO face aux lobbys

Publicité, campagne d'influence… Les laboratoires pharmaceutiques et l'industrie agroalimentaire frappent très fort. La prévention, elle, dispose de peu de moyens

- sécurité des données et vie privée

Sondage .....

- Aimeriez-vous que votre docteur accède à votre dossier de santé ?
- Aimeriez-vous que votre pharmacien accède à votre dossier de santé ?
- Aimeriez-vous que votre famille accède à votre dossier de santé ?
- Aimeriez-vous que votre assureur accède à votre dossier de santé ?
- Aimeriez-vous que votre banquier accède à votre dossier de santé ?
- Aimeriez-vous que votre employeur accède à votre dossier de santé ?
- Aimeriez-vous que votre voisin accède à votre dossier de santé ?
- Aimeriez-vous que votre supermarché en ligne accède à votre dossier de santé ?
- Aimeriez-vous que votre opérateur (téléphonie/ réseau) accède à votre dossier de santé ?
- Aimeriez-vous que votre réseau social accède à votre dossier de santé ?
- Aimeriez-vous que les GAFAMSS accèdent à votre dossier de santé ?
- Aimeriez-vous que n'importe qui accède à votre dossier de santé ?

du point de vue de la sécurité et de la vie privée, on distingue:

- Les équipements connectés dont les données sont analysées, utilisées et/ou stockées *in situ* => *sécurité maximale*

- Les équipements connectés dont les données sont transmises pour être analysées et stockées *à l'extérieur du domicile ou du centre de soin.* => *aucune sécurité*

Les failles de sécurité existent dans tout maillon de la chaine

Génération des données, émission des données, transferts, stockage, analyse, consultation ....

Aucune sécurité des données n'est assurée à 100%

Aucun anonymat n'est assuré à 100%

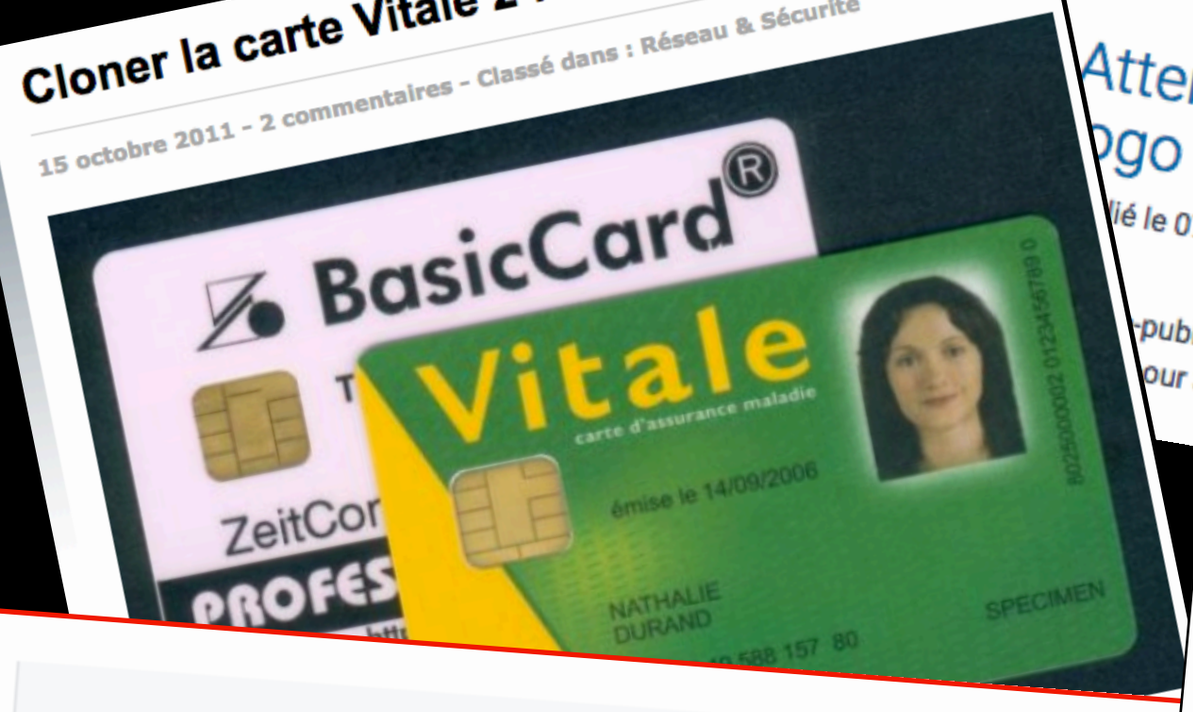
Tous ceux qui récoltent des données les valorisent

Boulogne: l'hôpital Duchenne victime d'un chantage informatique: 10 000 dossiers infectés

À trois reprises au cours des dernières semaines, le centre hospitalier a été victime d'un chantage à l'informatique. La direction de l'hôpital se veut rassurante : Non, il n'y a pas de

Cloner la carte Vitale 2 : un jeu d'enfant ?

15 octobre 2011 – 2 commentaires – Classé dans : Réseau & Sécurité



Un demi-million de pacemakers vulnérables

par Guillaume Périssat, le 01 septembre 2017 14:42

465 000 pacemakers sont concernés par des vulnérabilités dans leur firmware, prévient l'administration américaine. En janvier, c'est le transmetteur faisant le lien entre le pacemaker et le médecin qui révélait des failles.

