Office of the
Privacy Commissioner
of Canada

L'Internet des objets

Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison

Rapport de recherche préparé par le Groupe des politiques et de la recherche du Commissariat à la protection de la vie privée du Canada

Février 2016

Table des matières

Résumé

Le présent rapport de recherche a pour objet d'aider les gens à comprendre l'incidence sur leur vie privée de la mise en réseau d'une multitude d'objets connectés d'usage courant qui sont dotés d'un identificateur unique — c'est-à-dire l'Internet des objets. Il est primordial de se pencher dès maintenant sur ces enjeux puisque l'innovation technologique rapide, la demande des consommateurs et la baisse des coûts favorisent le développement et l'adoption d'une nouvelle génération de capteurs à faible consommation d'énergie. Ces capteurs, intégrés aux biens de consommation et à l'infrastructure, peuvent accroître le risque de suivi et de profilage qui caractérise l'environnement actuel des appareils mobiles et des accessoires intelligents à porter sur soi. En l'absence de mesures de protection adéquates, ces nouveautés peuvent présenter des risques considérables pour notre vie privée.

Le présent rapport donne un aperçu des technologies de l'Internet des objets et explore plus particulièrement leur utilisation dans le commerce de détail et à la maison. Il aborde ensuite quelques défis liés à ce nouvel environnement dans l'optique d'enjeux précis liés à la protection de la vie privée : le profilage des consommateurs, la responsabilité, la transparence et l'éthique dans la collecte des données, les droits d'accès et de correction, le modèle de consentement actuel ainsi que les défis liés à la sécurité des appareils et de l'information.

Introduction

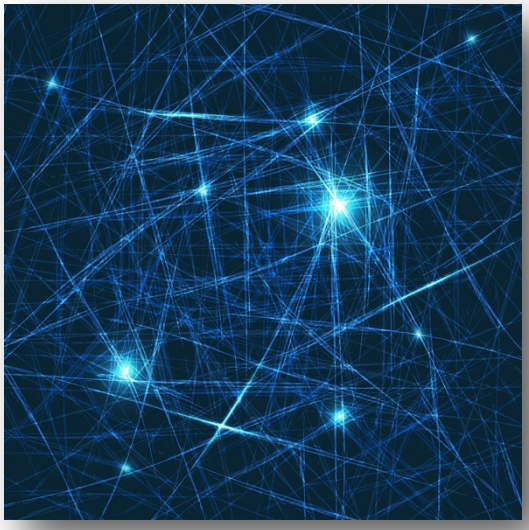
On a comparé l'Internet des objets à un réseau d'électricité[1] ou à un système nerveux planétaire[2] pour illustrer ce phénomène à la fois omniprésent et invisible qui fera partie intégrante de notre tissu social.

En général, l'expression « Internet des objets » désigne la mise en réseau d'objets physiques au moyen d'Internet. L'Internet des objets n'est pas un concept nouveau puisque les appareils communiquent entre eux depuis bon nombre d'années. Le phénomène actuel présente toutefois plusieurs caractéristiques nouvelles :

- les appareils électroniques et objets d'usage courant, en particulier les biens de consommation, sont de plus en plus conçus pour favoriser la communication interopérable au moyen de capteurs et de la connectivité Internet;
- les capteurs sont de plus en plus perfectionnés;
- les objets et les appareils ont la capacité de se connecter de façon invisible et de communiquer un large éventail d'information en ligne et hors ligne (notamment l'emplacement, des données biométriques, les achats effectués et l'historique de navigation en ligne);
- les appareils de l'Internet des objets sont maintenant abordables et accessibles pour les particuliers et les organisations de toutes les tailles, y compris les petites et moyennes entreprises (PME);
- toutes les organisations peuvent utiliser l'infonuagique et l'analytique des mégadonnées pour emmagasiner de l'information, la communiquer et tirer des conclusions sur leur clientèle.

Les gouvernements, les entreprises et les autorités de protection des données partout dans le monde tentent – avec raison – de prévoir les répercussions possibles de l'Internet des objets. Sur la scène internationale, plusieurs experts, intellectuels et concepteurs de technologies prévoient[3] de profondes transformations politiques, sociales et économiques, principalement au chapitre de la protection de la vie privée et de la surveillance. Des gouvernements en Europe[4] et aux États-Unis[5] ont entrepris des consultations publiques afin d'explorer les répercussions attendues. De nombreuses associations de l'industrie mènent actuellement des projets liés à l'Internet des objets[6]. De même, le groupe de travail Article 29 sur la protection des données, mis sur pied par la Commission européenne et composé de représentants des autorités européennes de protection des données, a adopté une opinion sur l'Internet des objets[7] dans laquelle il énumère un certain nombre de risques graves pour la vie privée et formule des recommandations détaillées pour gérer ces risques.

En se faisant l'écho de plusieurs des messages contenus dans l'opinion du groupe de travail Article 29, des autorités internationales de protection des données ont adopté la Déclaration de Maurice sur l'Internet des objets[8]. Dans cette déclaration, des organismes de réglementation ont formulé plusieurs observations et ont conclu que la quantité, la qualité et la sensibilité des données recueillies au moyen des capteurs sont si élevées que ces données devraient être considérées et traitées comme des données personnelles. Ils ont commenté les modèles d'affaires qui devraient selon eux découler de l'Internet des objets, en reconnaissant que la valeur de l'Internet des objets ne se trouve pas dans les appareils eux-mêmes, mais dans les nouveaux services connexes et les données qu'ils permettent de recueillir et de combiner. Les organismes de réglementation ont également mentionné que la transparence constitue une importante préoccupation et soutiennent que le consentement obtenu sur la base des politiques actuelles en matière de protection de la vie privée — souvent longues et complexes — ne sera probablement pas un consentement éclairé. Ils ont en outre exprimé de vives préoccupations concernant les défis en matière de sécurité que pose l'Internet des objets.



Les pratiques actuelles de profilage, de suivi et de ciblage des particuliers ou des groupes par des organisations de toutes sortes sont appelées à devenir plus nuancées, spécifiques et précises dans l'Internet des objets. Si un appareil est relié à nous d'une façon ou d'une autre, il devient un point de données qui peut être suivi et examiné par quiconque souhaiterait brosser un portrait de nos comportements[9]. Les entreprises chercheront à exploiter ces données pour élaborer de nouveaux modèles d'affaires et délaisser progressivement la seule vente d'« objets » de façon ponctuelle, par exemple des détecteurs de fumée à pile, au bénéfice de services payants à valeur ajoutée, par exemple la surveillance et la détection d'incendies à distance.

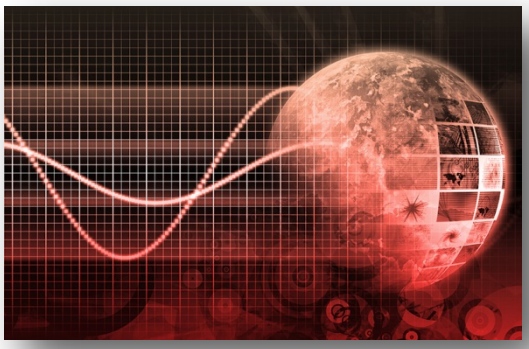
Les données générées par ces appareils, leurs interactions et leur capacité de révéler de l'information contiguë sur nos activités quotidiennes constitueront des éléments cruciaux de l'analytique des mégadonnées par les gouvernements et le secteur privé. Ces développements présenteront des défis de taille pour les cadres législatifs qui protègent la vie privée et la sécurité des renseignements personnels et pourraient permettre d'exercer une cybersurveillance et une surveillance physique parfaitement intégrées.

La communication d'information pertinente sur les risques pour la vie privée afin de permettre aux consommateurs de faire des choix éclairés demeure un défi dans l'espace mobile, en particulier en raison des petits écrans et de l'attention intermittente des utilisateurs, comme nous l'avons décrit dans notre document d'orientation à l'intention des concepteurs d'applications mobiles[10]. Dans le cas des accessoires intelligents à porter sur soi, que nous avons explorés dans un autre rapport de recherche[11], il est encore plus difficile de communiquer à l'utilisateur de l'information pertinente au moment voulu dans un format accessible et compréhensible. L'Internet des objets, dans lequel la capacité informatique pourrait devenir entièrement invisible à l'utilisateur, rend l'information sur les risques d'atteinte à la vie privée encore plus opaque et fait en sorte qu'il sera encore plus difficile d'obtenir un consentement éclairé.

1. Qu'est-ce que l'Internet des objets?

Il existe différentes définitions et représentations graphiques[12] de l'Internet des objets, qui comprennent pour la plupart les éléments suivants :

- des capteurs, appareils ou « objets » peu coûteux, répandus et dotés d'un identificateur unique;
- la capacité d'exécuter une commande ou de réagir à une commande;
- l'intégration à une infrastructure réseau dynamique mondiale ou à un « réseau de réseaux »;
- l'utilisation de protocoles de communication standard et interopérables;
- la connexion du monde physique au cyberespace;
- des « objets » physiques et virtuels qui ont des « identités, des caractéristiques physiques et des personnalités virtuelles »;
- des appareils qui communiquent sans intervention humaine et qui sont autoconfigurables;
- des appareils qui génèrent des données stockées dans le nuage et qui supposent le traitement, l'agrégation et l'analyse de données[13].



L'Internet des objets contient des éléments de différents degrés de complexité, allant de simples étiquettes d'identification à des communications complexes de machine à machine[14]. Les objets sont de plus en plus dotés de capacités informatiques et de capacités de communication qui permettent de

reproduire et de remplacer les observations et les sens humains dans le monde virtuel[15]. Les caméras de circulation mises en réseau et l'identification par radiofréquence des envois dans la chaîne d'approvisionnement sont des exemples bien connus. Des dispositifs de géolocalisation permettent maintenant de trouver nos clés d'autos[16], nos animaux[17] et même nos enfants ou nos parents âgés ou grands-parents[18]. La surveillance à distance de la température et de l'activité dans nos maisons est également de plus en plus courante. Nous commençons à porter des accessoires qui permettent de surveiller et de suivre notre niveau de forme physique et de produire un bilan de notre condition physique. Les compteurs d'électricité intelligents nous aident à suivre notre consommation à la maison. Les automobiles branchées détectent elles-mêmes leurs problèmes; elles peuvent recevoir de l'information sur la congestion routière et transmettre de l'information sur nos habitudes de conduite aux compagnies d'assurance, ce qui peut avoir une incidence sur nos primes.

Aperçu des technologies utilisées

L'Internet des objets utilise plusieurs technologies, notamment l'identification par radiofréquence (IRF), les communications en champ proche, la communication de machine à machine ainsi que les réseaux sans fil de capteurs et de positionneurs.

- L'IRF est une technologie fondamentale de l'Internet des objets qui sert principalement à suivre et à localiser des objets. Au cours de la dernière décennie, le Commissariat à la protection de la vie privée du Canada a produit[19] et financé plusieurs ressources sur les répercussions de l'IRF sur la protection de la vie privée. Cette technologie permet de relier entre eux toutes sortes d'objets inanimés que nous utilisons couramment[20].
- Les communications en champ proche peuvent être vues comme une évolution de l'IRF et consistent en un moyen à faible consommation d'énergie et de courte portée de transférer par la technologie sans fil de petites quantités de données entre des appareils[21].
- La communication de machine à machine renvoie généralement à l'Internet des objets pour les applications industrielles, opérationnelles et commerciales, tandis que l'Internet des objets proprement dit est analysé davantage sous l'angle des applications de consommation[22].
- Les capteurs sans fil sont différents des technologies d'IRF puisqu'ils mesurent des caractéristiques de notre environnement physique comme la pression, la chaleur et l'humidité[23].
- Les positionneurs transforment en actions l'information ou l'énergie provenant des capteurs, en les transmettant à un autre mécanisme ou système d'alimentation en électricité qui sert par

> « Compte tenu de la quantité phénoménale de données présentes dans l'Internet des objets, il ne fait aucun doute que l'Internet des objets, dans son ensemble, est de nature personnelle. Si vous pouvez consulter, relier et associer une identité et des activités dans l'Internet des objets, vous serez en mesure d'écrire une biographie que les mères de famille trouveront scandaleuse et qui brisera des mariages. Dans tous les cas. » [traduction]
>
> *The Privacy Engineer's Manifesto, 2014*

exemple à réchauffer ou à rafraîchir une pièce[24]. Aucune intervention humaine n'est nécessaire dans le processus décisionnel[25].

Les notes[26] qui se trouvent à la fin du présent rapport de recherche contiennent des ressources sur l'histoire[27] et le fonctionnement technique de l'Internet des objets.

