Internet des objets et vie privée :

le cas de la « maison intelligente »

Vincent Roca

Plan du cours

1. Introduction
2. Exemples dans le domaine de la « maison intelligente »
3. Les acteurs, leurs motivations (supposées) et la vie privée
4. Cas d'étude : analyse d'une ampoule connectée…
5. Que faire ? Quelques solutions alternatives
6. Conclusion : « maison intelligente », vie privée, etc.

Protection de la vie privée

Internet des objets et vie privée

Introduction :
Internet des objets, un pas de plus vers le monde entièrement numérique…

Vincent Roca

informatiques mathématiques Inria

L’Internet des objets : une rupture…

- **Révolutionne** Internet
  - Prédominance des communications machine-à-machine (plus d'humain).
  - Croissance considérable de la connectivité et du trafic.
- **Révolutionne** beaucoup de secteurs
  - Bâtiment, ville, infrastructures, véhicules, services, etc.

- **… qui vient avec son lot de questions !**
  - Notamment **sécurité** et respect de la **vie privée**
  - Des questions **sociétales.**

La fin de la « vie privée par défaut » ?

- Contribue largement à l'idée que la vie privée fait partie du passé.
  - Il y a 20 ans, capter des données personnelles **demandait des efforts**…
  - …c'est désormais **l'inverse** !

  - Après notre navigation web, nos recherches Internet, notre messagerie, nos déplacements, nos achats, notre smartphone, les derniers bastions de notre intimité tombent progressivement :
    - Maison
    - Véhicule
    - Ville

Des réseaux d'accès parfois un peu spéciaux…

- Réseaux dédiés à très large couverture
  - Les "Low Power Wide Area Networks" (LPWAN) tels Sigfox et LoRa
  - Réseaux spécifiques, bas débit, très faible consommation énergétique et coût
- 5G
  - L'augmentation des débits n'est pas le bénéfice principal de la 5G, la faible latence et la connexion d’un grand nombre d’objets si.

Des réseaux d'accès parfois un peu spéciaux… (2)

- Des réseaux locaux à faible consommation énergétique :
  - Bluetooth et Bluetooth Low Energy (BLE)
  - ZigBee
  - (ou autre Z-Wave, 6LowPAN, etc.)
- Mais aussi le WiFi

Ce à quoi on va s'intéresser principalement.

Point de vue adopté : « maison intelligente »

- Des **objets** connectés
  - prises, ampoules, thermostat, chauffage, caméra, verrous de porte, etc.

- Des systèmes pour les **contrôler**
  - application smartphone, enceinte connectée, assistant vocal, interrupteur, etc.

NB: on ne parlera pas des compteurs connectés, des véhicules autonomes ou de la ville « intelligente ».

Protection de la vie privée

Internet des objets et vie privée

Exemples dans le domaine de la « maison intelligente »

Vincent Roca

informatiques mathématiques Inria

Côté objets : l'ampoule connectée

- Une ampoule LED dont on peut varier l'intensité lumineuse ou la couleur.

- Exemple : ampoules Philips Hue™ et IKEA Tradfri™
  - Connectées en **ZigBee**, un pont la connecte au réseau domestique.

- Exemple : ampoule LIFX
  - Connectée en **WiFi** sur le réseau de la maison.

Côté objets : la prise connectée

- Une prise que l'on peut allumer ou éteindre manuellement ou par planification horaire, qui peut effectuer un relevé de consommation précis.

- Exemple : prise TP-Link
  - Directement connectée au réseau **WiFi** de la maison.

Réseau WiFi de la maison

Côté objets : l'aspirateur autonome

- Un aspirateur qui fait tout tout seul.

- Exemple : l'aspirateur Roomba de iRobot.
  - Des capteurs pour **cartographier** la maison et se localiser.
  - Pertinent car :
    - l'aspirateur sait où il est, ce qui est fait ou à faire, répond à des injonctions précises.
  - Connectable en WiFi avec le réseau de la maison.

© iRobot

Côté objets : bien d’autres choses encore

- Des thermostats intelligents, des portiers, des caméras de surveillance avec reconnaissance faciale, etc.

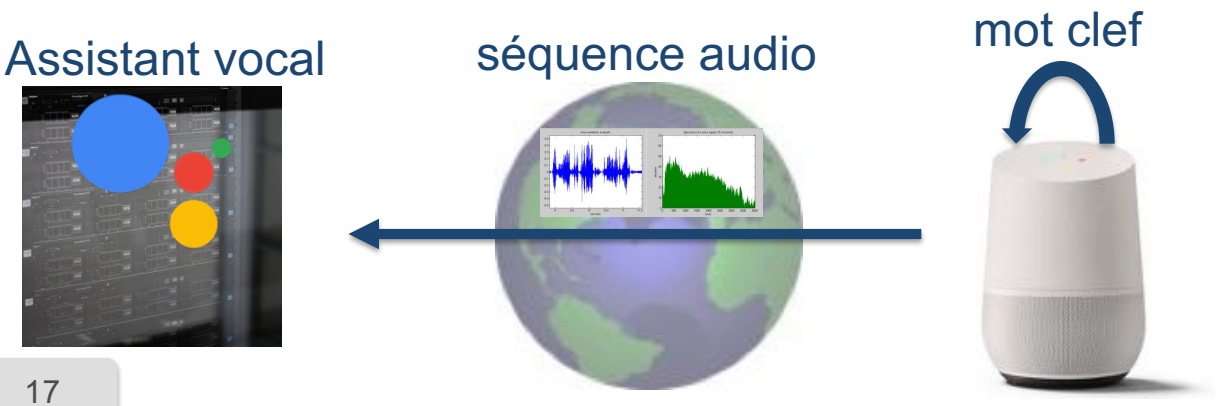
Côté contrôle : l'application smartphone

- Application **spécifique** à un fabriquant d'objet ou application **générique**.

- Fonctionnement :
  - cas d'un smartphone connecté par le réseau **WiFi de la maison :**
    - Il est possible que appli et smartphone communiquent directement avec l'objet…
    - … mais pas toujours !
  - cas d'un smartphone connecté **en 4G :**
    - On passe par le réseau de l'opérateur et Internet…
    - … même si l'on est physiquement chez soi !