La santé connectée doit simplifier la circulation d'informations entre soignant et soigné. Et éventuellement mettre la vie de ce dernier en danger. Mardi, la Food and Drug Administration (FDA) américaine **a révélé que** 465 000 pacemakers de la société Abbot (anciennement St Jude Medical) étaient affligés de failles de sécurité. En cause : le firmware de ces appareils permettant de réguler le rythme cardiaque d'un patient. Six modèles de pacemakers sont concernés.

Les vulnérabilités pouvaient potentiellement être exploitées par des tiers afin d'accéder au pacemaker et d'en modifier la programmation, en résultant « *l'épuisement prématuré de la batterie ou l'administration d'une stimulation* [cardiaque] *inappropriée* » pouvant causer du tort (potentiellement fatal) au porteur. La FDA précise néanmoins ne connaître aucun accès illicite auxdits pacemakers.

Des failles partout

Depuis, Abbot a mis au point un patch correctif du firmware de sorte que seuls des appareils autorisés puissent avoir accès aux pacemakers. Par exemple, le

EN BREF Hameçonnage (

Attention aux courriels frauduleux sur la carte Vitale V3 a

ogo de Service-public.fr

lié le 07 novembre 2017 - Direction de l'information légale et administrative (Premier ministre)

Mutuelle Générale de la Police

Les données de santé de 112 000 policiers piratées

par la rédaction

Les données de santé de 112 000 policiers et leurs proches ont fuité sur Internet. Un acte malveillant est à l'origine de cette fuite.

LIRE AUSSI : Des hôpitaux britanniques paralysés plusieurs jours par un virus informatique

Des cas similaires dans le monde entier

« Cela ne vise pas le NHS, c'est une attaque internationale et
plusieurs pays et organi

#CYBERSÉCURITÉ

Hôpitaux : la cible idéale des hackers

Des pirates dérobent les données de 1,3 million de clients Orange

Par Le figaro.fr | Mis à jour le 07/05/2014 à 16:13 / Publié le 06/05/2014 à 19:40

32 millions de comptes Twitter piratés

par Guillaume Périssat, le 09 juin 2016 14:58

La série noire des bases de données d'utilisateurs de réseaux sociaux mis vente se poursuit. C'est désormais au tour de Twitter. Néanmoins, le gazo ne semble pas avoir été piraté : les hackers se seraient directement servis les machines des utilisateurs.

Le piratage de Yahoo! en 2013 a finalement touché ses 3 milliards de comptes

Par Le figaro.fr | Publié le 04/10/2017 à 11:19

Equifax: les données de 143 millions d'Américains piratées

Alexis Buisson, à New York , le 17/09/2017 à 17h22

La société Equifax, qui réalise des évaluations de crédit, vient
l'objet d'un énorme piratage informatique.
Les données perso

plus de 25 terabytes de données sensibles (adresse, orientation politique...)

concernant 198 millions de citoyens américains étaient accessibles sur un serveur e
ligne non sécurisé. En cause : une société d'analyse de données recrutée par le Pa
pendant la campagne pour mieux cibler les électeurs
Trump.

Derniers articles | Archives | Recherche

Dropbox s'est bien fait dérober 68 millions de mots de passe

Faits divers | Uber | piratage informatique

Uber : les données de 57 millions d'utilisateurs piratées

> Faits divers | R. Bx avec AFP | 22 novembre 2017, 0h11 | 8

teurs américains
aucune protection, libres
découvrai

Jean-Noé Landry | Nicelab.eu | 25 nov. 2017

BlueBorne : des failles dans le protocole Bluetooth menacent des milliards d'appareils

par La rédaction, le 14 septembre 2017 16:13 ★★★★☆

Spécialiste de la sécurité de l'Internet des Objets, Armis explique qu'elle a découvert pas moins de huit failles zero-day, dont quatre sont classées comme critiques, dans le protocole Bluetooth mettant en danger de nombreux OS comme Linux, Windows, iOS ou Android.

Les failles détectées et répertoriées par Armis, une start-up experte en sécurité IoT basée à Palo Alto (Californie), sont décrites sous le nom de « BlueBorne » ; « Blue » en référence au Bluetooth, « Borne » en référence à « airborne » dans le sens où elles peuvent être exploitées « par les airs » pour attaquer des périphériques.

Santé connectée : "La protection des données est insuffisante"

Par Elena Sender le 21.02.2016 à 19h00, mis à jour le 21.02.2016 à 19h00

Sciences et Avenir a posé 3 questions sur la protection des données de santé rassemblées par les objets connectés à Delia Rahallofskog, chef du service de la santé à la direction conformité de la CNIL.