Bien que l'expression « Internet des objets » comprenne le terme « Internet », la structure des réseaux désignés par cette expression est beaucoup plus diversifiée que celle d'Internet. Par exemple, un réseau maillé peut être un Internet des objets puisque chaque point de connexion ou nœud du réseau est connecté aux autres nœuds qui l'entourent au lieu de passer par un routeur central[28]. Toutefois, dans la plupart des maisons, le routeur sert de lien entre les appareils connectés à Internet et le monde extérieur[29].

Le traitement des données dans l'Internet des objets peut se faire de différentes façons; il peut être fait localement, dans l'appareil comme tel, ou à distance, ce qui suppose que l'information est envoyée pour être traitée dans des serveurs centralisés situés ailleurs. Lorsque des machines communiquent directement entre elles, un appareil recueille l'information au moyen d'un capteur. Ce capteur utilise ensuite un émetteur radio qui envoie les données dans un réseau filaire ou un réseau sans fil. Les réseaux sans fil peuvent être des réseaux cellulaires ou des réseaux qui utilisent la technologie satellite ou Wi-Fi pour les communications à grande portée, ou Bluetooth, ZigBee et l'IRF pour les communications à courte portée[30]. Une fois que les données arrivent à destination, elles peuvent être analysées et un autre appareil ou une personne peut poser une action en fonction de cette analyse[31].

Prévisions de croissance du marché

Les prévisions de croissance du marché de l'Internet des objets sont très favorables. Selon la recherche menée par la International Data Corporation sur 36 cas d'utilisation dans certaines industries au Canada, ces cas d'utilisation à eux seuls entraîneront des investissements de 6,5 milliards de dollars en 2018[32]. BI Intelligence estime que 1,9 milliard d'appareils d'usage courant et appareils industriels qui étaient auparavant inertes sont déjà connectés à Internet, qu'il s'agisse de parcomètres ou de thermostats résidentiels, et prévoit que ce nombre dépassera la barre des neuf milliards d'ici 2018[33]. Selon ABI Research, il y a plus de 10 milliards d'appareils connectés à un réseau sans fil dans le marché actuel, et plus de 30 milliards d'appareils devraient l'être d'ici 2020[34]. Cisco Systems prévoit que ces appareils seront au nombre de 50 milliards d'ici 2020, ce qui représente un marché de 15 milliards de dollars[35], tandis que Gartner prévoit que la valeur économique totale créée par l'Internet des objets sera de 1 900 milliards de dollars d'ici 2020[36]. Le McKinsey Global Institute affirme que l'Internet des objets pourrait avoir un impact économique de 2 700 à 6 200 milliards de dollars annuellement d'ici 2025[37] et que les ventes de capteurs ont progressé de 70 % par année depuis 2010[38].

Ces prévisions reposent sur un ensemble d'innovations et de changements[39] :

- l'émergence de technologies sans fil normalisées, de petite taille et à très faible consommation d'énergie;
- l'accès abordable à l'informatique mobile;

- la tendance observée chez les concepteurs d'applications à déplacer l'information de la couche application vers la couche réseau ou le nuage;
- l'amélioration des communications de machine à machine;
- la croissance des mégadonnées et de l'analytique, et l'essor du suivi de la santé et de la condition physique au moyen d'accessoires à porter sur soi[40];
- la croissance constante de la capacité et de la rapidité des réseaux à des coûts toujours plus bas;
- la personnalisation de l'expérience enrichie liée à l'utilisation des objets;
- la mise en œuvre de l'IPv6, ce qui permettra de fournir suffisamment d'adresses pour que tous les appareils puissent se connecter[41].

Toutefois, des observateurs de l'industrie ont relevé des obstacles importants à la mise en œuvre de l'Internet des objets[42] :

- le coût des capteurs et des positionneurs doit être assez bas pour favoriser une vaste utilisation;
- des normes d'interopérabilité et de sécurité doivent être mises en place pour les capteurs, les ordinateurs et les positionneurs[43];
- des solutions adéquates doivent être appliquées pour répondre aux préoccupations en matière de protection de la vie privée et de sécurité.

Les sections qui suivent présentent des exemples d'applications de l'Internet des objets dans le commerce de détail et à la maison.

2. Utilisations particulières dans le commerce de détail

La pratique de l'analytique dans le commerce de détail continue d'évoluer. Au moment de la rédaction du présent rapport, il était déjà possible d'analyser le comportement des consommateurs automatiquement, efficacement et discrètement. Les principaux facteurs qui favorisent cette évolution sont les appareils électroniques (téléphones intelligents, tablettes électroniques, etc.) que beaucoup de gens portent sur eux quand ils font des courses. Ces appareils émettent fréquemment de l'information en utilisant leurs interfaces radio (p. ex. les technologies cellulaires, Wi-Fi et Bluetooth), souvent à l'insu de la personne qui porte l'appareil ou sans son intervention. Cette information est très utile pour les détaillants qui souhaitent suivre et reconnaître les consommateurs lorsqu'ils se déplacent dans leur magasin ou qu'ils y reviennent à plusieurs reprises.

Les commerces de détail utilisent depuis longtemps différentes formes d'analytique pour recueillir des données sur les consommateurs pendant qu'ils magasinent. Les détaillants ont notamment recours à des observations dans le magasin, à l'analytique vidéo et au déploiement de faux clients, qu'ils combinent avec l'information que le consommateur soumet volontairement, notamment en répondant à des sondages sur la satisfaction de la clientèle. Les avancées technologiques font toutefois en sorte que les méthodes évoluent pour faciliter l'analytique au moyen d'importants ensembles de données recueillies automatiquement comme l'historique des achats, l'information recueillie au moyen des cartes de fidélité et les profils de consommateurs provenant de courtiers en données.

Le suivi dans l'Internet des objets peut aider une entreprise à gérer ses actifs, à effectuer le contrôle de ses stocks et à mieux aménager son magasin. Les renseignements plus détaillés obtenus peuvent servir à effectuer des analyses poussées à des fins de marketing et de profilage. Le suivi des appareils personnels mobiles (comme les téléphones intelligents) représente également pour les commerces traditionnels un

moyen amélioré de « connaître » les consommateurs qui se rendent dans leur magasin, un peu comme le font les commerçants virtuels et en ligne au moyen de témoins et d'autres technologies. Les techniques avancées de suivi et de profilage peuvent être utilisées de façon invisible, mettre à contribution des tiers à l'insu des particuliers et permettre un regroupement de l'information en ligne et hors ligne, comme les habitudes de déplacement (dans un magasin ou dans une ville), la navigation en ligne, l'historique des achats et l'activité dans les médias sociaux. Il est important que les personnes sachent dans quelle mesure leurs allées et venues, leur emplacement et leurs interactions courantes qui peuvent sembler normales font l'objet d'une surveillance lorsqu'elles entrent dans un magasin traditionnel ou en sortent.

Les appareils grand public et « objets » qui peuvent « communiquer » en permanence avec une entreprise peuvent transmettre de l'information de nature personnelle parfois délicate. Les détaillants s'intéressent particulièrement aux données que ces objets transmettent ainsi qu'à l'interaction des consommateurs et des détaillants qui peut avoir lieu lorsque les objets en question sont utilisés. Cette information peut être utilisée de différentes façons pour approfondir l'analyse des comportements des consommateurs et améliorer les pratiques commerciales. Selon une étude menée en 2014 sur le commerce de détail au Canada par Deloitte et commandée par le Conseil canadien du commerce de détail :

Le magasin n'est plus simplement un magasin, mais un point de convergence des opinions, des évaluations, des médias sociaux, de la technologie mobile, des attentes, de l'expérience, de la technologie et des attitudes, ce qui crée des connexions.[44]

C'est cette convergence des technologies qui rend possible l'omnicanal, et au cœur de ce processus se trouvent les données maîtresses. Les données, qu'elles portent sur des articles, des consommateurs ou des fournisseurs, doivent être structurées, analysées et disponibles pour avoir de la valeur.[45] [traduction]

Bien qu'un détaillant puisse disposer de plusieurs canaux pour joindre les consommateurs— par exemple, un emplacement physique, un magasin en ligne ou des sites de médias sociaux —, si tous ces canaux fonctionnent de façon indépendante, ils ne permettront peut-être pas de proposer aux consommateurs des prix, des promotions et un contenu uniformes. L'Internet des objets donne un moyen de produire des analyses détaillées à partir de l'interaction des consommateurs avec tous ces canaux et d'offrir des promotions et des campagnes de marketing uniformes dans toutes ces plateformes. La combinaison de données en ligne et hors ligne, y compris l'information provenant de l'activité d'applications mobiles, peut toutefois permettre de brosser un portrait détaillé des endroits où un appareil s'est trouvé, des magasins ou endroits fréquentés et des activités en ligne de l'appareil et de son utilisateur.

Le niveau détaillé des analyses en temps réel rendues possibles par l'Internet des objets contribue à sa valeur commerciale et économique, mais soulève également d'importantes questions en matière de protection de la vie privée qu'il faudra régler pour respecter les règles et les pratiques exemplaires en matière de protection de la vie privée et pour mériter la confiance des consommateurs.

La mise en évidence des répercussions possibles de l'Internet des objets sur la protection de la vie privée dans le commerce de détail ne signifie pas que ce concept est sans mérite. Elle permet plutôt de relever les éléments de base sur lesquels repose la confiance des consommateurs qui sont essentiels au succès des applications commerciales novatrices. Il s'agit également de sensibiliser les entreprises au fait que certains éléments d'information dans l'Internet des objets peuvent être considérés comme des renseignements personnels même si, à première vue, ils ne semblent pas correspondre à la définition traditionnelle de renseignements personnels.

Suivi et profilage par les commerces de détail

De nombreuses technologies permettent de suivre des appareils dans des commerces de détail et d'interagir avec eux. Le tableau qui suit donne un aperçu de ces technologies, qui varient au chapitre du rayon d'action et de l'exactitude de l'information de géolocalisation qu'elles fournissent.

Technologie	Description
Cellulaire	▪ La radio cellulaire offre une couverture de signal très vaste, habituellement à l'échelle des quartiers. ▪ Les appareils disposent d'identificateurs uniques qui les identifient dans le réseau de télécommunications.
Wi-Fi	▪ La technologie Wi-Fi suppose généralement des communications de portée moyenne, par exemple à l'intérieur ou dans les environs d'un immeuble. ▪ Si la technologie Wi-Fi d'un appareil est activée, l'appareil cherche constamment à se connecter à un réseau Wi-Fi. ▪ Lorsque cet appareil se trouve dans la portée d'un réseau Wi-Fi qu'un magasin (ou un tiers) a placé dans un établissement physique, l'adresse Media Access Control (MAC), qui est un numéro unique associé à l'appareil, peut être enregistrée. ▪ Par conséquent, si la technologie Wi-Fi d'un appareil est activée, des observations peuvent être faites et révéler quels appareils se trouvent dans un magasin. ▪ Les réseaux Wi-Fi peuvent aussi être présents dans des endroits publics comme des rues ou des centres commerciaux et peuvent servir à déterminer quels sont les magasins qui se trouvent à proximité de l'appareil ou qui sont souvent fréquentés par le propriétaire de l'appareil. L'information sur un appareil qui est recueillie par plusieurs réseaux Wi-Fi peut donner lieu à des observations détaillées ou permettre d'établir des tendances concernant la géolocalisation, la date et l'heure.
Technologie Bluetooth	▪ La technologie Bluetooth suppose généralement des communications de courte portée à l'échelle d'une pièce. Cette technologie a une portée plus restreinte que celle de la technologie Wi-Fi et nécessite moins de matériel que le suivi par Wi-Fi; elle utilise aussi moins de bande passante et peut transmettre les données plus rapidement que la technologie Wi-Fi[46]. ▪ Comme pour le suivi par Wi-Fi, on peut placer les balises (qui sont des capteurs) dans un magasin ou d'autres lieux publics pour recueillir par Bluetooth de l'information au sujet d'un appareil se trouvant à l'intérieur ou à l'extérieur du magasin. ▪ Pour qu'une entreprise amorce une communication bilatérale avec un appareil par Bluetooth, il faut qu'une personne ait posé une action, par

	exemple télécharger l'application d'un magasin. ▪ La technologie Bluetooth Low Energy (BLE) utilise la connectivité Bluetooth, mais permet une connexion plus rapide et plus économétique que Bluetooth. Elle s'active uniquement au moment de la connexion à un appareil; il s'agit donc d'une technologie optimale pour envoyer de façon périodique de petites quantités de données[47]. Les appareils BLE peuvent être alimentés pendant de longues périodes et conservent leur charge pendant une période pouvant aller jusqu'à un an[48]. ▪ Ce type de transmission à faible consommation d'énergie peut être utilisé dans l'équipement, les appareils électroménagers et les accessoires fixes.
Communications en champ proche et identification par radiofréquence (IRF)	▪ L'IRF utilise un signal radio pour transmettre de l'information d'une étiquette à un lecteur d'IRF[49]. ▪ Les communications en champ proche ont évolué depuis l'IRF et constituent une méthode à faible consommation d'énergie pour transférer de petites quantités de données entre des appareils. ▪ Les communications en champ proche et l'IRF nécessitent que les appareils soient situés à proximité pour pouvoir communiquer. ▪ Les communications en champ proche peuvent être utilisées pour de nombreuses applications, par exemple pour recevoir des coupons ou des promotions en présentant un appareil devant un panneau d'affichage ou une borne numérique. Cette technologie permet également d'effectuer des paiements par appareil mobile, c'est-à-dire qu'une personne qui possède un appareil pouvant utiliser les communications en champ proche peut simplement passer son appareil près d'un terminal de paiement sans contact.