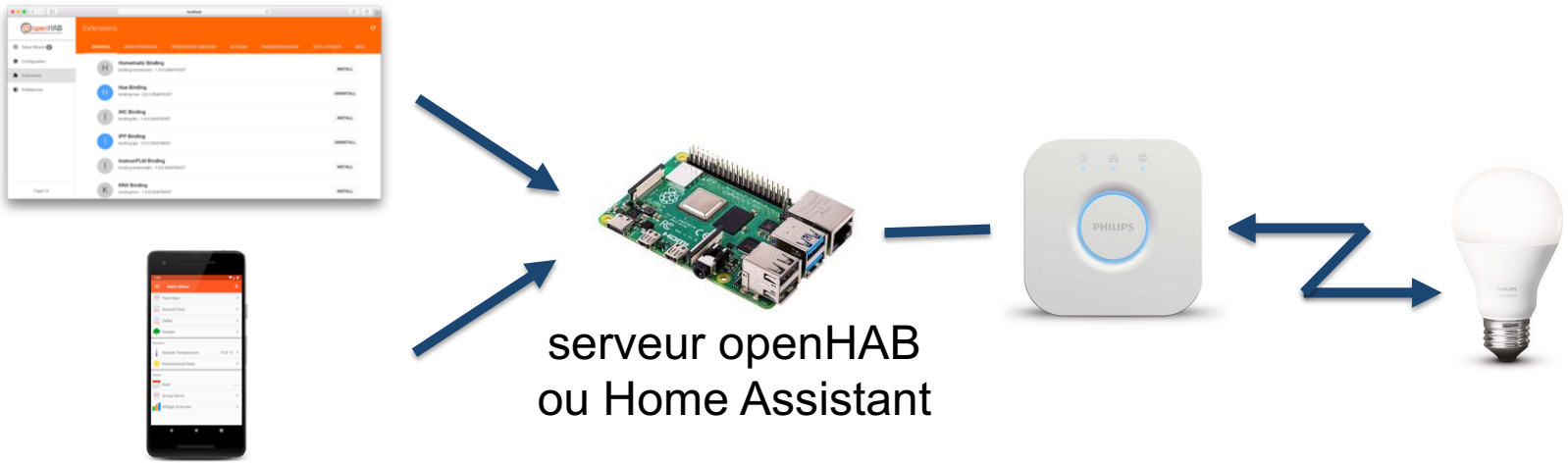
Côté contrôle : l'enceinte connectée

- Utilise un « assistant vocal », logiciel qui assure la reconnaissance vocale.
    - Siri (Apple), Alexa (Amazon), Assistant Google, Cortana (Microsoft).
  - Reconnaissance faite à distance sur des serveurs dédiés (Internet requis).
  - Fonctionnement :
    - Recherche permanente du mot déclencheur (en local).
    - Transmission des séquences audio à des serveurs sur Internet pour reconnaissance vocale et interprétation.
    - Déclenche une action.



Côté contrôle : les systèmes génériques

- Par des développeurs indépendants, pour contrôler divers objets connectés.
  - **openHAB** (https://www.openhab.org/)
  - **Home Assistant** (https://www.home-assistant.io/)
- Requiert un **serveur** (par ex. un micro-ordinateur type Raspberry Pi)
  - Le « serveur » exécute le logiciel openHAB ou H.A. et est en lien avec les objets.



Côté contrôle : l’interrupteur BLE ou Zigbee ou…

- Communication directe (par ex. en ZigBee) sans « concentrateur » avec une ampoule ZigBee
  - Ne s’applique pas aux ampoules WiFi.
  - Version connectée de l’interrupteur qui ouvre ou ferme un circuit électrique.

Pour résumer

- Des **objets connectés**…
  - De nature très diverse.
- …des **moyens de contrôle** pour ces objets.
  - Application smartphone, enceinte connectée, interrupteur, etc.
- Une grande diversité de situations et produits.
  - Rien n'est simple dans ce domaine.
  - Plusieurs technologies réseau, avec des implications importantes.

Protection de la vie privée

Internet des objets et vie privée

Les acteurs, leurs motivations (supposées) et la vie privée

Vincent Roca

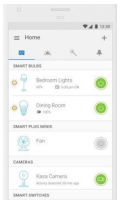
informatiques mathématiques
Inria

Ça se complique dans la « maison intelligente »

- Plusieurs catégories d'acteurs :
  - Des fabricants **d'objets connectés**

  - Des fabricants de **smartphones**

  - Des développeurs d'**applications**



  - Des fabricants d'**enceintes connectées**

NB: on ne parlera pas des fournisseurs d'énergie ni des compteurs connectés.

Quels modèles économiques ?

- Ça dépend…
  - Un fabricant d'objet connecté vend du matériel. Mais est-ce tout ?
  - Idem, un fabricant de smartphone veut rester dans la course et vendre des smartphones. Mais est-ce tout ?
  - Quid des autres acteurs ?

Captation, traitement et échange de données personnelles font ils partie du modèle économique ?

Des données qui ont intrinsèquement du sens

- Allumer/éteindre une ampoule…
  - … informe sur la présence, les habitudes de vie, des comportements atypiques.
- Une courbe de charge électrique précise…
  - … informe sur la nature des équipements électriques et les habitudes de vie.
- Le plan de la maison (aspirateur connecté)…
  - …informe sur la composition (possible) de la famille.

… Surtout si elles sont croisées avec d'autres

- Elles ne restent pas isolées :
  - Les gros acteurs se sont imposés : tout objet connecté **doit être contrôlable** via une enceinte Google ou Amazon.
    - Sinon le fabricant risque un échec commercial.
  - Ces gros acteurs ont des données issues d'autres services qui sont croisées avec celles de la maison.
    - Ex. : une adresse + plan de l'habitation
      donne une idée **précise** du niveau de vie.

… Surtout si elles sont croisées avec d'autres (2)