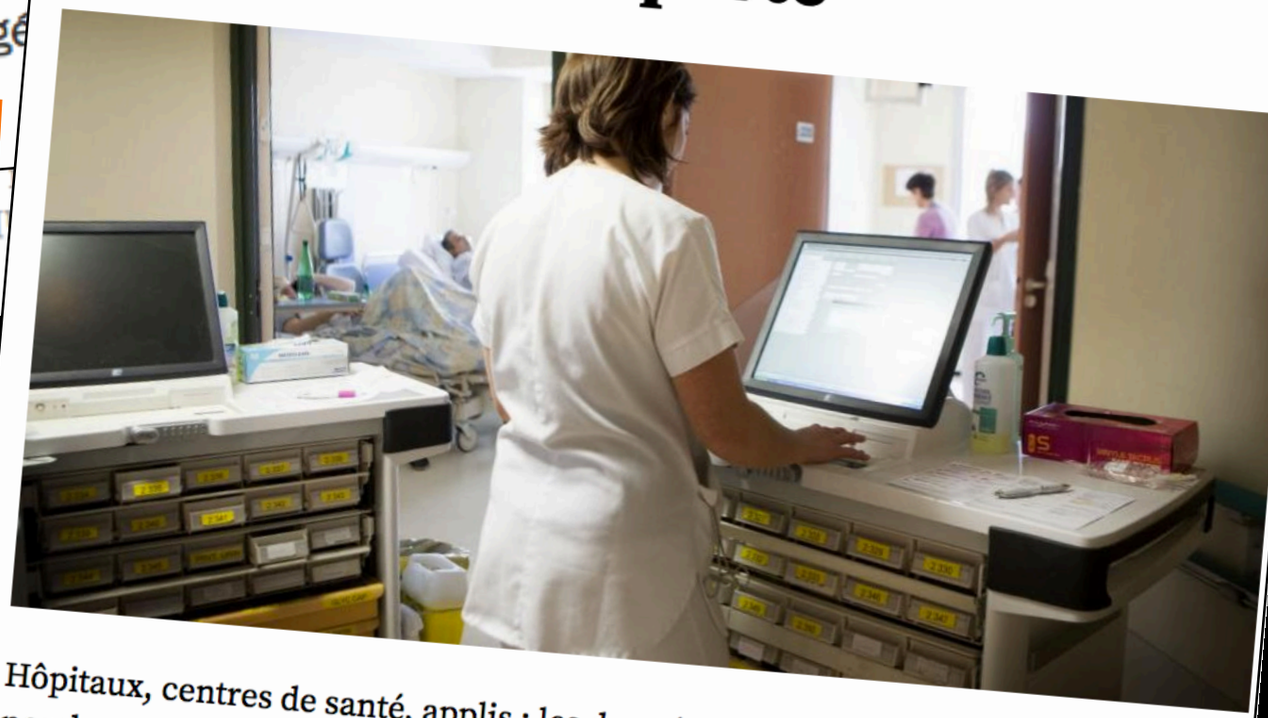
Les données de santé attirent les hackers

Mais pour être pleinement utilisables par les médecins, les données enregistrées doivent impérativement être partagées. Sauf qu'il s'agit là de données souvent sensibles. Qui y aura accès ? Qui pourra les utiliser ? Comment garantir la confidentialité ? Laure de La Raudière, député Les Républ[illegible]ure-et-Loir, et très engagée sur les questions du numérique, met les pieds d[illegible] chose que je demande, c'est que ces données soient tra[illegible] sur le sol français. Aujourd'hui, quand vous a[illegible] pas où elles sont héberg[illegible]

'Sur le darkweb, l'underground d'internet, le dossier médical a une valeur, sa cotation de la semaine est aux alentours de 17$. Si vous êtes à la tête d'une base de données que vous avez subtilisée à un établissement d'une centaine de milliers de dossier médicaux, vous avez potentiellement entre 2 et 3 millions de dollars.'

L'Obs > Rue89 > Internet

Piratage de données médicales : la France n'est pas prête



Hôpitaux, centres de santé, applis : les données médicales sont de plus en plus nombreuses et convoitées. Leur piratage se répand, mais la France n'y est pas assez préparée.

France : usage de nos données de santé par le secteur public

et imaginons qu'on y rajoute peu à peu des données numériques issues de la santé connectée

France, 10 Avril 2017:
Ouverture du Système National des Données de Santé (SNDS)

"Créé par la loi de modernisation de notre système de santé, le « Système national des données de santé » (SNDS) **regroupe les principales bases de données de santé publiques existantes.**"

Derniers articles | Archives | Recherche

SNDS : le fichier des données de santé des Français est effectif aujourd'hui

par Emilien Ercolani, le 03 avril 2017 16:22 ★★★★☆

Le « Système National des Données de Santé » entre en vigueur ce lundi 3 avril 2017. Il crée ainsi un fichier géant et centralisé qui regroupe les informations de santé de plus 65 millions de Français. Bienvenue dans l'ère du big data et de la santé !

Ce lundi est inauguré le SNDS pour « Système National des Données de Santé », qui avait été promulgué par un **décret du 28 décembre 2016**. Concrètement, il s'agit d'une base de données centralisée qui va regrouper pour le moment quatre types de données : feuilles de soin, consultations, hospitalisations et achat de médicaments.

Les données sont ouvertes, sous conditions, au secteur public de la santé, au secteur privé, à la recherche, etc.

L'accès aux données sera géré par la CNIL

CNIL:

"Dans la mesure où cette base contient des données de santé, c'est-à-dire des données dites « sensibles » au titre de la loi Informatique et Libertés (article 8), et permet un accès permanent au bénéfice de certains organismes, la CNIL a estimé que des garanties particulières de sécurité devaient être mises en place.

Ainsi, un référentiel de sécurité, fixé par un arrêté du 22 mars 2017 et pris après avis de la CNIL, fixe les règles de la gestion sécurisée du SNDS, notamment en termes de pseudonymisation et de traçabilité."