Dans le commerce de détail, l'analyse peut se faire au moyen d'*observations* recueillies dans un magasin par des appareils et des capteurs installés dans le magasin ou à proximité de celui-ci. Il suffit qu'une personne passe près d'un magasin ou entre dans un magasin pour que de l'information sur son appareil soit recueillie à des fins de suivi ou de marketing. De plus, si des personnes effectuent un certain type d'*interaction*, par exemple télécharger une application ou se connecter au réseau Wi-Fi gratuit d'un magasin, des informations encore plus détaillées peuvent être obtenues de ces appareils. Voici quelques exemples du recours à l'analytique dans le commerce de détail qui supposent des modes passifs et interactifs à l'intérieur et à l'extérieur des magasins :

	Dans le magasin	À l'extérieur du magasin
Observation passive	▪ Suivi de l'emplacement au moyen de la radio à courte portée ▪ Analyse des comportements à court terme ▪ Utilisation de caméras vidéo pour analyser la circulation des consommateurs dans le magasin ▪ Détection et analyse des visages afin de personnaliser l'affichage numérique et les annonces	▪ Suivi de l'emplacement au moyen de la radio à moyenne et à longue portée ▪ Suivi à l'échelle des quartiers ▪ Analyse des comportements à long terme

Interaction active	▪ Télécharger une application pour recevoir des coupons pendant que le consommateur est dans le magasin ▪ Se connecter à un service Wi-Fi « gratuit » ▪ Effectuer une transaction par communication en champ proche (par exemple, un paiement par téléphone intelligent)	▪ Créer un périmètre numérique autour d'un magasin pour que les coupons puissent être transmis dès qu'un consommateur approche ▪ Lorsqu'une personne s'approche d'un commerce concurrent, lui envoyer un coupon pour l'attirer dans son propre magasin

L'Internet des objets dans le contexte du commerce de détail : cas d'utilisation

La présente section explore certaines des applications de l'Internet des objets auxquelles les consommateurs pourraient être exposés dans les commerces locaux qu'ils fréquentent. Ces exemples illustrent en quoi le profilage, la surveillance et le suivi sont des éléments clés qui ajoutent de la valeur au marketing, à la promotion de produits, à l'engagement des consommateurs et aux expériences des consommateurs.

Cette section montre aussi comment les détaillants et d'autres entreprises peuvent tirer des renseignements à partir de l'ensemble des comportements des consommateurs — passer devant un magasin, traverser un magasin, regarder des produits sur une étagère ou sur un téléphone intelligent et faire des achats[50].

A. Suivi passif en magasin

Certaines organisations installent des stations radio fixes et des capteurs qui permettent de recueillir les identificateurs uniques associés aux fonctions cellulaires, Wi-Fi et Bluetooth d'appareils grand public. Ces identificateurs peuvent être utilisés pour effectuer le suivi des sections d'un magasin dans lesquelles l'appareil a été localisé et des produits et articles dont l'appareil s'est approché. Ce type de suivi peut être effectué par le magasin lui-même ou par un tiers que la personne ne connaît pas.

La société Euclid Analytics offre ce genre de services d'analytique aux magasins et fait la promotion de ses produits de suivi par Wi-Fi sur son site Web :

> *Étant donné que les consommateurs n'ont pas à se brancher à votre réseau Wi-Fi ni à installer une application mobile, vous pouvez mesurer leur activité sans interrompre leur expérience de magasinage*[51].
>
> *Le Wi-Fi permet aux clients d'Euclid de mesurer les visites effectuées dans leur magasin, la durée de ces visites ainsi que les visites répétées, et de déterminer précisément les pratiques de marketing et les pratiques opérationnelles qui sont les plus efficaces pour générer des revenus*[52]. [traduction]

La société torontoise Aislelabs[53], qui propose des services similaires de suivi passif par Wi-Fi[54], offre des renseignements sur les personnes qui se trouvent à l'intérieur ou à l'extérieur des magasins, les clients nouveaux ou réguliers, les parcours des clients et la durée de leurs visites[55].

B. Suivi interactif en magasin

De nombreux magasins offrent à leurs clients la possibilité de se connecter à un réseau Wi-Fi gratuit ou d'interagir avec des stations Bluetooth situées dans le magasin. Si un consommateur a installé et activé l'application du magasin sur un appareil mobile, il peut également recevoir des offres et des promotions.

Par exemple, Philips vend maintenant des ampoules intelligentes qui peuvent être installées dans des magasins et se connecter aux téléphones intelligents des utilisateurs au moyen de balises[56]. Lorsque l'utilisateur télécharge l'application d'un magasin, les ampoules peuvent envoyer de l'information et des offres en fonction de la section du magasin où se trouve l'appareil, ce qui permet d'effectuer le suivi des habitudes et des préférences des consommateurs dans le magasin[57].

L'information sur l'appareil d'une personne et ses allées et venues peut être suivie par un magasin qui offre un service Wi-Fi gratuit ou des tiers avec lesquels le magasin est associé. Ce suivi permet parfois de combiner l'information de géolocalisation et celle sur les activités de recherche en ligne[58], les paniers d'achat virtuels[59] et les programmes de fidélité[60]. La quantité d'information recueillie peut être encore plus grande si la personne utilise son authentificateur d'un site de réseau social (comme un compte de réseau social) pour se connecter aux services Wi-Fi[61].

Une autre méthode de suivi actif consiste à utiliser des balises. Les balises sont des capteurs qui communiquent par Bluetooth avec un appareil doté de cette technologie. Elles peuvent servir à mesurer le nombre de visites d'un consommateur dans un magasin ou les sections où il passe le plus de temps, ce qui permet de déterminer les présentoirs qui sont probablement les plus efficaces ainsi que les promotions ou les coupons que le consommateur utilise[62]. Les services de balises nécessitent souvent qu'une personne télécharge une application sur son téléphone mobile, que ce soit l'application du magasin ou celle d'un tiers.

La société Shopkick offre aux détaillants une balise appelée « shopBeacon »[63], qu'elle présente comme suit sur son site Web :

> *ShopBeacon peut accueillir une cliente qui entre dans un magasin et lui présenter des offres, des rabais, des recommandations et des points de fidélité en fonction du lieu où elle se trouve, sans qu'elle ait à ouvrir une application. La balise peut également accorder des avantages en magasin en fonction de la navigation à domicile — si la cliente indique qu'elle « aime » un produit en particulier dans l'application, shopBeacon peut le lui rappeler lorsqu'elle entre dans le magasin qui vend ce produit. La balise peut également lui communiquer des offres concernant une section en particulier du magasin — par exemple, de manière à ce que l'offre sur les bottes qu'elle aime s'affiche au moment le plus opportun, c'est-à-dire lorsqu'elle se trouve dans la section des chaussures*[64]. [traduction]

Des médias ont indiqué que le détaillant canadien La Baie a mis en place un projet pilote axé sur la technologie des balises dans certains magasins du Canada. Selon une déclaration du vice-président directeur et chef du marketing, les balises servent à détecter les consommateurs qui ont téléchargé une application compatible sur leur téléphone intelligent et à interagir avec eux[65].

De plus, les mannequins dans les magasins peuvent être dotés de la technologie Bluetooth afin d'interagir avec l'appareil mobile d'une personne qui passe devant le mannequin[66]. Le consommateur qui a téléchargé une application peut interagir avec le mannequin et recevoir de l'information sur les

vêtements qu'il porte ou des indications sur la façon de faire un achat, communiquer l'information à des amis ou recevoir des offres connexes[67].

Les panneaux d'affichage numériques dans les commerces de détail sont également utilisés conjointement avec des balises, ce qui permet aux appareils mobiles dans lesquels l'application d'un magasin a été installée de fournir un contenu ciblé aux affiches numériques dans le magasin et de recevoir en même temps des offres personnalisées[68]. Ces balises peuvent également être conçues pour comprendre du contenu fondé sur les habitudes et les préférences d'un utilisateur en particulier[69] et l'historique de ses achats[70].

Des miroirs et des écrans dans les salles d'essayage peuvent permettre à des personnes d'essayer virtuellement des vêtements et de comparer différents ensembles en les affichant côte à côte. En plus d'aider une personne à prendre une décision d'achat, les images virtuelles peuvent être partagées dans les médias sociaux ou d'autres canaux de diffusion du magasin[71]. Le fondateur de MeMomi, qui propose un produit appelé MemoryMirror, aurait déclaré : « Puisque MemoryMirror "se souvient" de chaque interaction avec des clients, le produit permet aux détaillants du domaine de la mode d'offrir une expérience emballante en magasin, sur le Web et sur les plateformes mobiles, en plus de recueillir des données précieuses sur les comportements et les préférences des consommateurs[72]. » [traduction]

Les paiements par appareil mobile peuvent aussi intégrer l'ensemble de l'expérience d'un consommateur dans un magasin. Prenons l'exemple d'un restaurant qui associe les paiements par appareil mobile avec son système électronique de réservation et de commande. Toutes ces interactions peuvent être regroupées, enregistrées et suivies[73,74].

C. Suivi physique à tout endroit

Le suivi des activités des consommateurs et de l'endroit où ils se trouvent peut aussi être effectué à l'extérieur d'un magasin, par exemple dans l'ensemble d'un centre commercial, dans le quartier environnant ou dans la ville. Si les données recueillies par plusieurs magasins participants sont combinées, il est possible de créer un profil plus détaillé des comportements et des déplacements des consommateurs. De nouveaux services offerts par des tiers comportent des fonctions de suivi en magasin dans de nombreux emplacements et permettent de combiner et d'agréger les données pour créer des profils généraux.

Par exemple, des médias ont révélé que la société Turnstyle avait installé quelques centaines de capteurs dans des commerces de Toronto et fournissait à ses clients des renseignements sur les autres entreprises fréquentées par leurs consommateurs et sur les services auxquels ils avaient recours, ce qui permettait à ces commerces d'élaborer des campagnes de marketing fondées sur cette information[75]. Turnstyle affirme que cette information n'est associée à aucun nom en particulier; toutefois, elle est associée à une adresse MAC hachée[76].

Des médias ont aussi indiqué que cette forme de suivi effectuée par Turnstyle est possible pour *tout* appareil doté de la technologie Wi-Fi ou Bluetooth[77]. Turnstyle offre sur son site Web un lien qui permet de se soustraire à ce suivi en entrant l'adresse MAC de l'appareil à cette fin[78]. L'entreprise propose également aux entreprises traditionnelles un service Wi-Fi gratuit pour leurs clients, et lorsque des personnes se connectent en utilisant un compte de médias sociaux, elle est en mesure de recueillir le nom, l'âge, le sexe et les profils de médias sociaux de la personne[79].