Comment votre Assistant Google peut vous aider au quotidien

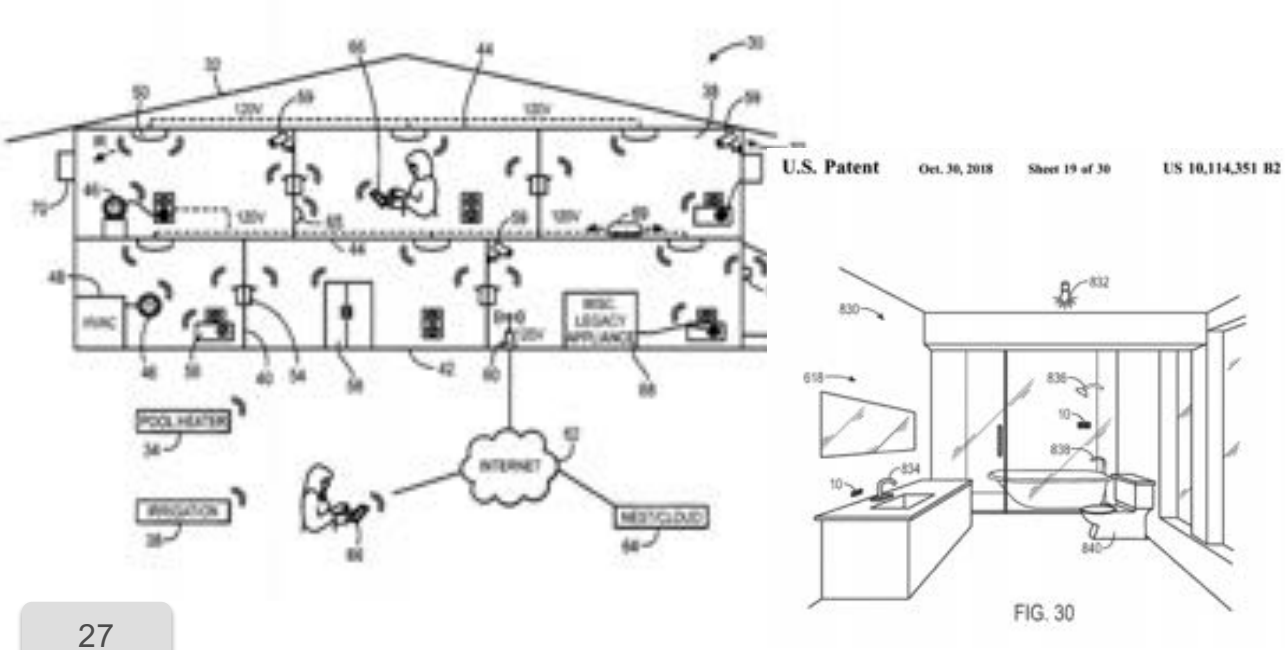
Que vous soyez à la maison ou en déplacement, votre assistant est toujours prêt à vous aider. Lorsque vous lui demandez quelque chose, il utilise des données provenant d'autres services Google pour vous répondre. Par exemple, si vous lui demandez "Quels sont les cafés dans les environs ?" ou "Est-ce que j'aurai besoin d'un parapluie demain ?", votre assistant utilise des informations provenant de Google Maps et de la recherche Google, ainsi que votre position, vos centres d'intérêt et vos préférences, pour vous donner la réponse la plus pertinente. Consultez l'outil "Mon activité" pour voir ou supprimer les données recueillies lors de vos interactions avec votre assistant.

Google Assistant

Extrait de la charte de vie privée de Google.

… Surtout si elles sont croisées avec d'autres (3)

- Brevet obtenu par Google sur « système automatisé pour la maison intel. »
  - "routinely eavesdrop on your daily life".
  - "would aid parents in managing the household, using cameras and sensors to monitor kids' behavior".
  - https://www.zerohedge.com/news/2018-11-20/google-wants-data-mine-your-home-and-kids-bedroom



Pour résumer

- Une multitude d'acteurs aux motivations potentiellement très différentes.
  - Question de fond : la captation de DP fait elle partie du modèle économique ?

- Chaque donnée a individuellement du sens… mais les croiser est clef.
  - Explique que les gros acteurs manœuvrent pour être à la croisée des chemins.
  - Ces derniers croisent les données issues des différents services.

Protection de la vie privée

Internet des objets et vie privée

Cas d'étude : analyse d'une ampoule connectée…

Vincent Roca

informatiques mathématiques
Inria

La cible : une ampoule et ses moyens de contrôle

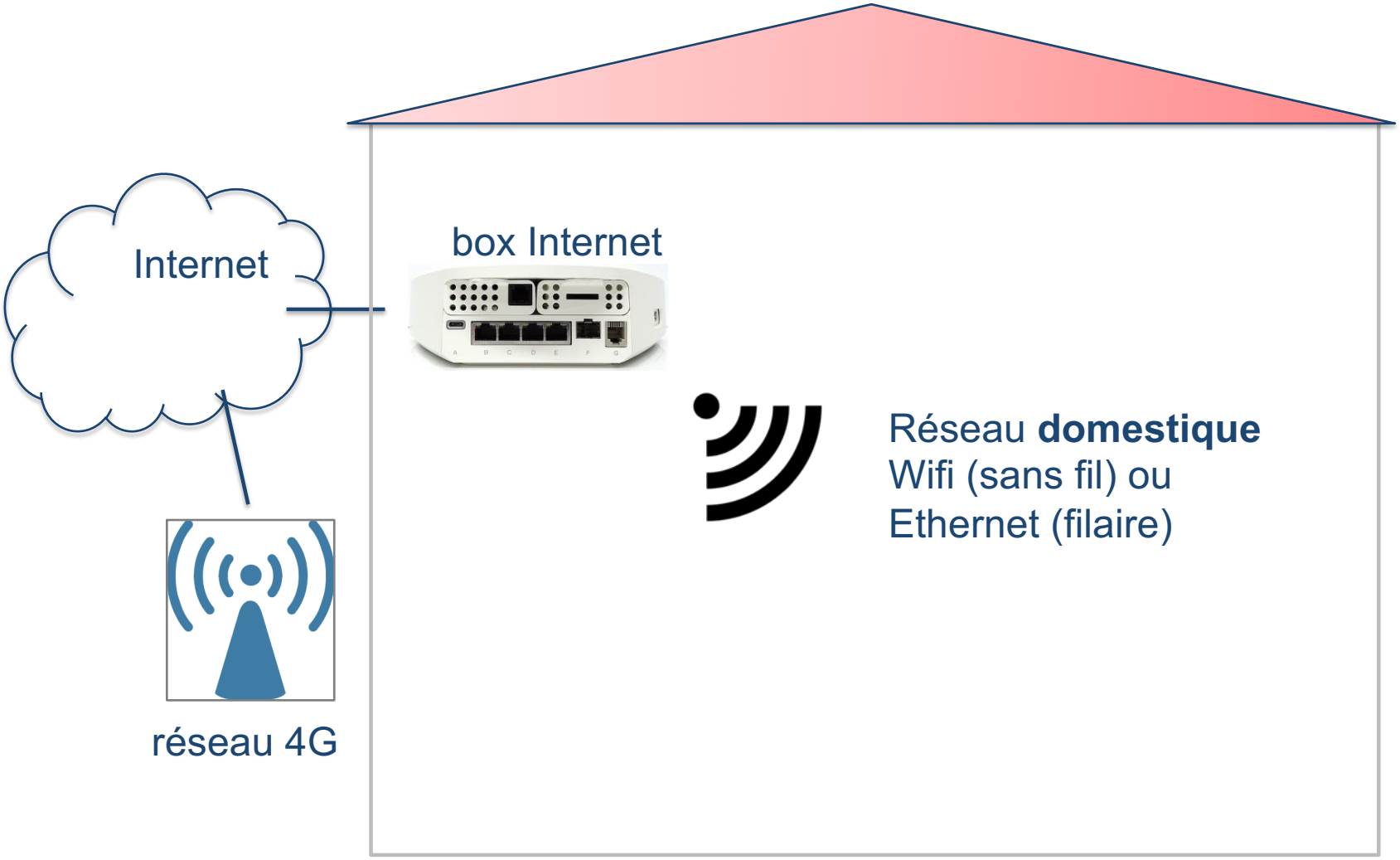
- Une **ampoule connectée**, Philips Hue™, et le pont Philips associé
- Des **applications smartphone** pour **contrôler** l'ampoule
- Des **enceintes connectées** pour **contrôler** l'ampoule
- Un **interrupteur connecté** pour **contrôler** l'ampoule

La cible : ampoule et moyens de contrôle (2)

- On veut comprendre :
  - les différents **échanges** de données,
  - les **acteurs** impliqués dans ces échanges,
  - la **territorialité** des échanges.