Concrètement, chaque individu se voit attribuer un code spécifique auquel est rattaché l'ensemble des données du SNDS le concernant. Ce processus est construit pour être irréversible : il est impossible, partant du code, de revenir à l'identité de l'individu.

source : https://www.snds.gouv.fr/

JORF n°0071 du 24 mars 2017
texte n° 28

Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé

NOR: AFSE1705146A
ELI: https://www.legifrance.gouv.fr/eli/arrete/2017/3/22/AFSE1705146A/jo/texte

□ Jeu de données : Tout ou partie du SNDS mis à disposition des utilisateurs du SNDS, dans le cadre d'une autorisation pour sa mise à disposition.

□ Pseudonymisation : Procédé visant à la génération d'un identifiant pseudonymisé, appelé ici pseudonyme, à partir d'un identifiant initial signifiant lié à une personne (par exemple : nom, prénom, numéro de sécurité sociale NIR). Le procédé de pseudonymisation ne doit pas permettre l'identification individuelle directe de la personne associée à ce pseudonyme (l'identification indirecte reste toutefois possible). Ce processus est utilisé pour contribuer à l'anonymat et au respect de la vie privée des individus.

□ Ré-identification : Capacité à découvrir l'identité réelle d'une ou plusieurs personnes dont on ne connaît pas directement l'identité (par exemple par déduction ou inférence sur un ou plusieurs jeux de données).

Près de 100 000 applications santé

Applis santé : la CNIL veut protéger nos données intimes

par la rédaction

A l'occasion de son rapport annuel, la Cnil met en garde contre le manque de protection des données personnelles des applications santé pour smartphone, et de la vogue du « moi quantifié ».

Extrait d'étude sur des applis pour diabétiques:

Une protection quasi-inexistante

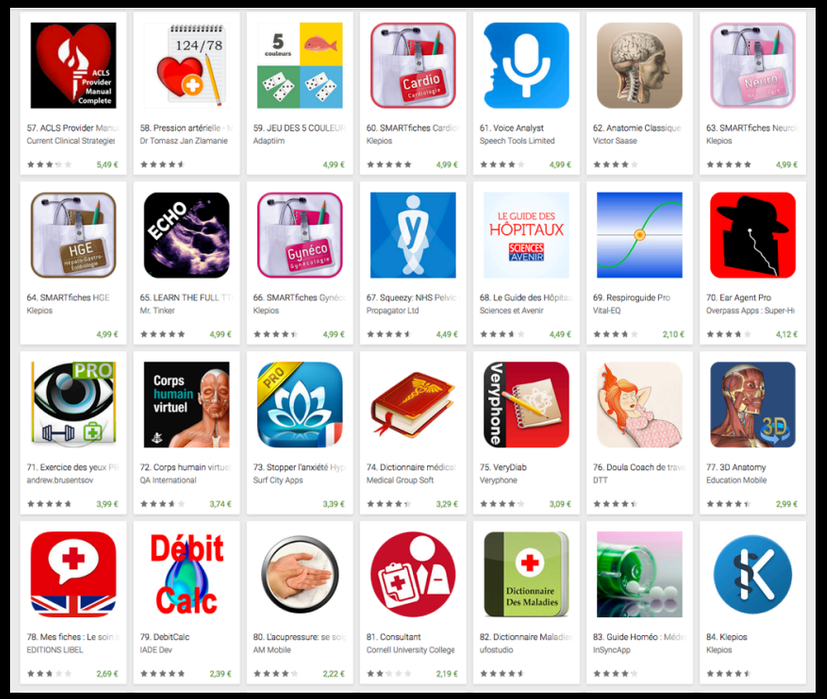
Parmi les applis étudiées, 81 % n'ont pas de politique de protection de la vie privée. Seulement 4 d'entre elles demandent à leurs utilisateurs l'autorisation de partager leurs données de santé.

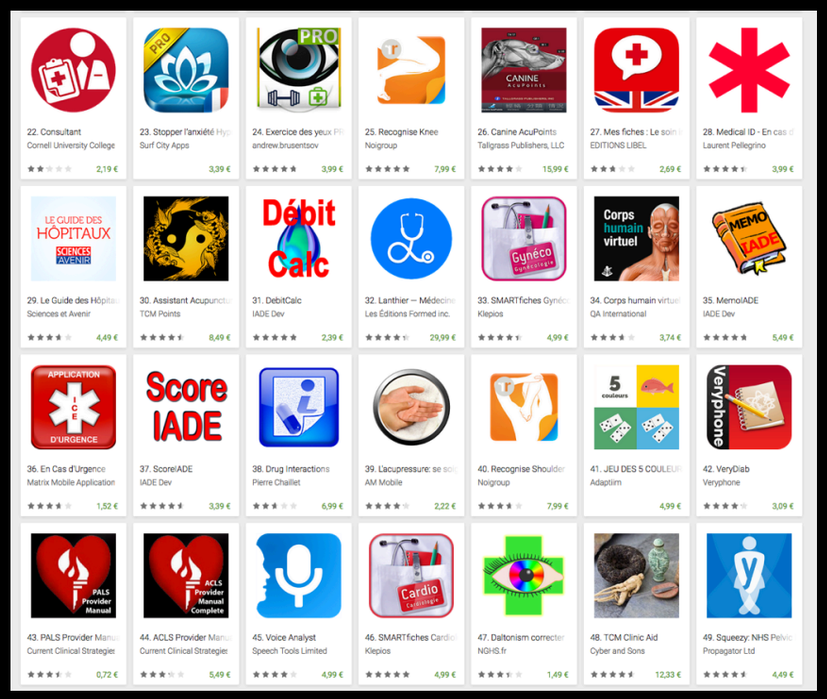
Par ailleurs, 65 applications enregistrant les taux de glucose et d'insuline des patients diabétiques partagent ces informations à des aggrégateurs de données et des agences de publicité. Et près de 9 sur 10 placent également des cookies pour « pister » les habitudes de navigations sur internet de ces patients. Plus inquiétant, sur les 19 applis ayant une politique de confidentialité et partageant les données de santé de ces utilisateurs, 11 d'entre elles n'en faisaient pas mention.