Une autre entreprise torontoise, Via Interactive, utilise l'information provenant d'entreprises de téléphonie cellulaire pour effectuer un suivi « dans la rue ». L'entreprise affirme ce qui suit sur son site Web : « Nous sommes des spécialistes des données et nous croyons à la perspective de recueillir des données "invisibles" pour aider à donner un sens à toutes les actions – consommer, conduire, marcher, courir, observer, manger, acheter, etc. – qui ont lieu dans le "monde réel" »[80]. [traduction]

Des rapports indiquent que Via Interactive posséderait environ 50 millions d'éléments de données de géolocalisation afin de générer des profils de géolocalisation qui sont combinés à des données provenant des réseaux sociaux[81]. L'entreprise serait également en mesure d'utiliser des données cellulaires pour repérer l'emplacement des utilisateurs au mètre carré près[82]. Selon son site Web, elle propose notamment des données agrégées marquées géographiquement provenant d'information affichée dans les réseaux sociaux, des données agrégées se rapportant à la géolocalisation et au contexte provenant des accessoires intelligents à porter sur soi ainsi que des données « anonymisées » recueillies aux points de vente. Le site Web fait également état de « données de géolocalisation en temps réel riches et incroyablement révélatrices »[83]. [traduction]

SkyHooks, une entreprise d'analyse de données, propose une solution d'affaires qu'elle décrit ainsi sur son site Web : « Nous offrons des données contextuelles anonymisées sur le comportement de chaque utilisateur en fonction de son emplacement, ce qui permet de personnaliser le contenu, de créer des expériences en temps réel ou de cibler la publicité[84]. Elle ajoute que cette information peut être recueillie pendant que les utilisateurs vaquent à leurs occupations quotidiennes, qu'ils interagissent avec l'application d'une entreprise ou non[85]. SkyHooks utilise les données Wi-Fi, cellulaires et GPS pour ses services de géolocalisation[86].

Le « géorepérage », dans le domaine du marketing mobile, renvoie à la capacité d'un appareil de recevoir des notifications en fonction d'un secteur en particulier[87]. Il peut s'agir, par exemple, d'une personne qui télécharge une application et qui permet à cette application d'accéder aux données de géolocalisation de son appareil[88]; il peut même s'agir d'utiliser d'autre information, comme l'historique de recherche en temps réel[89]. Par exemple, une personne qui passe près d'un fleuriste pourrait recevoir une publicité ou des coupons pour l'achat de fleurs, ou une personne qui passe près d'un magasin participant pourrait recevoir des publicités sur des produits gratuits[90]. La géolocalisation pourrait même servir à diffuser des annonces visant à dissuader une personne d'entrer dans le magasin d'un concurrent[91].

Le géorepérage pourrait aussi servir à influencer les personnes d'un secteur en particulier en fonction de certains facteurs environnementaux. Une étude de cas réalisée par une association qui représente l'industrie de la publicité fait état d'un test de géolocalisation mené par Wal-Mart au Canada qui n'était pas fondé uniquement sur l'emplacement, mais aussi sur d'autres facteurs comme la météo et l'heure[92].

3. Utilisations particulières à la maison

Les technologies de l'Internet des objets sont maintenant mises à la disposition des consommateurs, qui les adoptent avec enthousiasme dans leur maison. On dit que les appareils « intelligents » connectés à Internet aux fins d'un usage résidentiel assurent sécurité et commodité. Les réfrigérateurs intelligents peuvent prévenir la détérioration des aliments, ce qui permet aux consommateurs d'économiser; les compteurs intelligents aident à gérer la consommation d'énergie; et la surveillance intelligente du domicile peut s'avérer un gage de sécurité. Par contre, tous ces appareils ont un coût sur le plan de la vie privée qui ne saute peut-être pas immédiatement aux yeux de ceux qui choisissent de les utiliser.

Le déploiement de technologies intelligentes dans les maisons suscite un enthousiasme considérable — et compréhensible — puisque c'est là que l'Internet des objets peut avoir les répercussions les plus profondes sur notre vie quotidienne. La possibilité d'installer un éventail de capteurs pour garantir notre sécurité personnelle et un fonctionnement efficient de nos maisons est certes intéressante. Toutefois, comme la Cour suprême du Canada l'a reconnu, « [i]l n'existe aucun endroit au monde où une personne possède une attente plus grande en matière de vie privée que dans sa "maison d'habitation" »[93].

De nombreux analystes considèrent 2014 comme l'année de l'avènement de la maison branchée : « Le marché de la domotique n'est pas nouveau; toutefois, ce qui est relativement nouveau, c'est sa grande notoriété principalement attribuable aux initiatives d'entreprises de sécurité et, plus récemment, de compagnies de télécommunications et de câblodistribution[94]. » [traduction] La « maison intelligente » est munie ou équipée d'une gamme de capteurs interconnectés qui relèvent des données externes — par exemple, la luminosité, la température, le mouvement, l'éclairage, la sécurité et le taux d'humidité de systèmes, entre autres ceux de chauffage — et d'appareils multimédias, ménagers, etc., qui peuvent être automatisés, surveillés et commandés au moyen d'un ordinateur ou d'un téléphone intelligent, même de l'extérieur de la maison, ou par Internet. La maison intelligente peut être le fruit d'une conception intégrée ou de l'amalgame de composantes interconnectées au fil du temps, peut-être en réponse à des besoins changeants ou à la technologie offerte sur le marché. La maison intelligente a pour but d'alimenter les occupants en données de pointe sur l'état de leur résidence et de leur permettre de contrôler les appareils connectés[95].

L'Agence européenne chargée de la sécurité des réseaux et de l'information envisage trois scénarios probables relativement à l'évolution de la technologie de la maison intelligente :

- une maison intelligente entièrement décentralisée, où chaque appareil est indépendant et utilise le réseau existant connecté à Internet dans la maison et transmet des données au fournisseur de services dans le nuage informatique;
- une maison dotée d'une connectivité locale active entre les appareils intelligents, sans l'utilisation d'une connexion vers des services infonuagiques et sans un portail central;
- une maison munie d'une plateforme centralisée dont le système logiciel central — accessible à partir d'un appareil central — coordonne tous les appareils intelligents et intègre leurs services afin de générer de la valeur ajoutée[96].

Les avancées actuelles se traduisent par une combinaison de ces scénarios à des degrés variés. Le marché des maisons intelligentes en est toujours à un stade embryonnaire, mais selon les prévisions, il devrait enregistrer une croissance exponentielle au cours des cinq prochaines années. Le marché mondial des maisons et des immeubles intelligents devrait croître à un taux annuel composé de 29,5 % entre 2012 et 2020[97]. En 2015, il est prévu que les consommateurs canadiens dépenseront 0,79 milliard de dollars en systèmes, appareils et logiciels pour maison intelligente. En juin 2014, les ménages canadiens possédaient dans l'ensemble 63 millions d'appareils connectés à Internet. Ce chiffre devait passer à 86 millions à la fin de 2015[98].

Nombre de ménages utilisent déjà des composantes d'une maison intelligente. On ne peut affirmer qu'il s'agit à proprement parler de maisons intelligentes et les appareils ne sont peut-être pas entièrement connectés de façon intrinsèque et invisible les uns aux autres et avec leurs utilisateurs, mais on peut d'ores et déjà affirmer que les premières étapes menant à une maison connectée ont pour la plupart été franchies. On prévoit également que les appareils ménagers intelligents modifieront en profondeur la manière dont les consommateurs achètent, gèrent, préparent et consomment la nourriture. Les analystes prévoient d'ailleurs que ce marché mondial connaîtra un véritable envol, passant de 613 millions de dollars en 2012 à environ 35 milliards en 2020.

L'Internet des objets à la maison : cas d'utilisation

A. Compteurs intelligents : connecter les maisons à des réseaux plus vastes

Bon nombre de maisons au Canada sont équipées de compteurs électriques intelligents permettant de mieux gérer la consommation et de réaliser des économies. Ces compteurs mesurent et enregistrent les périodes et les niveaux de consommation et transmettent ces données automatiquement à l'autorité de l'électricité. Ils permettent d'introduire la tarification en fonction de l'heure de consommation afin d'inciter les clients à modifier leurs habitudes et à utiliser l'électricité pendant les périodes creuses[99]. Ils sont de plus en plus utilisés, surtout pour résoudre les problèmes causés par un réseau électrique vieillissant[100]. Un autre avantage réside dans la facturation, qui est beaucoup plus précise lorsque la consommation est mesurée et transmise petit à petit — généralement toutes les heures, quoiqu'il arrive que ce soit toutes les dix minutes.

Les premières versions des compteurs intelligents ne permettaient que la communication unilatérale, du compteur à la compagnie offrant le service. Les modèles plus récents permettent également aux utilisateurs d'en apprendre davantage sur leur consommation d'énergie. L'Initiative du Bouton vert, projet pilote lancé en 2013 en Ontario, donne aux utilisateurs la possibilité de communiquer leurs données sur leur consommation à une tierce partie par l'entremise d'une application pour les aider à suivre de près leur consommation et à trouver des moyens de réaliser des économies[101]. Cette norme commune de données est actuellement adoptée dans d'autres régions de l'Amérique du Nord[102]. Les compteurs intelligents offrent une autre possibilité : avec le consentement de l'utilisateur, la compagnie d'électricité peut installer un dispositif lui permettant de moduler à distance la consommation d'énergie dans la maison pendant les périodes de pointe, par exemple en réglant les thermostats à quelques degrés de plus pendant une vague de chaleur, afin d'atténuer la pression sur le réseau électrique[103].

B. Systèmes de divertissement intelligents : en route vers une structure d'infodivertissement intégrée

Une télévision intelligente est une télévision qui peut se connecter à Internet pour avoir accès à des services de médias en continu et peut exécuter des applications de divertissement, comme des services

de location vidéo sur demande, des stations de musique Internet ou des navigateurs Web. Les modèles haut de gamme sont dotés de caméras vidéo intégrées, de microphones et de la reconnaissance vocale et gestuelle. Les télévisions intelligentes peuvent être intelligentes par elles-mêmes pour peu qu'elles comportent un microprocesseur interne et la connexion Internet, ou il peut s'agir de télévisions ordinaires que l'on rend intelligentes en les connectant à une boîte numérique comme Roku, Apple TV ou Fire TV donnant accès à Internet et aux services en continu. En 2013, on estimait que 25 % des ménages canadiens, soit un ménage sur quatre, possédaient déjà une télévision intelligente; on s'attendait à ce que cette proportion augmente pour atteindre 40 % d'ici 2015[104]. Le niveau de pénétration sur le marché de ces nouvelles télévisions intelligentes ou options intelligentes a tellement pris de l'ampleur qu'il est de plus en plus difficile de trouver des télévisions « ordinaires ».

La connexion des télévisions intelligentes à plusieurs autres appareils sans fil, comme des ordinateurs portables, des claviers sans fil, des souris, des téléphones intelligents et des tablettes, afin de faciliter la saisie de texte, la navigation, la navigation Web et le partage de contenu est vue comme une étape décisive vers une convergence de l'informatique et du divertissement. Elle donne également au consommateur la possibilité d'avoir accès au contenu recherché sur ses nombreux appareils au moyen d'un simple toucher — par exemple, regarder un film en passant d'un appareil à l'autre sans interruption, démarrer là où l'utilisateur avait interrompu l'écoute, ou afficher sans fil des photos contenues dans un téléphone intelligent sur l'écran de la télévision.

L'interconnectivité de la télévision intelligente est appelée à évoluer, et cette évolution pourrait l'amener à aller chercher du contenu à partir de n'importe quelle source (télévision, film, balado, médias sociaux), à analyser la consommation et les habitudes de visionnement, et à formuler des recommandations intelligentes ou à diffuser des annonces sur la base de l'analyse du contenu consommé sur tous les supports et toutes les plateformes[105].

C. La surveillance de la maison à même le téléphone intelligent

Les systèmes de sécurité sont une autre technologie de la maison intelligente qui gagne rapidement en popularité chez les consommateurs. Aux entreprises de sécurité résidentielle bien établies qui mettent à jour leurs produits viennent s'ajouter de nouveaux joueurs sur ce marché, notamment des fournisseurs de services de télécommunications locaux, des développeurs indépendants et des géants comme Google et (bientôt) Apple[106], qui nivellent le marché et se disputent une part de ce marché en plein essor.

Par le passé, seules les entreprises commerciales, comme les banques, les entrepôts et les aéroports, utilisaient des systèmes de surveillance[107]. La technologie ayant évolué et les prix ayant chuté, il est devenu possible d'installer dans une résidence un réseau de caméras de surveillance en temps réel et de haute définition qui est surveillé soit par une tierce partie (comme des entreprises de sécurité et de télécommunications), soit par les propriétaires eux-mêmes au moyen d'applications sur leurs téléphones intelligents. Peu importe l'appareil ou le système choisi, les fonctions habituellement offertes comprennent des serrures de porte intelligentes, des ouvre-porte de garage, des caméras vidéo, la vision nocturne, des capteurs sur les portes et les fenêtres, et des détecteurs de mouvement, d'incendie et de température. Les systèmes de sécurité peuvent être surveillés par les propriétaires — dits autosurveillés — ou par une tierce partie, par exemple une entreprise de télécommunications ou de sécurité résidentielle. Les systèmes autosurveillés sont équipés d'un système de communication bilatéral entre le système et l'utilisateur, et les données recueillies peuvent également être conservées dans le nuage. Les systèmes surveillés par une tierce partie, quant à eux, sont installés par une entreprise de sécurité ou de télécommunications à qui ils renvoient certaines données. Certaines entreprises font

équipe avec des fournisseurs de services d'analyse de données afin d'offrir des avis ou des solutions plus personnalisés selon l'utilisateur.