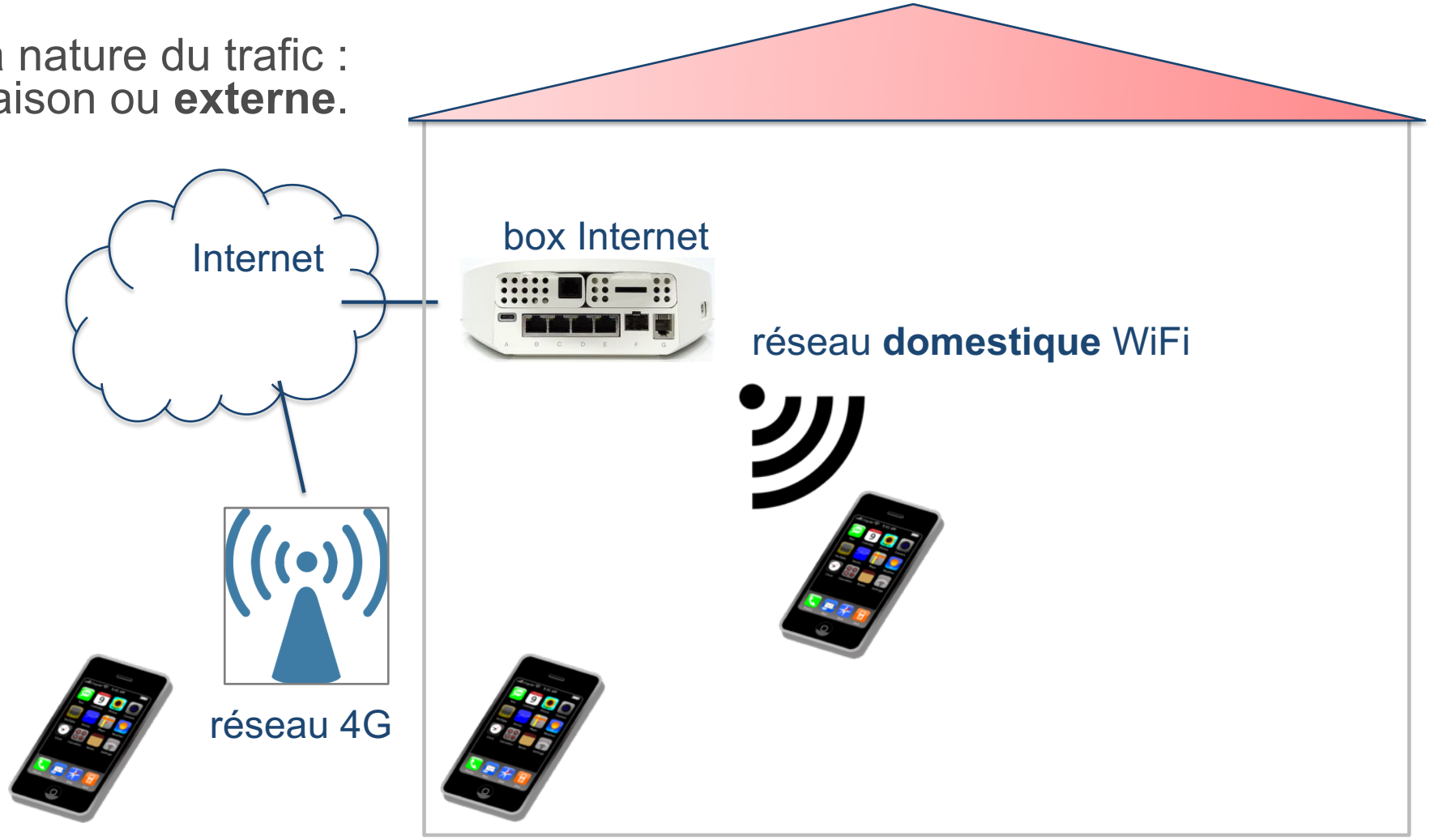
Ceci (1) pour l'ampoule et (2) pour chaque moyen de contrôle.

La configuration réseau

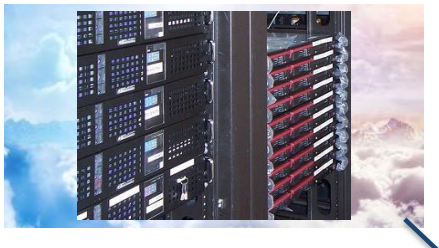


Le smartphone : connexion 4G ou WiFi ?

- Détermine la nature du trafic : **local** à la maison ou **externe**.



L’ampoule Philips Hue et son pont



serveur Cloud Philips (hébergé par **Google**)

Internet

box Internet

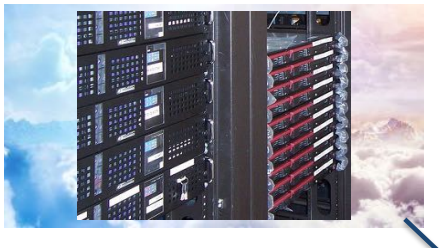
pont Philips

Philips Hue

ZigBee
(réseau sans fil à faible conso électrique)

appli. Philips dédiée
(configuration + contrôle)

Contrôle via l'appli Philips Hue, en Wifi local



serveur Cloud Philips (hébergé par **Google**)

Internet

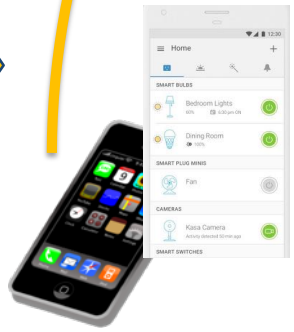
(3) échanges périodiques

box Internet

Philips Hue

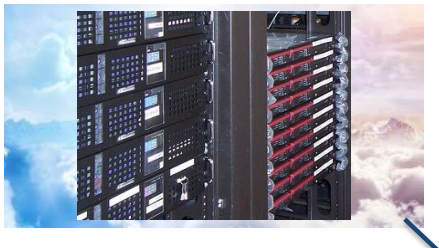
(2) ordre « allumer »