- exploitation des données

150 000 applications *Médecine et Santé* pour smartphones Alphabet (Android) et Apple (iOS)

(60 000 dédiées patients et 80 000 dédiées médecins)





Quasi-personne ne lit les contrats signés lors de l'installation de l'application

(Contrats de droit étranger à 95%)

Quasi-personne ne lit les contrats des OS des smartphones et plateformes (USA), ni des opérateurs (FR).

Jean-Noël Montagné | Nicelab.eu | 25 nov 2017

Les 100 premières sociétés d'achat de données de santé en 2016

agrègent, classent, puis revendent au commerce de biens / services / assurances / big pharma / équipementiers du health care, etc.

Marketing Technology Landscape 2017

Content Marketing

Optimization, Personalization & Testing

DAM & MRM

SEO

Marketing Automation & Campaign/Lead Management

CMS & Web Experience Management

Social Media Marketing & Monitoring

Advocacy, Loyalty & Referrals

Influencers

Chat

Customer Experience, Service & Success

CRM

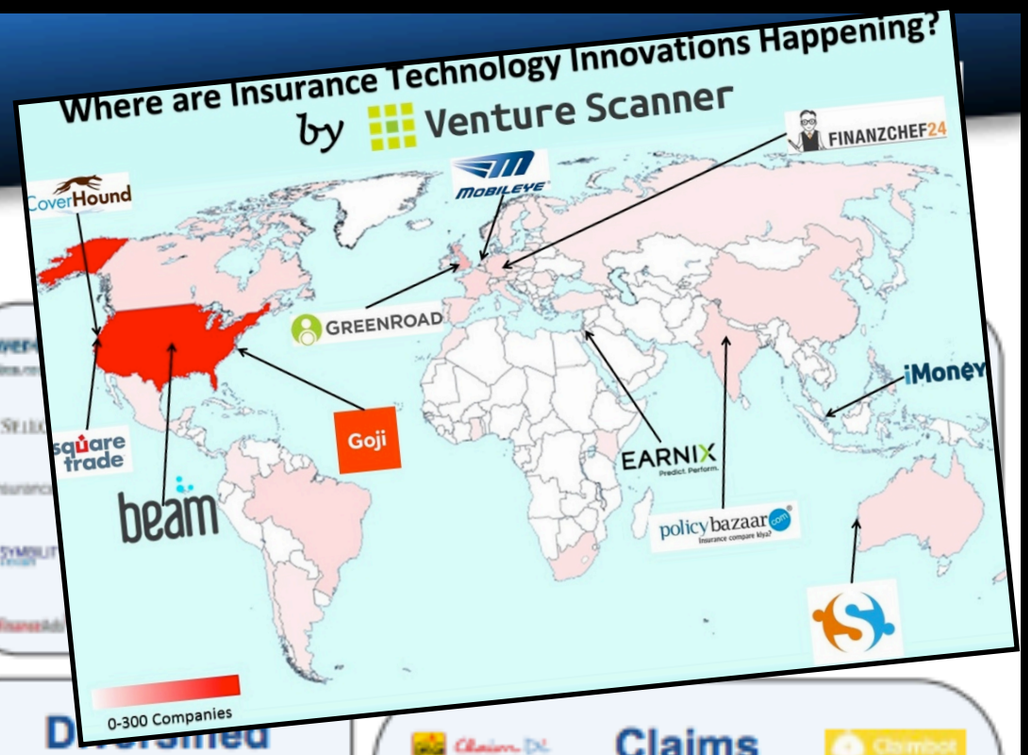
Sales Automation, Enable

Affiliate Marketing & Ma

Ecommerce Marketing

Ecommerce Platforms &

InsureTech Landscape



Insurance Software

QuanTemplate, Llimex, INSLY, Risk App, Brolly, Knip, GUIDEWIRE, mitchell, CLARK, enservio, Velocify, Surely, GetSafe, LAPETUS, Shift Technology, Velocity, ONE, Dynamis, opengi, Praedicat, KASKO, AGENTAVE, MAJESCO

P2P

friedsurance, TTY PEER COVER, inspool, InsPeer, UVAMO, Huddle, SHAcom, DYNAMIS, Tribe Color, Teambrella, GUEVARA

Life

Ladder, IPIPELINE, HAVEN life, Abaris

Sales & Marketing

SURIFY, CLIENTDESK, SAPIENS, messup!, miEdge, Sofarc, zipari, APPLIED, ZYWAVE

Diversified

Microsoft, Tech, SAP, IBM, ORACLE

Claims

Claim DI, Clearbot, dropin, INSURIFY, ClaimKit, Claimbase, [BAUXY], nquitive, snapsheet, CLAIM LOGIK