Aux États-Unis, ceux qui choisissent d'installer ce genre de systèmes peuvent bénéficier de primes d'assurance habitation moins élevées du fait que leur résidence risque moins d'attirer les criminels[108]. Cela suppose que ces systèmes sont à la vue de tous, que ce soit par des caméras visibles à l'extérieur de la maison, des affiches promotionnelles plantées sur les pelouses ou des autocollants apposés dans les fenêtres indiquant qu'un système de surveillance est en place. Cela dit, il est également possible d'installer de petites caméras qui se dissimulent bien pour surveiller à leur insu les gens et leurs activités dans la maison ou à proximité. La caméra utilisée pour surveiller les gardiennes d'enfants, habituellement de petite taille et dissimulée à l'intérieur d'une poupée, en est un bon exemple. La « caméra judas », quant à elle, peut photographier quiconque s'approche à une certaine distance, qu'il s'agisse de visiteurs, de messagers, de vandales ou de cambrioleurs. Des modèles de caméra plus récents peuvent être activés par le mouvement et programmés pour envoyer un courriel ou un texto d'avertissement vers un téléphone intelligent lorsque la caméra est activée[109].

D. Appareils ménagers intelligents : l'électronique qui parle

Le marché des appareils ménagers intelligents est encore à un stade embryonnaire. L'efficacité énergétique étant de plus en plus un moteur d'innovation, on accorde beaucoup d'importance à la connexion des appareils ménagers intelligents au réseau des compteurs intelligents afin d'optimiser la consommation d'énergie des ménages, de sorte que les appareils consommant beaucoup d'électricité, comme la laveuse ou la sécheuse, puissent être mis en marche à distance en dehors des périodes de pointe[110].

Certains appareils ménagers intelligents, comme les réfrigérateurs, sont munis de capteurs qui détectent la fraîcheur des aliments, puis tiennent les utilisateurs informés au moyen de messages textes pour les aider à gérer et à acheter les aliments[111]. Un autre scénario, qui nécessite toutefois une interconnectivité des appareils, suggère par exemple qu'un utilisateur regardant une émission de cuisine pourrait envoyer l'information relative à une recette intéressante au réfrigérateur au moyen d'une télévision intelligente. Le réfrigérateur enregistrerait alors la recette, puis vérifierait s'il contient les aliments nécessaires. Si l'utilisateur a tout ce qu'il faut pour faire la recette, il pourrait alors démarrer le four à distance pour le préchauffer[112]. S'il manque des ingrédients, le réfrigérateur pourrait envoyer une liste des ingrédients manquants à une épicerie en ligne.

Une autre technologie qui fait son entrée sur le marché des maisons haut de gamme est le dosseret numérique, qui remplace le dosseret traditionnel dans la cuisine et permet à l'utilisateur de se connecter à son système de caméra, de faire afficher des photos et de l'art ou de se connecter à Internet au moyen d'écrans tactiles[113].

Les cuisines et les appareils ménagers intelligents prendront sans doute quelques années à bien s'établir dans les foyers, car les choix d'appareils sont limités, les prix demeurent exorbitants pour le consommateur moyen et, plus important encore, la valeur ajoutée de ces appareils n'a pas encore été bien définie et vantée au consommateur.

E. La maison intelligente et « sûre » au service d'un mode de vie indépendant

Outre les usages évidents des systèmes de surveillance résidentielle sur le plan de la sécurité, la population vieillissante et les pressions exercées sur les systèmes de soins de santé font de la surveillance une option viable pour s'assurer que les personnes à risque, comme les personnes handicapées ou âgées, peuvent demeurer à la maison en toute sécurité. Le concept « vieillir chez soi », qui désigne le fait de vieillir dans sa maison plutôt que dans un établissement institutionnel, est désormais plus réalisable grâce, notamment, aux systèmes de surveillance à domicile permettant de connecter électroniquement les personnes âgées avec les services de soins de santé ou les personnes soignantes[114]. Ces systèmes et capteurs peuvent surveiller les schémas de comportement pour détecter les chutes, déterminer si une démence est apparue ou en progression et suivre de près les habitudes de sommeil. Les périodes d'attente pour avoir accès aux établissements avec services de soutien s'allongeant sans cesse[115], les systèmes de surveillance sont de plus en plus populaires au Canada, particulièrement les systèmes activés par des capteurs, qui peuvent être vus comme moins envahissants que les systèmes de caméras[116].

Les appareils ménagers connectés pourraient changer complètement la donne pour les personnes handicapées[117]. L'installation de réseaux de capteurs sans fil ou d'appareils ménagers activés par la voix à l'intérieur de la maison peut remplir plusieurs fonctions pour offrir une certaine autonomie dans la vie de tous les jours. Il peut être très utile pour les personnes à mobilité réduite de pouvoir contrôler les appareils ménagers à distance, voir qui est à la porte et régler le thermostat à l'aide de leur téléphone intelligent. Des capteurs placés sur le corps peuvent interagir avec des capteurs environnementaux placés dans la maison pour signaler les chutes ou autres incidents à une personne soignante, activer la climatisation si la température interne du corps dépasse un certain seuil, ou rappeler aux patients de prendre certains médicaments[118]. Lorsque le coût de ces systèmes et appareils diminuera, il est fort probable que leur utilisation se répandra.

4. Répercussions sur la vie privée

Dans un monde où nos activités et nos comportements quotidiens sont appelés à être de plus en plus mesurés, enregistrés et analysés, il est urgent que les concepteurs et les décideurs réfléchissent à la manière d'informer les consommateurs et les citoyens afin qu'ils sachent qui recueille leurs renseignements personnels, quels renseignements personnels sont recueillis, la manière dont ils sont conservés, utilisés et communiqués, à qui ils sont communiqués, et à quelles fins. Selon les principes de protection de la vie privée, les utilisateurs devraient pouvoir exercer un contrôle sur leurs données et choisir de se soustraire à l'environnement « intelligent » sans pour autant subir de conséquences négatives. Comment cela se déroulera-t-il et comment respectera-t-on les principes traditionnels de protection de la vie privée?

Avant d'adopter trop rapidement des appareils et des capteurs intelligents pouvant envoyer dans le nuage des renseignements sur plusieurs aspects personnels de notre vie quotidienne, il est impératif d'avoir une discussion éclairée sur les répercussions de l'Internet des objets et de planifier l'intégration des principes de protection de la vie privée et de mesures de protection dans la conception et la mise en œuvre des nombreuses composantes d'un environnement intelligent.

Les capteurs intégrés aux objets interconnectés peuvent générer une quantité impressionnante de renseignements qu'il est possible de combiner et d'analyser et à partir desquels on peut prendre des mesures, peut-être en l'absence de la responsabilité, de la transparence et de la sécurité appropriées ou d'un consentement valable des intéressés.

Identifiabilité des données de l'Internet des objets

Dans certains cas, on dit que le suivi des appareils met en jeu des renseignements qui sont agrégés, anonymisés ou désidentifiés[119]. De façon générale, les renseignements agrégés peuvent être considérés comme des données compilées ou statistiques ne permettant pas d'identifier la personne à laquelle elles se rapportent[120]. Toutefois, des études ont montré que même les renseignements agrégés peuvent permettre d'identifier une personne[121]. Certains soutiennent que l'information en jeu dans l'environnement de l'Internet des objets est anonymisée ou pseudonymisée, mais il est difficile d'anonymiser complètement l'information dans ce contexte[122]. Comme le groupe de travail Article 29 l'a fait remarquer, même les données anonymisées ou pseudonymisées pourraient devoir être considérées comme des renseignements personnels[123].

Si la collecte de données dans l'Internet des objets suppose le suivi d'un appareil, le but consiste toutefois à comprendre le comportement de la personne derrière l'appareil. En fait, la véritable valeur de cette collecte de données réside dans les renseignements précieux recueillis au sujet de la personne, de ses activités, de ses déplacements et de ses préférences. Lorsque des déductions sont faites au sujet du propriétaire d'un appareil, il y a lieu de se demander si c'est l'appareil qui est suivi ou si c'est la personne. La Commission européenne, dans l'un de ses rapports, conclut que les objets dans l'Internet des objets peuvent devenir une forme d'extension du corps et de l'esprit humains comportant des fonctions perfectionnées, comme une intelligence et un savoir intégrés[124]. Par ailleurs, les schémas de données de géolocalisation sur une longue période se rapportant à un appareil en particulier pourraient révéler de l'information sur le lieu où l'appareil se trouve à certaines périodes du jour ou de la nuit et, par ricochet, le lieu où une personne travaille ou habite[125].

En 2013, l'organisme américain Future of Privacy Forum a publié un code d'éthique à l'intention des compagnies d'analytique des données de géolocalisation mobile qui offrent à des entreprises des services d'analyse des données de géolocalisation des consommateurs[126]. Selon le code, ces compagnies ne sont pas autorisées à recueillir des renseignements personnels ou des renseignements relatifs à un appareil en particulier, à moins que ces renseignements ne soient rapidement désidentifiés ou dépersonnalisés ou que le consommateur n'ait donné un consentement affirmatif[127]. Bien qu'il soit reconnu dans le code qu'une adresse MAC hachée peut être considérée comme un élément d'information dépersonnalisé[128], le Future of Privacy Forum a souligné qu'« […] il est important de comprendre que le code ne prétend **PAS** que le hachage des adresses MAC constitue un processus de désidentification qui répond à toutes les

préoccupations relatives à la protection de la vie privée » [traduction] (le caractère gras et les majuscules se trouvent dans l'original) [129].

Le hachage est un processus qui permet de convertir un numéro en un nouveau numéro unique appelé « valeur de hachage »[130]. Comme l'a noté l'organisme américain Electronic Frontier Foundation, l'une des limites du hachage est le fait que, par définition, hacher la même valeur produit toujours le même résultat[131]. Par conséquent, le fait de hacher un numéro unique, comme une adresse MAC, ne rend pas nécessairement l'information vraiment anonyme ou n'élimine pas complètement le risque que l'identité soit récupérée, une conclusion à laquelle sont également arrivés le Commissariat à la protection de la vie privée du Canada[132] et des experts en matière de technologie [133]. Selon TRUSTe, entreprise qui attribue une marque de confiance en matière de respect de la vie privée, dans certains cas, on conserve les données hachées dans le seul but d'identifier un utilisateur discret lorsqu'il reviendra sur le site[134].

À ce jour, les tribunaux se sont prononcés à diverses reprises sur les circonstances dans lesquelles un renseignement concerne un individu identifiable et, par conséquent, peut être considéré comme un renseignement personnel. Par exemple, selon un jugement de la Cour fédérale[135], un renseignement concerne un individu identifiable lorsqu'il y a de fortes possibilités qu'un individu puisse être identifié par l'utilisation de ce renseignement, que celui-ci soit pris seul ou en combinaison avec d'autres renseignements disponibles.

Plus récemment, la Cour suprême du Canada a jugé[136] qu'il y a une attente raisonnable en matière de respect de la vie privée en ce qui a trait aux renseignements d'un abonné en lien avec son activité Internet, car ces renseignements peuvent constituer la clé permettant l'accès à des détails délicats sur les activités en ligne de l'abonné et devraient par le fait même être protégés par la Constitution. Cette décision indique qu'il ne suffit pas d'examiner chaque élément d'information séparément, mais qu'il faut aussi examiner ce que les données peuvent révéler, comme des détails potentiellement intimes au sujet des modes de vie et des choix personnels qui peuvent être déduits à partir des données[137].

Le Commissariat a montré dans une autre étude qu'il est possible de glaner des renseignements très utiles sur une personne à partir de données comme les adresses IP[138]. Dans un autre rapport de recherche, intitulé *Métadonnées et vie privée — Un aperçu technique et juridique*[139], il conclut que les métadonnées (des données qui fournissent de l'information à propos d'autres données) peuvent en révéler beaucoup au sujet d'une personne et devraient donc faire l'objet de mesures de protection de la vie privée, tout en reconnaissant qu'il importe de tenir compte du contexte. De plus, comme nous l'avons vu dans le rapport de recherche du Commissariat sur l'analyse prédictive[140], on observe dans le domaine de la protection de la vie privée une série de problèmes nouveaux causés par le regroupement de quelques renseignements personnels ici et là à première vue inoffensifs et non sensibles. Combinés, ces renseignements permettent d'en apprendre beaucoup plus sur les comportements personnels[141]. Grâce à ces travaux, nous comprendrons mieux les vérifications, les contrôles et les processus adéquats qui pourraient devoir être mis en place dans l'environnement de l'Internet des objets.