(1) ordre « allumer »



appli. Philips dédiée **smartphone à la maison en Wifi**

Contrôle via l'appli Philips Hue, en 4G



serveur Cloud Philips (hébergé par **Google**)

(2)

serveurs (**Google**)

Internet

(3) ordre « allumer »

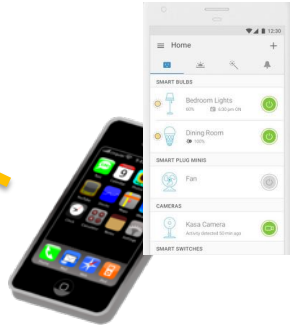
box Internet

Philips Hue

(4) ordre « allumer »

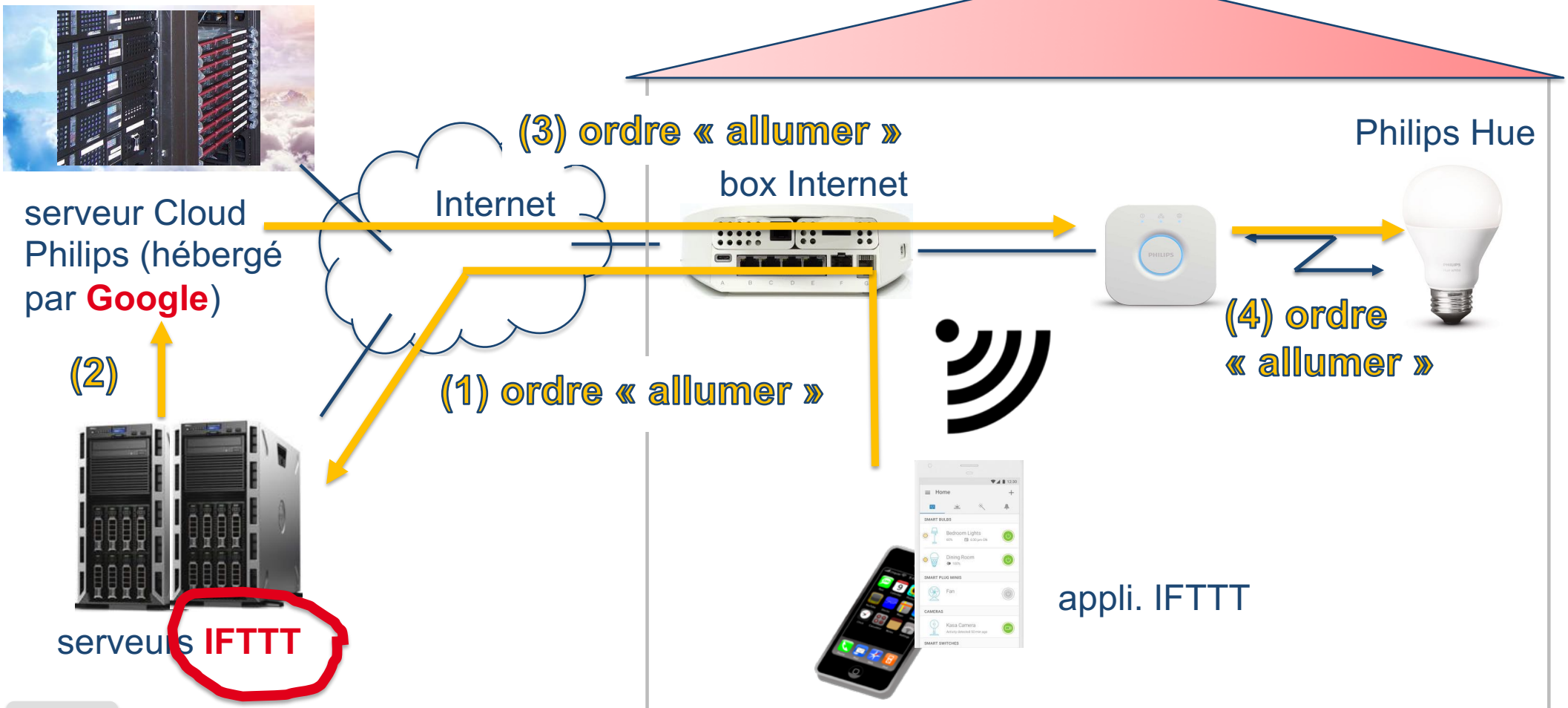
(1) ordre « allumer »