Health

BIOBEATS, HealthCare.com, BIMA, Accolade, Vencred, Clover, bayrat, oscar, bright HEALTH, LimelightHealth, beam, Welltok, Sense, benefitter, ELIGIBLE

IoT

ring, hive, fitbit, cocoon

Auto / PC

RenewBuy, BUNGALOW, SURE, Hippo, Matic, LeaseLock, CompareAsia, BOLT, trov, Loculitx, LeaseLock, estify, Lemonade, insurun, the zebra, Metromile, INSHUR, RISK, INSURIFY, ValChoice, CoverHound, carvva, SafelyStay, CAPE, URGENTLY, insurify, Goji, Insure My Rental Car

Telematics

OCTO, carrot, COVERBOX, edriving, Driveway, lytx, TrueMotion, roosta, Zubie, VivaDrive, MyDrive, yatis, Zendrive, THE FLOOW

SMB, Specialty, Other

METROPROTECT, TypTap Insurance, Insquirer, PassportCard, Blink, CYENCE, coverager, Agero, Cyberwrite, GIVEASURANCE, CyberFortright

Benefits

BENEFITFOCUS, pokitdok, benefitsolver, GUSTO, Allay, Gather, LUMITY, NAVERA, EMPYREAN, JUSTWORKS, Namely, zuman, PLANSOURCE, ZENEFITS, SimplyInsured, easecentral, Hixme

Life Insurance Companies in Canada

Big Three Life Insurers

- Canada Life
- GREAT-WEST LIFECO INC. → Great-West Life
- London Life
- Standard Life
- Sun Life Financial
- Manulife Financial → Manulife

Did you know that...

... very recently Manulife was the second largest North American Insurance company?

Big Five Banks

- RBC Insurance → RBC Royal Bank
- TD Insurance → TD Bank Financial Group
- CIBC Insurance → CIBC
- ScotiaLife Financial → Scotiabank
- BMO Insurance → BMO

Did you know that...

... by law, banks in Canada are not allowed to sell insurance through their banking branches?

LifeCos and Mutuals

- Equitable Life of Canada
- PRIMERICA
- UL MUTUAL
- Canada Protection Plan
- Empire Life
- Assumption Life
- HUMANIA ASSURANCE INC.

Universal Insurers (Both Life and Non-Life Insurers)

Provide life products

- BCAA
- CAA AMA
- CAA
- CUMIS
- the co-operators
- Wawanesa Insurance → Wawanesa Life
- CPP Investment Board → Transamerica Life Canada
- Northbridge → Federated Insurance
- La Capitale Financial Group → La Capitale
- Old Republic Insurance Company of Canada
- Reliable Life Insurance Company
- Desjardins Insurance → Desjardins
- State Farm
- IA Pacific
- IA Excellence Life Insurance Company
- IA Industrial Alliance → IA Industrial Alliance
- Foresters → Foresters
- Unity Life
- SSQ Insurance
- AXA
- SSQ Financial Group

Non-Profits

- FaithLife Financial
- Blue Cross Association
- Alberta Blue Cross
- Manitoba Blue Cross
- Saskatchewan Blue Cross
- Nunavut Blue Cross
- Medavie Blue Cross

d'autres entités peuvent récupérer les données:

Authorities allowed to access Internet connection records [edit]

List of authorities allowed to access Internet connection records without a warrant:[39][40][41]

- Metropolitan Police Service
- City of London Police
- Police forces maintained under section 2 of the Police Act 1996
- Police Service of Scotland
- Police Service of Northern Ireland
- British Transport Police
- Ministry of Defence Police
- Royal Navy Police
- Royal Military Police
- Royal Air Force Police
- Security Service
- Secret Intelligence Service
- GCHQ
- Ministry of Defence
- Department of Health
- Home Office
- Ministry of Justice
- National Crime Agency
- HM Revenue & Customs
- Department for Transport
- Department for Work and Pensions
- NHS trusts and foundation trusts in England that provide ambulance services
- NHS National Services Scotland
- Competition and Markets Authority
- Criminal Cases Review Commission
- Department for Communities
- Department for the Economy
- Department of Justice (Northern Ireland)
- Financial Conduct Authority
- Fire and rescue authorities under the Fire and Rescue Services Act 2004
- Food Standards Agency
- Food Standards Scotland
- Gambling Commission
- Gangmasters and Labour Abuse Authority
- Health and Safety Executive
- Independent Police Complaints Commission
- Information Commissioner
- NHS Business Services Authority
- Northern Ireland Ambulance Service
- Northern Ireland Fire and Rescue Service Board
- Health & Social Care Business Services Organisation
- Office of Communications
- Police Ombudsman for Northern Ireland
- Police Investigations and Review Commissioner
- Scottish Ambulance Service Board
- Scottish Criminal Cases Review Commission
- Serious Fraud Office
- Welsh Ambulance Services National Health Service Trust

Investigatory Powers Act 2016,

UK

Exemple:
Royaume Uni
nov. 2016

www.parliament.uk

France

Loi renseignement : une première «boîte noire» activée pour surveiller les communications

Par Elsa Trujillo | Mis à jour le 14/11/2017 à 15:49 / Publié le 14/11/2017 à 15:46

Que font les GAFAMSS avec nos données de santé ?