La question de savoir ce qui constitue un renseignement personnel prend toute son importance lorsqu'il y a à la fois une collecte de données en ligne et hors ligne. Il arrive que des organisations affirment ne pas recueillir de renseignements personnels comme les noms et les adresses, mais recueillent les adresses MAC ou d'autres identificateurs qui pourraient être considérés comme étant des renseignements personnels, tout dépendant du contexte et des autres données recueillies[142].

En outre, il existe des modèles d'affaires dans le secteur du commerce de détail qui combinent et agrègent des données recueillies en ligne et hors ligne afin d'élaborer des profils de consommateur. S'il est vrai que ce genre de profil peut être créé à l'aide de renseignements agrégés ou désidentifiés, la quantité de renseignements détaillés qui peut être obtenue à partir d'appareils omniprésents et en activation constante amplifie la portée, l'étendue et la sensibilité potentielle de l'information recueillie. La combinaison de données de géolocalisation et de renseignements recueillis en ligne et hors ligne liés à l'historique d'achat et à la navigation sur Internet pourrait brosser un portrait détaillé d'une personne, fournissant notamment des renseignements de nature sensible sur ses finances, ses achats ou ses intérêts.

Par exemple, le *Wall Street Journal* a décrit une étude réalisée par le Massachusetts Institute of Technology (MIT) dans le cadre de laquelle des renseignements désidentifiés ont été recueillis à partir d'achats effectués par carte de crédit par 1,1 million de personnes; dans 90 % des cas, il a été possible de remonter aux habitudes d'achat particulières en comparant l'activité à d'autres renseignements accessibles au public sur LinkedIn, Facebook, Twitter et Foursquare[143].

La responsabilité à l'ère des machines

La responsabilité est un principe clé de la législation sur la protection de la vie privée. Une organisation responsable doit être en mesure de montrer ce qu'elle fait et a fait des renseignements personnels à sa disposition et d'en expliquer la raison. Cela peut être plus facile à dire qu'à faire dans l'environnement de l'Internet des objets où il y a une multitude d'intervenants, comme les fabricants d'appareils, les plateformes sociales et les applications de tierces parties[144]. Certains de ces intervenants recueillent, utilisent ou communiquent peut-être des données et peuvent jouer un rôle plus ou moins important dans la protection de cette information à divers points de la chaîne. Cependant, il est parfois difficile de distinguer ces intervenants, même dans une situation idéale. Par exemple, qui est ultimement responsable des données transmises par le compteur intelligent? Le propriétaire de la maison qui utilise l'appareil, le fabricant ou la compagnie d'électricité qui le fournit, la compagnie tierce qui conserve les données, l'entreprise qui traite les données, tous ces intervenants ou une combinaison de certains d'entre eux? À qui un consommateur pour qui la protection de la vie privée est importante doit-il s'adresser pour se plaindre? Dans l'éventualité d'une atteinte à la vie privée, où la responsabilité d'une partie prend-elle fin et où la responsabilité d'une autre commence-t-elle? Il pourrait être utile de schématiser les flux de données dynamiques et de définir les responsabilités des différents intervenants ainsi que les relations entre chacun pour clarifier la manière dont l'information circule entre les parties et jeter les fondements d'un programme de gestion de la vie privée d'une organisation.

Dans le cas des décisions « prises mécaniquement », il pourrait être encore plus difficile pour les concepteurs et les propriétaires des algorithmes, des systèmes et des produits sous-jacents de montrer qu'ils sont responsables[145]. Outre cette question épineuse, les responsabilités juridiques et éthiques en cas d'erreurs ou d'accidents sont loin d'être évidentes[146]. La portée des programmes de gestion de la vie privée et le niveau de responsabilité auquel on est en droit de s'attendre des organisations seront complexes dans l'environnement de l'Internet des objets.

La transparence et l'éthique dans la collecte des données

Dans l'Internet des objets, les appareils sont souvent conçus pour fonctionner en silence et se fondre à notre environnement, si bien que nous ne savons pas toujours qu'ils sont là. C'est pourquoi il peut être difficile de savoir les renseignements à notre sujet qui sont recueillis, utilisés et communiqués par nos appareils dans un réseau de capteurs. Il sera également sans doute difficile pour nous de savoir qui tire parti des renseignements recueillis par ces appareils. Bien que les modèles d'affaires pour l'Internet des objets en soient toujours au stade embryonnaire, les observateurs de l'industrie voient des possibilités liées au développement de services axés sur les *données* recueillies grâce à ces appareils, plutôt qu'à la vente des appareils en tant que telle.

Prenons, par exemple, les questions entourant la transparence dans la collecte des données à l'intérieur même de notre maison, c'est-à-dire l'endroit où nous passons la plus grande partie de notre temps lorsque nous ne sommes pas au travail ou à l'école. C'est également le lieu que nous considérons comme le plus intime. Pourtant, l'introduction d'appareils connectés modifiera forcément en profondeur la manière dont nous menons notre vie privée. Certains risques tirent leur son origine de l'utilisation répandue d'appareils et de réseaux sans mesures de sécurité adéquates. D'autres émanent de l'information recueillie, de ceux qui y auront accès et des fins auxquelles elle sera utilisée.

Dans le secteur du commerce de détail, les méthodes passives de suivi en magasin et de profilage incitent à s'interroger sur la façon dont les personnes sont informées des fins auxquelles leurs renseignements personnels sont recueillis, la mesure dans laquelle les pratiques de gestion de l'information employées par tous les intervenants concernés sont transparentes, ainsi que la manière dont les personnes sont avisées de ces pratiques et dont ces communications leur sont présentées afin qu'elles donnent un consentement valable. Compte tenu de l'utilisation de petits appareils électroniques portables, la *manière* dont l'information est communiquée aux personnes est également un facteur important à prendre en compte.

Le Future of Privacy Forum, dans son code d'éthique à l'intention des compagnies d'analytique des données de géolocalisation mobile, demande que soient affichés dans les magasins des avis visibles informant les clients de ces pratiques et de la manière dont ils peuvent choisir de participer — ou de ne pas participer. L'organisme ajoute que ces avis ne doivent pas se limiter à des avis physiques[147]. Les entreprises doivent fournir un lien menant à un site Web sectoriel central qui comprend un service centralisé permettant de se soustraire au suivi. Leurs sites Web peuvent également fournir un lien menant au formulaire de refus d'une entreprise[148]. Cependant, compte tenu de la nature passive de ce type de surveillance, il est important que l'information sur la possibilité d'exercer ce droit de refus soit mise en évidence et facile à trouver. Selon l'approche actuellement utilisée au sein de l'industrie, pour refuser la transmission de ses renseignements personnels, l'utilisateur doit saisir manuellement une adresse URL compliquée ou une adresse MAC longue et complexe, processus qui peut ne pas être simple ou facile pour certaines personnes.

Aux États-Unis, la Federal Trade Commission (FTC) a intenté un recours contre Nomi Technologies Inc. (Nomi), entreprise qui installe des capteurs dans les établissements de clients traditionnels pour suivre à la trace les personnes qui entrent dans ces magasins ou passent devant[149]. Bien que la FTC ait noté que Nomi offrait une option de refus sur son site Web, aucun avis n'était affiché dans les magasins en question pour informer les personnes de leur droit de refus ou même qu'une telle pratique avait cours dans ces magasins. La FTC a également noté que même si Nomi hache les adresses MAC, le processus donne malgré tout lieu à un identificateur qui est unique à l'appareil mobile d'un client et peut être suivi au fil du temps[150]. En avril 2015, par suite des accusations de la FTC qui pesaient contre elle, Nomi s'est

engagée à offrir une option de refus en magasin et à informer les personnes lorsque les lieux où elles se trouvent sont équipés de ses technologies de suivi[151].

Le Commissariat à la protection de la vie privée du Canada, dans son document d'orientation sur les accessoires intelligents, note qu'il existe des difficultés relativement au mode de consentement actuel dans un monde où les appareils informatiques et mobiles sont omniprésents et qu'« il faut faire davantage pour montrer aux utilisateurs, de manière créative et intelligible, à quoi servent réellement leurs renseignements personnels »[152].

Il dit, elle dit, la machine dit : droits d'accès et de correction

Les droits d'accès et de correction sont directement liés à la responsabilité et à la transparence. Comment une personne saura-t-elle qu'elle doit demander les renseignements qui lui appartiennent et contester leur exactitude si elle n'a jamais su que les renseignements étaient recueillis? De même, comment une personne saura-t-elle vers quelle organisation se tourner pour avoir accès à ses renseignements personnels et, au besoin, les corriger?

Les lois canadiennes sur la protection des renseignements personnels qui s'appliquent tant au secteur public qu'au secteur privé reposent en grande partie sur le processus de plainte, qui est un mécanisme offert pour aider les individus à contester les décisions organisationnelles prises à leur sujet. Ce modèle est efficace lorsque l'on connaît l'organisation à contacter ou que l'on dispose d'une liste de banques d'information[153], mais perd toute efficacité lorsqu'il est difficile d'établir quelle organisation a recueilli les renseignements. De quelle façon pourrions-nous schématiser efficacement les flux de données dynamiques et les rendre explicites et transparents pour tous afin que nous puissions exercer de manière plus significative nos droits d'accès et de correction?

Difficultés inhérentes au modèle de consentement actuel

La collecte de données au moyen d'appareils dans l'environnement de l'Internet des objets peut souvent être imperceptible et c'est pour cette raison que nous avons du mal à bien comprendre cette pratique ou à évaluer la manière dont elle se manifeste. Cet état de fait a des répercussions évidentes sur l'obtention d'un consentement valable.

Le consentement binaire et unique ainsi que les définitions traditionnelles de « renseignements personnels » sont de plus en plus perçus comme étant dépassés, car ils font référence à une décision prise à un moment précis dans le passé, dans des circonstances particulières et liée au contexte initial dans lequel elle a été prise. Les politiques de gestion des données personnelles simplistes qui reposent sur l'obtention d'un consentement ou d'un refus (« oui » ou « non ») ne sont peut-être pas assez souples ou appropriées dans un environnement connecté qui évolue à un rythme effréné[154].

Le Commissariat a relevé des difficultés associées au modèle de consentement et en a fait un enjeu dans le cadre de sa priorité intitulée « L'économie des renseignements personnels ». Il a adopté une stratégie pour déterminer, étudier et valider les améliorations à apporter au modèle de consentement afin de tenir compte des préoccupations soulevées autant par les personnes que par les organisations.

Il existe plusieurs options intéressantes pour surmonter les difficultés inhérentes au mode de consentement dans l'environnement de l'Internet des objets. Le Commissariat en examinera un bon nombre, comme l'établissement de règles en fonction de l'appareil aux fins de prise de décision par procuration[155] ou la programmation d'un appareil afin qu'il « apprenne » les actions qui sont acceptables

(ou non) pour les utilisateurs à des moments et dans des endroits donnés[156], dans ses travaux à venir sur le consentement.

D. Collecte, utilisation et communication d'information dans la maison

Les dispositifs intelligents résidentiels peuvent eux aussi en révéler beaucoup sur le nombre de personnes qui vivent dans la maison, leurs habitudes quotidiennes et les changements dans leur routine. Dans le cas des compteurs intelligents, on craint que le déploiement à grande échelle ait mis l'accent sur l'économie d'énergie au détriment de la protection de la vie privée. En l'absence d'un cadre qui donne clairement au consommateur le choix et le contrôle et qui fixe des règles strictes en matière de collecte, d'utilisation et de communication des données, l'information obtenue pourrait être utilisée aux fins d'exploration de données, de réclamation d'assurance ou de litige, pour ne nommer que quelques-uns des usages secondaires potentiels. Les commissariats à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Ontario ont publié des rapports qui abordent en détail les problèmes que posent les compteurs intelligents au chapitre de la protection de la vie privée.