réseau 4G

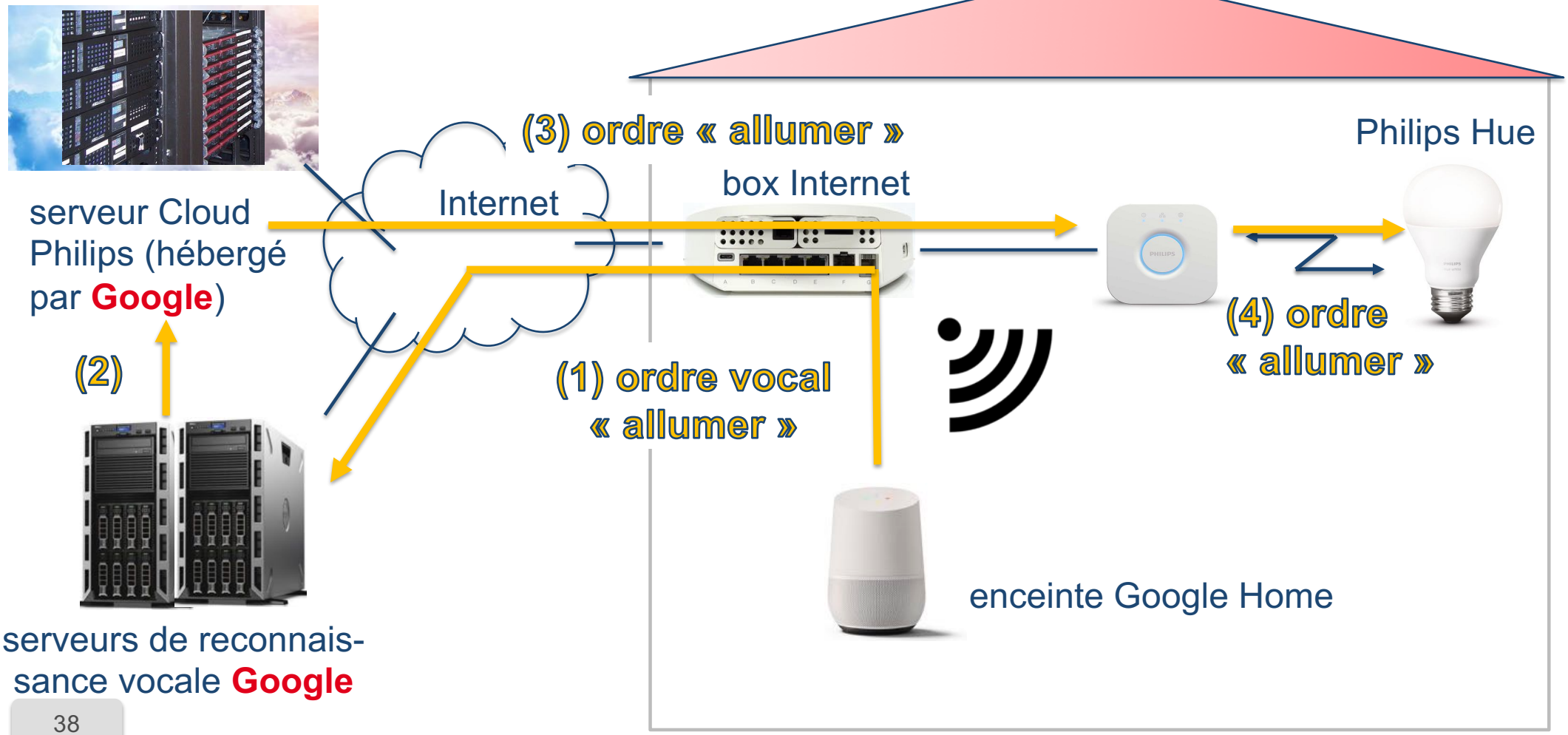


appli. Philips dédiée **smartphone en 4G, à la maison ou à l'extérieur**

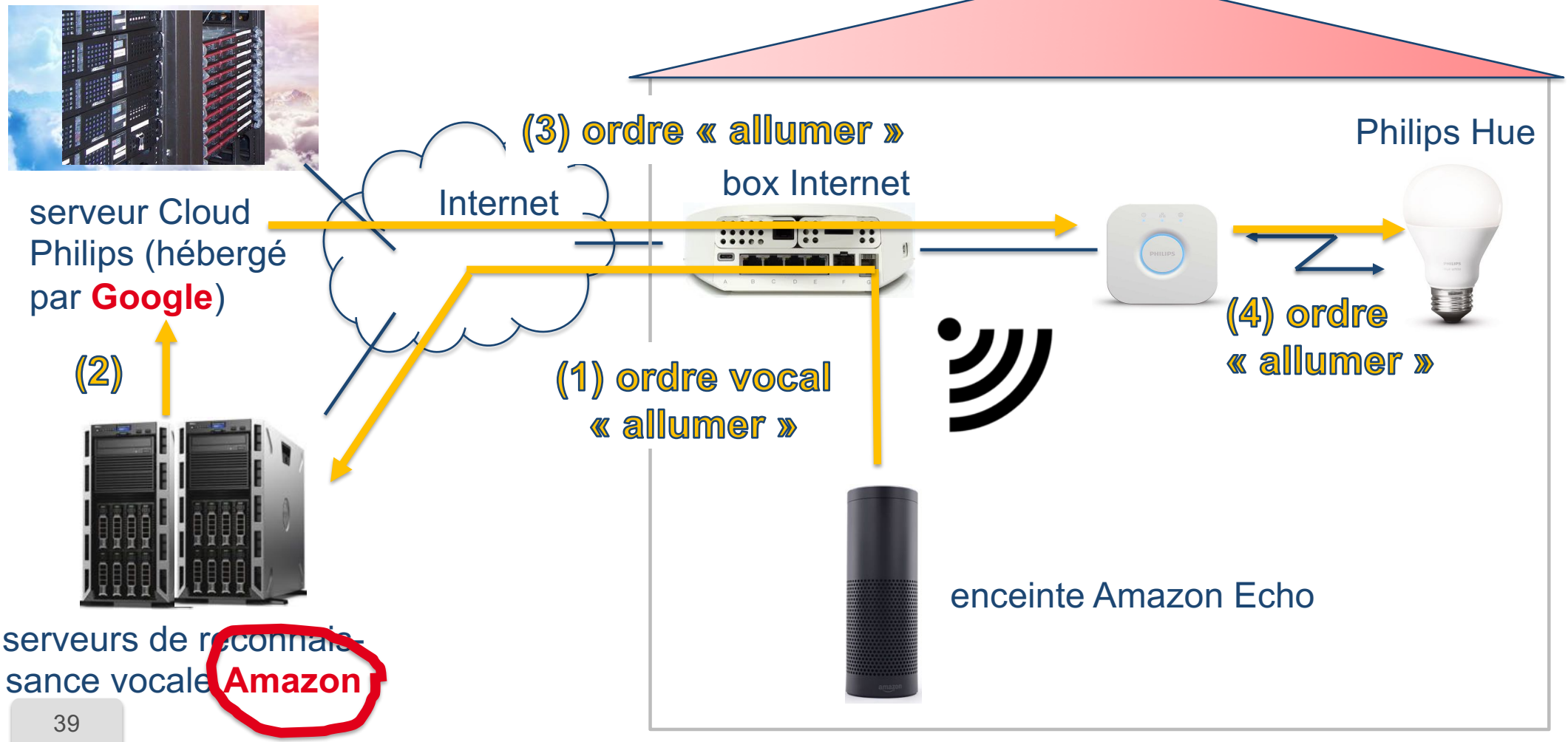
Contrôle via une autre appli. smartphone : IFTTT



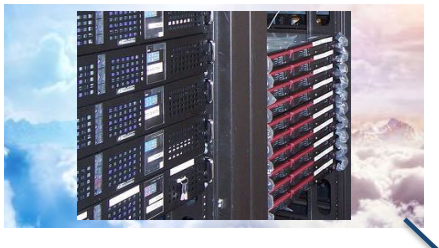
Contrôle via une enceinte Google Home



Contrôle via une enceinte Amazon Echo



Contrôle via un interrupteur ZigBee (ici IKEA)



serveur Cloud Philips (hébergé par **Google**)

(2) échanges périodiques

Internet

box Internet

Philips Hue

(1) ordre « allumer »

interrupteur ZigBee

Le moyen de contrôle est essentiel !

- Définit quels sont les **acteurs impliqués**, potentiellement « au courant ».
  - Google/Amazon se sont imposés dans les « maisons intelligentes » via :
    - leurs enceintes ;
    - leurs services : Cloud, env. de développement, reconnaissance vocale.

- Des questions de **souveraineté**.
  - Beaucoup de flux sortent de la maison, voire de France et d'Europe.

Le moyen de contrôle est essentiel (2)

- Crée une **dépendance** : une coupure Internet peut empêcher tout contrôle.
  - Même à 2 mètres de son ampoule. Est-ce raisonnable ?