m PIXELS | CHRONIQUES DES (R)ÉVOLUTIONS NUMÉRIQUES | VIE

TION
NNÉS

L'ampleur des données de santé collectées par Google inquiète outre-Manche

Avec Simband et SAMI, Samsung veut vendre vos données de santé

Guillaume Champeau - 29 mai 2014 - Sciences

Accueil > Sciences > Avec Simband et SAMI, Samsung veut

MWC 2017

Facebook combat les fraudes à l'assurance maladie aux côtés de la Sécu

ARGENT | ACTUALITÉS

Publié par Jeanic Lubanza le Mardi 29 Octobre 2013 : 16h43

11 COMMENTAIRES

La Sécurité sociale s'est alliée au géant facebook afin de lutter contre la fraude à l'assurance maladie. Comment ? En croisant les données des assurés à celles des [illegible]teurs des réseaux sociaux.

VOUS AIMEREZ AUSSI

Radars, électricité, carte d'identité… Voici tout ce qui change le ...

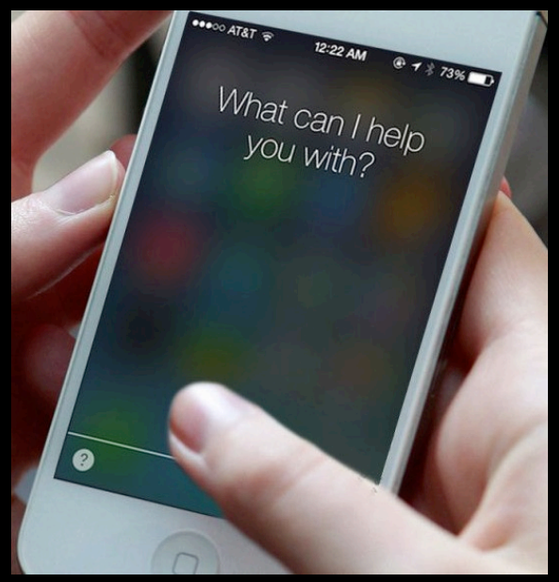
Apple approche les mutuelles pour divulguer le comportement des assurés

Guillaume Champeau - 22 août 2014 - Sciences

Vidéo : Ça y est, AXA conditionne un avantage santé à un objet connecté

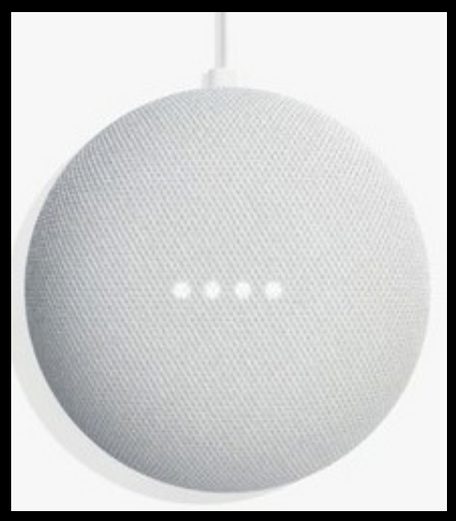
Guillaume Champeau - 02 juin 2014 - Scienc

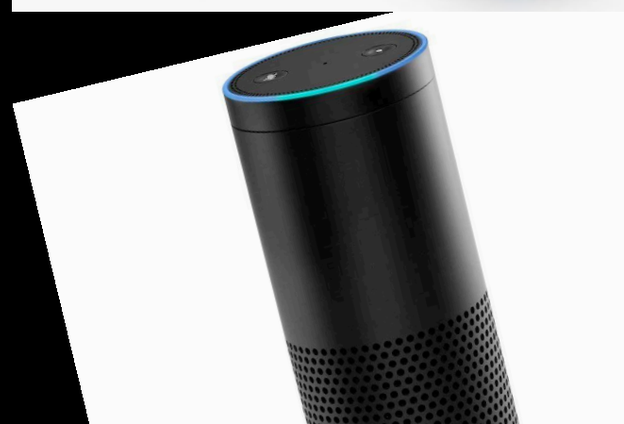
IA : Les maitres du jeu



- Apple Siri, 2012
- Amazon Alexa, 2014
- Microsoft Cortana, 2015

- Google Assistant, 2016
- Samsung Viv, 2016
- Facebook M (bots)





Les IA des GAFAMS, par le biais des assistants personnels récoltent des données directes sur les utilisateurs, les données issues des applications, les données issues des équipements embarqués connectés, les données issues des équipements connectés de l'environnement.

The Artificial Intelligence Arms Race: Alexa, Cortana, Google Assistant, Siri, Viv… and What's Next

Posted on October 12, 2016 by Charlotte O'Donnelly

Share this with others

It's On! 2017 Is The Year The Virtual Assistant Wars Get Real

Amazon's Alexa, Google's Assistant, and Microsoft's Cortana look to hardware partnerships and development deals to take on Apple's

Microsoft explains its plan to win the 'battle for the future' against Amazon's Alexa and Google Assistant

Matt Weinberger 10 Jan 2017, 01:34 Enterprise 27,740

CNN tech BUSINESS CULTURE GADGETS FUTURE

Samsung's new AI assistant will take on Siri and Alexa

by Sherisse Pham @Sherisse

March 21, 2017: 8:32 AM ET

We put Siri, Alexa, Google Assistant, and Cortana through a marathon of tests to see who's winning the virtual assistant race — here's what we found

- impact des technologies 3.0 sur l'environnement et la société

- impact sur l'utilisateur et son entourage
- impact sur les écosystèmes et la société
- impact sur la santé mentale

La réalité écologique des objets connectés:

Des milliards de petits objets électroniques à durée de vie courte (6 mois environ)

- un sourçage des matériaux de plus en plus destructeur
- une industrialisation irresponsable utilisant des esclaves et des enfants.
- une durée d'utilisation ultra réduite = gaspillage de ressources rares.
- miniaturisation = pas de recyclage possible = pollution de milliards d'objets toxiques.