En ce qui concerne les appareils ménagers ainsi que les systèmes de divertissement et de surveillance résidentielle intelligents, un certain nombre de problèmes relatifs à la protection de la vie privée ont déjà été relevés d'après l'expérience des premiers utilisateurs. Lorsqu'ils sont connectés au compteur intelligent et au réseau électrique, les appareils ménagers intelligents fournissent encore plus de données granulaires sur l'identité des personnes qui les utilisent, l'usage qui est fait de chacun d'eux, les habitudes de divertissement et la présence ou l'absence de certaines personnes dans la maison. Les dispositifs intelligents pour la maison et leurs applications connexes transmettent également des renseignements à leurs fabricants, et on ne sait trop les fins auxquelles ces derniers destinent ces données et à qui ils les communiquent. Les dispositifs activés par la voix, s'ils sont réglés en « mode activation », pourraient transmettre aux fabricants des conversations entre utilisateurs. Si l'information est transmise par l'entremise de téléphones intelligents, les fournisseurs de services Internet auront accès à ces données, qui pourraient être communiquées aux autorités chargées de l'application de la loi en réponse à des demandes d'accès légal. Enfin, il convient de noter qu'à mesure que les appareils et dispositifs intelligents deviendront la norme, on assistera de plus en plus à une « érosion du choix » pour les personnes qui auraient préféré leurs versions « non intelligentes ».

Piratage de l'Internet des objets

Les consommateurs et les organisations se tournant de plus en plus vers les dispositifs et les capteurs connectés à Internet, nous assistons à une multiplication des points vulnérables aux attaques. Une attaque sur l'un de ces dispositifs interconnectés pourrait permettre à un pirate non seulement de prendre le contrôle d'un appareil, mais également de s'en servir comme porte d'entrée pour avoir accès à toutes sortes de renseignements personnels. Ce ne sont pas seulement les bases de données qui doivent être protégées, mais aussi les dispositifs connectés à Internet, comme les capteurs, les ampoules, les caméras vidéo et les routeurs Wi-Fi qui facilitent ces communications.

Tout cela porte à croire que l'Internet des objets nécessitera un nouveau modèle de sécurité. Compte tenu des limites au chapitre de l'alimentation en électricité, de la capacité informatique et d'autres facteurs, il faudra modifier en profondeur le mode de protection de ces dispositifs, puisque les concepts traditionnels de pare-feu et d'anti-maliciels ne donneront probablement pas de bons résultats avec ces nouvelles capacités. Les routeurs sont de plus en plus une cible prisée par les pirates puisqu'ils sont généralement toujours allumés et peuvent contenir des logiciels dépassés parfois difficiles à mettre à niveau ou à corriger[157]. Chaque dispositif connecté représente une faille de sécurité potentielle

permettant d'attaquer ou de corrompre d'autres dispositifs qui lui sont connectés[158]. En outre, plusieurs dispositifs connectés peuvent ne pas être dotés de fonctions de cryptage très avancées, ne possédant pas les composantes informatiques et l'alimentation nécessaires[159]. Pour reprendre une métaphore couramment utilisée, une chaîne n'est pas plus solide que son maillon le plus faible.

Comment peut-on faire confiance à un dispositif sans savoir s'il a été compromis de quelque façon que ce soit? Une attaque novatrice pourrait couper l'alimentation des capteurs ou des dispositifs[160]. Un dispositif compromis peut mettre à risque les renseignements personnels et la réputation d'une personne. Il peut également compromettre sa santé, voire sa vie, si, par exemple, une personne ayant pris le contrôle d'un dispositif médical lui commandait d'injecter une dose excessive de médicament à un patient[161]. Bien que nous nous employions à l'heure actuelle à nous assurer que les diverses parties dans l'écosystème de l'Internet des objets mettent en place des mesures de sécurité proportionnelles aux risques posés par ces dispositifs[162], il faut intégrer des composantes de protection fiables et solides si nous voulons mettre en place un écosystème de l'Internet des objets sûr.

La conception ou le déploiement de nombreux dispositifs intelligents pour les maisons ne sont pas sécurisés. Cette situation est peut-être attribuable au manque d'expérience des concepteurs en matière de sécurité, au fait qu'ils veulent maintenir les coûts les plus bas possible pour s'assurer que le dispositif demeure abordable ou aux limites inhérentes aux dispositifs miniaturisés[163]. Une étude réalisée par HP en 2014 révèle qu'environ 70 % des dispositifs de l'Internet des objets, entre autres les capteurs et l'infrastructure connectée, comportaient des points faibles pouvant être exploités. Ces dispositifs comprennent des télévisions, des caméras Web, des thermostats, des prises de courant commandées à distance, des gicleurs, des serrures de porte, des alarmes pour la maison, des balances et des ouvre-porte de garage. Voici certaines des conclusions dignes de mention : 80 % des dispositifs, y compris les applications infonuagiques et mobiles, n'exigeaient pas de mots de passe difficiles à deviner; 70 % des dispositifs ne cryptaient pas leurs communications; 60 % ne cryptaient pas les mises à jour logicielles; et 60 % comprenaient des interfaces Web non sécurisées[164].

Une étude de suivi publiée en février 2015 examinait dix des tout derniers systèmes de sécurité résidentielle. Cette étude a révélé qu'aucun de ces systèmes n'exigeait de mot de passe difficile à deviner et qu'un seul demandait une authentification à deux facteurs[165]. Sur les sept systèmes dotés de caméras, quatre donnaient accès à des utilisateurs supplémentaires. La plupart des systèmes ne verrouillaient pas les comptes après un certain nombre de tentatives de connexion infructueuses. Parmi les autres problèmes cernés figurent les faiblesses dans la configuration du cryptage, ce qui rend ces systèmes vulnérables aux accès non autorisés[166].

L'utilisation de caméras connectées à Internet a commencé à soulever des inquiétudes lorsqu'un site Web s'est mis à diffuser en direct des images provenant de caméras Web non sécurisées de partout dans le monde. En novembre 2014, le Commissariat et plusieurs autres commissaires à la protection des données au Canada et dans le monde ont écrit à l'opérateur du site Web, puis à plusieurs fabricants de caméras Web, pour leur faire part de leurs inquiétudes relatives aux caméras connectées à Internet et les presser de s'assurer que les mesures de sécurité appropriées sont en place pour protéger la vie privée de leurs clients[167].

Un pirate pourrait tirer parti de vulnérabilités comme des mots de passe faciles à deviner, des mécanismes non sécurisés de récupération de mot de passe ou des authentificateurs mal protégés pour accéder à un système. Tous ces problèmes pourraient mener à une « collecte » d'information sur un compte, dans le cadre de laquelle un pirate pourrait mettre au jour les authentificateurs d'ouverture de session et accéder à tout le système. Des comptes pour lesquels le mot de passe est facile à deviner et l'accès à une caméra vidéo pourraient fournir au pirate une porte d'entrée lui permettant de trouver un compte dont il pourrait se servir pour accéder au reste du système et, en bout de ligne, à la maison. En outre, la popularité grandissante des accessoires intelligents à porter sur soi qui suivent l'humeur, la condition physique et la santé présente de nouveaux défis au chapitre de la sécurité et de la protection de la vie privée, lesquels sont abordés plus en détail dans un autre rapport[168].

Conclusion

En raison des capteurs et des positionneurs qui sont toujours allumés et en constante interaction avec leur corps et des autres dispositifs utilisés dans leur environnement, les utilisateurs auront plus de difficulté à séparer les différentes sphères de leur vie. Il devra également y avoir une responsabilité réelle pour les résultats des décisions que les soi-disant machines intelligentes prennent à notre sujet.

Dans un monde où nos activités et nos comportements quotidiens sont appelés à être de plus en plus mesurés, enregistrés et analysés, il est urgent que les concepteurs et les décideurs réfléchissent à la manière d'informer les consommateurs et les citoyens afin qu'ils sachent qui recueille leurs renseignements personnels, quels renseignements personnels sont recueillis, la manière dont ils sont conservés, utilisés et communiqués, à qui ils sont communiqués, et à quelles fins.

Si la transparence en ce qui concerne la collecte de données au moyen de dispositifs intelligents à l'ère de l'Internet des objets est importante pour nos relations avec le secteur privé, elle l'est tout autant pour nos relations avec le gouvernement. Il ne faudra guère nous surprendre que la manne de renseignements recueillis au moyen de l'Internet des objets à des fins commerciales suscite l'intérêt d'organismes d'application de la loi et de gouvernements.

L'évolution technologique dans le contexte de l'Internet des objets n'est pas accompagnée d'une évolution similaire dans les modèles de gouvernance fondamentaux en matière de protection de la vie privée. Jusqu'à maintenant, on n'a guère accordé d'attention aux nombreuses répercussions sur la vie privée attribuables à l'énorme quantité de données qui peuvent être recueillies et agrégées à partir de plusieurs dispositifs et analysées non seulement par les propriétaires des dispositifs, mais également par des tierces parties inconnues d'eux.

L'un des principaux problèmes tient au fait que l'omniprésence grandissante de ces technologies fait en sorte qu'il est difficile, voire impossible, de savoir même qu'elles sont en place[169]; elles se fondent tout simplement à notre quotidien. Dans ce contexte, comment les citoyens, qu'ils veuillent ou non utiliser une technologie en particulier, peuvent-ils s'assurer que quelqu'un est tenu responsable de son utilisation? Comment pourront-ils contester l'usage qui est fait de l'information, et comment pourront-ils donner une forme quelconque de consentement valable?

Toutes les répercussions de l'Internet des objets sur notre vie privée deviendront peut-être plus évidentes lorsque ses capacités seront conjuguées à d'autres innovations qui façonnent notre monde d'aujourd'hui et sont utilisées pour suivre non seulement nos activités, nos déplacements, nos préférences et nos comportements, mais aussi nos émotions et nos pensées.

Notes

[1] Pew Research Center, « Digital Life in 2025 », 11 mars 2014. Consulté le 12 mai 2015.
[2] Eric Savitz, « How The Internet Of Things Will Change Almost Everything », *Forbes*, 17 décembre 2012. Consulté le 12 mai 2015.
[3] Pew Research Center, « Digital Life in 2025 », 11 mars 2014. Consulté le 12 mai 2015.
[4] Par exemple, la Commission européenne a affiché les résultats des consultations publiques et les constatations des groupes de travail sur l'Internet des objets, février 2013. Consulté le 12 mai 2015.
[5] Voir le rapport du personnel de la Federal Trade Commission des États-Unis, *Internet of Things: Privacy and Security in a Connected World*, janvier 2015. Consulté le 12 mai 2015.
[6] Par exemple, IPSO Alliance et ZigBee Alliance.
[7] Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things, 14/EN WP 223, groupe de travail Article 29 sur la protection des données, 16 septembre 2014. (Ce groupe de travail, qui a été établi en vertu de l'article 29 de la directive 95/46/CE, est un organisme consultatif européen indépendant sur la protection des données et la vie privée. Ses tâches sont décrites à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.)
[8] Mauritius Declaration on the Internet of Things, 36e Conférence internationale des commissaires à la protection des données et à la vie privée, octobre 2014. Consulté le 12 mai 2015.
[9] *Comments of the Electronic Privacy Information Center to the Federal Trade Commission On the Privacy and Security Implications of the Internet of Things*, 1er juin 2013. Consulté le 12 mai 2015.
[10] Commissariat à la protection de la vie privée du Canada, *Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée*, octobre 2012.
[11] Commissariat à la protection de la vie privée du Canada, *Les accessoires intelligents — Défis et possibilités pour la protection de la vie privée*, rapport de recherche, janvier 2014.
[12] Voir le site Web de l'European Research Cluster on the Internet of Things.
[13] Voir, par exemple, le rapport Internet of Things: From Research and Innovation to Market Deployment de l'European Research Cluster on the Internet of Things (IERC), 2014. Consulté le 12 mai 2015.
[14] Jeremy Crump, « Time for debate about the societal impact of the Internet of Things », *The Policy and Internet Blog*, Université d'Oxford, 22 avril 2013. Consulté le 12 mai 2015.
[15] Chaochi Hakima (dir.), *The Internet of Things: Connecting Objects to the Web*, Wiley-ISTE, 2010, p. 252.
[16] « Finding the Best Lost-Item Trackers: Tile, TrackR and Duet Reviewed: Thanks to New Bluetooth Tags, Your Keys, Wallet and Purse Should Never Go Missing Again », *Wall Street Journal*, 17 juin 2014. Consulté le 12 mai 2015.
[17] Voir PetHub.
[18] Voir BuddyTag.
[19] Voir le document de consultation *L'identification par radiofréquence (IRF) en milieu de travail : Document de consultation sur les recommandations de règles de pratique* (2008) et les résultats de la consultation menée par le Commissariat à la protection de la vie privée du Canada.
[20] Pour plus de détails, voir Chaochi Hakima (dir.), *The Internet of Things: Connecting Objects to the Web*, Wiley-ISTE, 2010, p. 18 : mécanique (p. ex. position, force, pression), thermique (p. ex. température), champs électrostatiques ou magnétiques, radiation (p. ex. électromagnétique, nucléaire), chimique (p. ex. humidité, ion, teneur en gaz), biologique (p. ex. toxicité), militaire (p. ex. surveillance de l'ennemi ou du champ de bataille).
[21] Jamie Carter, « What is NFC? Everything you need to know », *Tech Radar*, 16 janvier 2013. Consulté le 12 mai 2015.