- Des impacts **écologiques** passés sous silence.
  - Des équipements toujours sous tension.
  - Omniprésence des échanges hors maison.
  - Les enceintes connectées génèrent un trafic conséquent envoyé sur Internet.
    - Pour analyse des séquences audio.
    - Quel bilan par rapport à un traitement local ?

Pour résumer

- Même si la « maison intelligente » peut avoir du sens, il y a des soucis :
  - Une **menace** pour la vie privée car ces données **ont du sens**, surtout croisées avec d'autres.
  - Domination des **acteurs hors Europe**
    - Sociétés américaines soumises au Cloud Act.

Pour résumer (2)

- Une situation techniquement très complexe qui dépend :
    - de l'objet cible,
    - des choix du fabriquant,
    - des moyens techniques utilisés pour les contrôler,
    - du type de connexion et de la localisation du smartphone.
  - Pas de réponse unique à la question « quels sont les risques ? », les possibilités sont trop nombreuses.

- Même les spécialistes n'ont pas une compréhension complète !

Protection de la vie privée

Internet des objets et vie privée

Que faire ? Lecture des chartes de VP et solutions alternatives

Vincent Roca

informatiques mathématiques
Inria

Que peut-on faire ? Redonner du contrôle aux utilisateurs

- On va discuter :
  - des moyens d'information accessibles à l'utilisateur final ;
  - de solutions alternatives respectueuses de la vie privée.

Où chercher des informations ?

- Le RGPD impose au responsable de traitement d'obtenir un consentement :
  - **Libre, spécifique et univoque, et éclairé.**
- Impose une **information de qualité** des utilisateurs

https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes

consentement de qualité

doit être **éclairé**

information de qualité

Où chercher des informations ? (2)

- Cette information passe par une « charte de vie privée » (ou « politique de confidentialité »)

- Un texte long et peu engageant, qui doit **informer** l'utilisateur.
  - Ex. Google, tous services et objets confondus : 33 pages + références externes
    https://www.gstatic.com/policies/privacy/pdf/20191015/9ad23b47/google_privacy_policy_fr_eu.pdf

RÈGLES DE CONFIDENTIALITÉ GOOGLE

Lorsque vous utilisez nos services, vous nous faites confiance pour le traitement de vos informations. Nous savons qu'il s'agit d'une lourde responsabilité, c'est pourquoi nous nous efforçons de les protéger, tout en vous permettant d'en garder le contrôle.

Où chercher des informations ? (3)

- L'exercice est certes très difficile pour le responsable de traitement…

- … mais c'est souvent plus un texte destiné à protéger le responsable de traitement qu'un texte destiné à être lu par un utilisateur.
    - Ex. : sanction à l'encontre de Google LLC par la CNIL pour « manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité ».

https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la

Où trouver les chartes ?

- Le cas d'un **objet physique :**
  - N'est jamais imprimée sur une notice, aller sur le **site web du fabricant.**

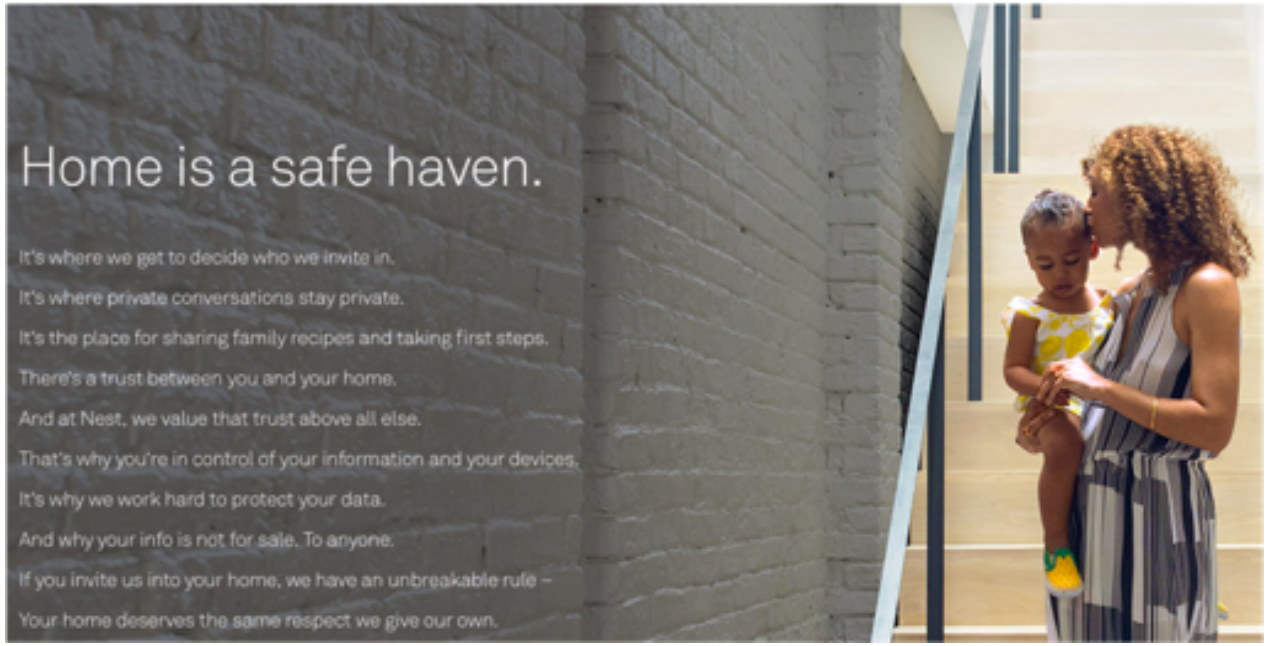
- Le cas d'une **application smartphone :**
  - Pour une appli smartphone, aller voir sur le **site web du développeur** mais aussi sur le **magasin d'applications**., ou dans l'application elle-même.

- Dans les deux cas, essayer de comprendre…

Où trouver les chartes ? Attention…

nest

https://nest.com/privacy/, novembre 2019



1. We believe home is a private place.
2. You should have control over your home.
3. We work hard to keep your data secure.

And we're repeating ourselves, but this is important: your personal information is not for sale. To anyone.

5. Neighbors have to earn your trust. We should too.

The Nest Privacy Policy

Now that you know our approach, read our privacy policy

Learn more >

C'est ce texte qui compte et qui engage la société !

Un exemple : le cas iRobot / aspirateur Roomba

Informations que nous recueillons à partir des appareils iRobot enregistrés.