Chaque appareil connecté contient une batterie au Lithium,
chaque appareil connecté contient du Cobalt et du Tantale

Prévision: 20 milliards d'objets connectés en 2025

60% du cobalt et tantale viennent du Congo et sont extraits majoritairement à la main.

FINANCE & MARCHES

Une poignée de « hedge funds » se ruent sur les stocks mondiaux de cobalt

J. JQ. - LES ECHOS | LE 27/02/2017

FRANCE-METALLURGIE

Home

Pour La Métallurgie, en France

La ruée sur le lithium et le cobalt (FR)

Posted on 10 September 2017 by Metallurgist | No Comments

Estimations de la période d'épuisement des réserves de métaux rares et précieux, Source: EcoInfo CNRS, 2014

de 5 à 50 ans :

- **l'indium** (In) : utilisé massivement depuis peu dans le cadre de la fabrication des écrans LCD, écrans tactiles des ordinateurs portables, tablettes, téléphones portables
- le **gallium** (Ga) : utilisé dans les leds d'affichage, les télécommandes infrarouges, les lecteurs/graveurs de CD, DVD, Blue-ray, disques durs
- le **germanium** (Ge) : utilisé dans la Wifi
- **l'antimoine** (Sb) : composant de plaques d'accumulateurs plomb-acide (courant secouru), des semi-conducteurs InSb, GaSb utilisés pour la détection dans l'infrarouge, pour les sondes à effet Hall (détection de champ magnétique), dans les processeurs, isolant remplaçant le dioxyde de silicium SiO_2, sous forme d'oxyde Sb_2O_3, il diminue la propagation des flammes dans les matières plastiques
- le **hafnium** (Hf) : les gisements exploitables à un coût admissible seront épuisés en 2018. On le trouve dans les processeurs, isolant remplaçant le dioxyde de silicium SiO_2
- **l'or** (Au) : utilisé dans l'électronique au niveau des contacts pour ses propriétés de conductivité, d'inaltérabilité, d'inoxydabilité et sa finesse
- **l'argent** (Ag) : conducteurs, interrupteus, contacts
- **l'étain** (Sn) : son succès dans l'industrie électronique est dû à l'abandon du plomb, jugé trop toxique, pour les soudures
- le **zinc** (Zn) : il n'a pas une utilité directe dans les TIC, mais l'indium est un de ces sous-produits
- le **rhénium** (Rh)
- **l'arsenic** (As) : utilisé dans les semi-conducteurs en association avec le gallium

La pollution hertzienne est croissante:

Toutes les technologies sans fil des smartphones, objets et équipements connectés de la santé connectée utilisent :

- bluetooth
- wifi
- zigbee
- LoRa
- 2G/3G/4G/5G

qui sont dans le domaine de fréquence des micro-ondes (classement "cancérogène probable" selon OMS)

- impact sur la santé mentale de l'utilisateur

- un utilisateur de moins en moins coopérateur et savant (IA)
- un utilisateur à l’affût permanent des signaux de «normalité»
- un utilisateur dépressif entre les gratifications de dopamine
- un utilisateur dépendant de son smartphone, de son assistant de santé
- un utilisateur manipulé par les algorithmes des GAFAMSS
- un transhumanisme délétère, augmentant le niveau d'anxiété.

La vision de quelques activistes technologiques, hackers et protecteurs de la vie privée

Jouer avec tous les protocoles, tous les objets, toutes les infrastructures, afin de les pénétrer, les détailler, les détourner, les confondre, les contourner, les arrêter, les limiter, les anonymiser, les dénoncer si besoin.

Faire soi-même l'analyse des données indispensables.
Faire soi-même ses objets connectés (Echopen, OpenEEG)

Créer des passerelles techniques de protection de la vie privée: 2 projets fondés par la Commission Européenne:

-Dowse de Dyne.org = anonymisation et contrôle
-Nervousnet de ETH Zurich= contrôle et refonte d'un écosystème en bien commun.

Influencer les innovateurs vers une prise en compte de la réalité sociale, géo-économique, géo-stratégique, géo-écologique, dans le contexte du chaos climatique à venir, et non de la vision des marchés financiers et des GAFAMSS

Favoriser l'open source comme gage d'inter-opérabilité et de contrôle citoyen dans les institutions sanitaires et les espaces de soin.

Dénoncer les technologies de contrôle M2H par l'IOT, aussi bien dans l'espace public, privé, les espaces de soin, que dans le monde du travail.

Utiliser l'IOT comme instrument de connaissance du corps, de responsabilisation du citoyen dans son corps, en préservant ou augmentant ses perceptions propres & autonomes, sans objet connecté.

Jean-Noël Montagné | nicelab.eu