Certains de nos appareils iRobot sont équipés d'une technologie intelligente qui permet aux appareils iRobot de transmettre des données sans fil aux Services. Nos appareils iRobot ne transmettent pas ces informations, sauf si vous enregistrez votre appareil en ligne et si vous vous connectez au réseau Wi-Fi ou à un autre appareil via Bluetooth. Nos appareils iRobot dotés d'une technologie intelligente peuvent être utilisés sans la transmission de données Wi-Fi ou Bluetooth. Pour ce faire, il vous suffit de déconnecter le réseau Wi-Fi ou Bluetooth de l'appareil ou de ne pas le connecter du tout.

Le tableau de l'Annexe 2 expose les catégories d'informations personnelles que nous collectons sur vous et votre appareil iRobot lorsque vous autorisez votre appareil iRobot à nous transmettre ces informations, et la manière dont nous utilisons ces informations. Le tableau

« Politique de confidentialité » iRobot

https://www.irobot.fr/legal/privacy-policy

version du 23 octobre 2019

Un exemple : le cas iRobot / aspirateur Roomba (2)

- **Connecter** l'aspirateur au WiFi, pour le contrôler via une application smartphone ou une enceinte connectée vaut pour **acceptation** !

> « **noms des pièces**, les heures de démarrage / d'arrêt » […]
> « les **plans des étages**, la détection d'objet, les cartes thermiques et images du réseau **Wi-Fi** » peuvent être utilisées « […] à des fins de **marketing** » par « Les fournisseurs **tiers** et autres **prestataires de services** qui fournissent des services pour nous ou pour notre compte, […] qui peuvent inclure l'identification et la diffusion de **publicités ciblées**, la fourniture de services de **commerce électronique**, […] »

« Politique de confidentialité » iRobot

https://www.irobot.fr/legal/privacy-policy

version du 23 octobre 2019

Des approches alternatives existent

1. Reconnaissance vocale « en local », respectueuse de la vie privée.

2. Les outils de contrôle open-source et libres : openHAB, Home Assistant.
   - Pour un contrôle local de la maison.

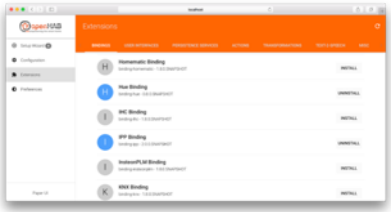
Reconnaissance vocale respectueuse de la VP

- Snips (https://snips.ai/)
  - Moteur de reconnaissance vocale **100% locale**, sans connexion Internet.
    - Fonctionne sur des équipements à faible puissance (ex. Raspberry Pi 3).
    - Respectueux de la vie privée des utilisateurs.
    - Seule la personnalisation de Snips (création d'un assistant) nécessite un apprentissage sur les serveurs Snips puis installation locale.
  - Cible des **intégrateurs**, pas l'utilisateur final
  - Société rachetée fin 2019...

Contrôle de la maison avec openHAB

- openHAB : une initiative open-source et libre (https://www.openhab.org/)
  - Un outil qui fédère tous les objets connectés de la maison, indépendamment du fabricant.
  - Un contrôle purement **local par défaut**.
    - Centré autour d'un mini-serveur local, qui exécute le logiciel openHAB.
  - En option : contrôle possible de l'extérieur via le cloud myopenhab.org, hébergé en Europe.

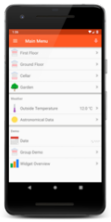
Contrôle de la maison avec openHAB (2)



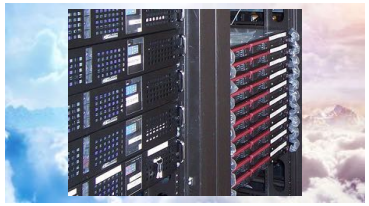
navigateur web ou
application smartphone

serveur openHAB
(ici sur Raspberry Pi3)

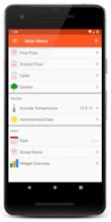
Internet



à la maison



service Cloud
myopenhab.org



à l'extérieur

Pour résumer

- Comprendre ce qui se passe avec un objet ou une application smartphone **est difficile**.
  - Informer l'utilisateur est une **obligation légale**.
  - Nécessite de trouver et lire une « charte de vie privée ».
  - Si le texte n'est pas toujours accessible à un non spécialiste, il peut révéler des choses importantes !

Pour résumer (2)

- Des objets et moyens de contrôles **centrés sur la maison** apparaissent.
  - Sans lien avec les géants d'Internet.
  - Respectueux de la vie privée par défaut.
  - Traitements purement locaux à chaque fois que c'est possible :
    - Plus **robustes** car évite toute dépendance à Internet.
    - Pas de problèmes de **souveraineté**.
    - **Moindre latence** dans le traitement des ordres.
    - **Moindre consommation** énergétique.

Protection de la vie privée

Internet des objets et vie privée

Bilan : « maison intelligente », vie privée, etc.

Vincent Roca

informatiques mathématiques
Inria

Ce n’est pas simple

- **Complexité** intrinsèque :
  - Grande variété de situations (à la maison, dehors, divers moyens de contrôle) ;
  - Grande variété de technologies qui interagissent ;
  - Grande variété d’acteurs en compétition.

- **Google/Amazon ont réussi à s’imposer** via :
  - leurs enceintes et objets connectés ;
  - leurs services : Cloud, kits de développement de qualité, reconnaissance vocale.

Mais les choix architecturaux posent problèmes

- Des choix technologiques **privilégiant des services Internet.**
  - Un argument commercial (produit « high tech »).
  - Une solution de facilité (ça marche aussi quand on est à la maison).
  - Permet de croiser des données d'origines diverses et de leur donner du sens.
    - La principale motivation de nombreux acteurs.
    - Pourtant on a payé pour ces objets (≠ applications gratuites du smartphone).

- Cela pose problème en matière :
  - de **respect de la vie privée,**
  - de **souveraineté,**
  - de **robustesse**,
  - d'**éco-responsabilité.**

Où va-t-on ? Que veut-on ?

- L'argument « on va faire des économies d'énergie » tient-il ?
  - Intègre-t-il l'énergie requise pour fabriquer objets et infrastructure ? Le cycle d'obsolescence ultra-rapide ? Les consommations induites, locales et distantes ?
  - Il y a d'autres techniques pour économiser l'énergie, sans risque et durables.

- Quels usages **sociétalement** bénéfiques pour la « maison intelligente » ?
  - L'aide aux personnes en situation de handicap

    ou en perte d'autonomie, oui.

Où va-t-on ? Que veut-on ? (2)

- Des solutions de contrôle privilégiant les **traitements locaux** existent :
  - Snips, openHAB, Home Assistant.
  - En phase avec les approches « d'hébergement personnel et de réappropriation de ses données » (type Cozy Cloud ™)

- On a un certain contrôle dans sa maison, profitons-en !

“Make our home private again.”