[22] Pour plus de détails, voir Alain Louchez, « L'Internet des objets — Machines, entreprises, individus, tout », *ITU News*, n° 6, 2013. Consulté le 12 mai 2015.
[23] Pour plus de détails, voir Chaochi Hakima (dir.), *The Internet of Things: Connecting Objects to the Web*, Wiley-ISTE, 2010, p. 18 : mécanique (p. ex. position, force, pression), thermique (p. ex. température), champs électrostatiques ou magnétiques, radiation (p. ex. électromagnétique, nucléaire), chimique (p. ex. humidité, ion, teneur en gaz), biologique (p. ex. toxicité), militaire (p. ex. surveillance de l'ennemi ou du champ de bataille).
[24] Ángel Asensio, Álvaro Marco, Rubén Blasco et Roberto Casas, « Protocol and Architecture to Bring Things into Internet of Things », *International Journal of Distributed Sensor Networks*, 13 avril 2014. Consulté le 12 mai 2015.
[25] Melanie Swan, « Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0 », *Journal of Sensors and Actuator Networks*, vol. 1, n° 3, 2012, p. 217-253. Consulté le 12 mai 2015.
[26] Pour des publications récentes sur la technologie et l'histoire de l'Internet des objets, voir : Organisation de coopération et de développement économiques, « Machine-to-Machine Communications: Connecting Billions of Devices », *OECD Digital Economy Papers*, n° 192, 2012; D. Uckelmann *et al.* (dir.), « An Architectural Approach Towards the Future Internet of Things », *Architecting the Internet of Things*, 2011; et Chaochi Hakima (dir.), *The Internet of Things: Connecting Objects to the Web*, Wiley-ISTE, 2010.
[27] Voir, par exemple, Union internationale des télécommunications, *The Internet of Things*, rapport Internet de l'UIT, 2005. Consulté le 12 mai 2015. Link doesn't work
[28] Pour des représentations visuelles de diverses configurations réseau, voir National Institute of Standards and Technology, Catalogue of Network Connectivity Models, 2001.
[29] Seth Rosenblatt, « 'Internet of Things,' not privacy, to dominate at Black Hat », *CNet*, 6 août 2014. Consulté le 12 mai 2015.
[30] Daniel Kellmereit et Daniel Obodovski, *The Silent Intelligence: The Internet of Things*, 2013, p. 30-31.
[31] Pour la citation dans la zone de texte adjacente, voir Michelle Finneran Dennedy, Jonathan Fox et Thomas R. Finneran, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*, 2014. Consulté le 4 avril 2015.
[32] « New IDC Research Forecasts Canadian Spending on Internet of Things to be Largest in Manufacturing, Healthcare and Transportation Industries », communiqué de la International Data Corporation, 23 avril 2015. Consulté le 12 mai 2015.
[33] Emily Alder, « The 'Internet Of Things' Will Soon Be A Truly Huge Market, Dwarfing All Other Consumer Electronics Categories », *Business Insider*, 17 juillet 2014. Consulté le 12 mai 2015.
[34] « More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020 », ABI Research, 9 mai 2013. Consulté le 12 mai 2015.
[35] « Privacy integral to future of the Internet of Things », *USA Today*, 11 juillet 2014. Consulté le 12 mai 2015.
[36] « Gartner Says It's the Beginning of a New Era: The Digital Industrial Economy », communiqué de Gartner, Inc., 7 octobre 2013. Consulté le 12 mai 2015.
[37] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson et Alex Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, mai 2013, p. 51. Consulté le 12 mai 2015.

[38] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson et Alex Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, mai 2013, p. 53. Consulté le 12 mai 2015.
[39] Voir, par exemple, Thomas Ohnemus, « The Internet Of Things: Enabler Of The Fourth Industrial Revolution », billet de blogue de l'invité de SAP, 21 mai 2014. Consulté le 12 mai 2015.
[40] Lou Frenzel, « The Connected World Awaits », *Electronic Design*, 10 mars 2014. Consulté le 12 mai 2015.
[41] Voir le renvoi de *Network World* à l'infographie d'Irish Telecom comparant l'IPv6 et l'IPv4, 7 octobre 2014. Consulté le 12 mai 2015.
[42] « Gartner Says the Internet of Things Will Transform the Data Center », Gartner, Inc., 18 mars 2014. Consulté le 12 mai 2015.
[43] Voir, par exemple, l'ordre du jour et la liste des spécialistes de divers domaines participant à l'atelier de l'Union internationale des télécommunications, « Internet of Things: Trends and Challenges in Standardization », qui a eu lieu à Genève le 18 février 2014. Consulté le 12 mai 2015.
[44] Deloitte et Conseil canadien du commerce de détail, *Omni-channel: Rethink, reshape, revalue – Retail Study 2014*, p. 12.
[45] Deloitte et Conseil canadien du commerce de détail, *Omni-channel: Rethink, reshape, revalue – Retail Study 2014*, p. 16.
[46]Page Web de ProximitySky, « Wi-Fi vs. Bluetooth ».
[47] Page Web de LinkLabs, « Bluetooth Vs. Bluetooth Low Energy: What's The Difference? », 1er novembre 2015.
[48] Page Web de Bluetooth, « Bluetooth Low Energy (also called Bluetooth Smart)», 1er novembre 2015.
[49] Commissariat à la protection de la vie privée du Canada, *L'identification par radiofréquence*.
[50] Pour de plus amples renseignements, voir Commissariat à la protection de la vie privée du Canada, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*.
[51] Page Web d'Euclid Analytics.
[52] Billet de blogue d'Euclid Analytics, « Why Wi-Fi is the right approach for retail analytics », 23 juillet 2014.
[53] Darrell Etherington, « Aislelabs Raises $1.5M To Bring Full Cycle Visitor Analytics To Brick-And-Mortar Retail », *TechCrunch*, 19 mars 2014.
[54] Chantal Tode, « Location tracking opt-out could land big blow to retail technology », *Mobile Marketer*, 19 février 2014.
[55] Page Web d'Aislelabs, « Cloud based in-store analytics to understand the behavior of your customers », *AislelabsFlow.*
[56] Jacob Kastrenakes, « Philips takes on Apple's iBeacon with lights that send deals to your smartphone », *The Verge*, 27 février 2014.
[57] Page Web de Phillips « Lighting systems for retail & hospitality ».
[58] Nestor E. Arellano, « New Fortinet solution offers retail analytics », *IT World Canada*, 13 janvier 2014.
[59] Retail Technology, « Modern retailing and omnichannel challenge », 14 août 2014.
[60] Cisco, *Wi-Fi: New Business Models Create Real Value for Service Providers*, 1er juin 2013, p. 8.
[61] Lee Badman, « Social WiFi Sign-In: Benefits With A Dark Side », *Information Week*, 7 mai 2014.
[62] Steven Skinner, « Beacon technology offers plenty of opportunities for retailers », *The Guardian*, 4 septembre 2014.
[63] Page Web de Shopkick, « What is shopBeacon™? ».

[64] Page Web de Shopkick, « What is shopBeacon™? ».
[65] Armina Ligaya, « Hudson's Bay keeps closer tabs on shoppers with new in-store mobile marketing », *Financial Post*, 28 juillet 2014.
[66] Claire Swedberg, « Iconeme Launches Bluetooth Beacon Solution for Mannequins », *RFID Journal*, 21 avril 2014.
[67] Page Web d'Iconeme, « How it Works ».
[68] DigitalSignageToday, « Digital signage leveraging beacon tech to boost shopper loyalty », 7 janvier 2015.
[69] intel, « Intelligent Mobile Advertising Solution Delivers Targeted Messages », p. 2.
[70]Madame Smith, « Digital Signage: Privacy in a "One-Way Mirror Society" », *NetworkWorld*, 15 février 2011.
[71] Ally Orlando, « Digital Mirrors Could Create Virtual Fitting Rooms In Retail Stores », *Integrated Solutions For Retailers*, 13 mai 2014.
[72] Ally Orlando, « Digital Mirrors Could Create Virtual Fitting Rooms In Retail Stores », *Integrated Solutions For Retailers*, 13 mai 2014.
[73] Mike Elgan, « How apps are changing fast food », *Computerworld*, 15 février 2014.
[74] Natalie Gagliordi, « Internet of Things, Big Data fuels latest batch of POS tech », *ZDNet*, 19 mai 2014.
[75] Shane Dingman, « Why your smartphone is telling this Toronto tech firm all about you », *The Globe and Mail*, 14 janvier 2014.
[76] Armina Ligaya, « "It's creepy": Location based marketing is following you, whether you like it or not », *Financial Post*, 1er février2014.
[77] Armina Ligaya, « "It's creepy": Location based marketing is following you, whether you like it or not », *Financial Post*, 1er février2014; Elizabeth Dwoskin, « What Secrets Your Phone Is Sharing About You », *The Wall Street Journal*, 13 janvier 2014.
[78] Page Web de Turnstyle, « Privacy ».
[79] Elizabeth Dwoskin, « What Secrets Your Phone Is Sharing About You », *The Wall Street Journal*, 13 janvier 2014.
[80] Page d'accueil de Via Informatics.
[81] Ivor Tossell, « Using "remarkable" source of data, startup builds rich customer profiles », *The Globe and Mail*, 6 janvier 2014.
[82] Elizabeth Dwoskin, « What Secrets Your Phone Is Sharing About You », *The Wall Street Journal*, 13 janvier 2014.
[83] Page d'accueil de Via Informatics.
[84] Page Web de Skyhook, « Personas ».
[85] Page Web de Skyhook, « Personas ».
[86] Page d'accueil de Skyhook.
[87] Mobile Marketing Association, *Mobile Location Based Services Marketing Whitepaper*, octobre 2011, p. 19.
[88] Lauren Brousell, « 5 Things You Need to Know About Geofencing », *CIO Magazine*, 28 août 2013.
[89] Interactive Advertising Bureau, *Mobile Location Use Cases and Case Studies*, mars 2014, p. 18.
[90] Lauren Brousell, « 5 Things You Need to Know About Geofencing », *CIO Magazine*, 28 août 2013.
[91] Benjamin Spiegel, « Geo-Location, Geo-Fencing & Creep Factor: The Future of Location Data and Mobile Advertising », *ClickZ*, 11 octobre 2013.
[92] Interactive Advertising Bureau, *Mobile Location Use Cases and Case Studies*, mars 2014, p. 14-16.
[93] Juge Cory dans *R c. Silveira*, [1995] 2 RCS 297, 1995 CanLII 89 (CSC).

[94] Adarsh Krishnan, analyste principal de recherche chez ABI, une entreprise de renseignements sur le marché de la technologie, cité par Morgan Brennan, « House of the Future: How Automation Tech Is Transforming The Home », *Forbes Magazine*, 10 octobre 2013. Consulté le 1er avril 2015.
[95] ENISA, *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*, p. 5, 1er décembre 2014. Consulté le 1er avril 2015.
[96] ENISA, *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*, p. 5-6, 1er décembre 2014. Consulté le 1er avril 2015.
[97] Mellissa Tolentino, « Smart Home market to boom in 2020: New trends in smart elevators + smoke detectors », blogue du *Silicon Angle,* 27 janvier 2014. Consulté le 1er avril 2015.
[98] ETS Insights, « U.K. and Canada Smart Home Market Brief », 18 juin 2014. Consulté le 1er avril 2015.
[99] Rapport annuel 2014 du Bureau de la vérificatrice générale de l'Ontario, p. 423. Consulté le 1er avril 2015. Le rapport conclut également que les avantages projetés de la mise en œuvre des compteurs intelligents sont moins élevés que prévu.
[100] Pour plus de renseignements, voir la page d'Hydro One sur les compteurs intelligents (en anglais seulement). Consulté en avril 2015.
[101] « Ontario's Green Button: Providing You with Access to Your Energy Data ». Consulté le 1er avril 2015.
[102] « Green Button: Helping You Find and Use Your Energy Data ». Consulté le 1er avril 2015.
[103] « Énergiconomies ». Consulté le 1er avril 2015.
[104] « Connected TVs Reach One in Four Homes », *eMarketer*, 3 janvier 2013. Consulté le 1er avril 2015.
[105] Dan Shust, vice-président du RI Lab chez Resource Interactive, cité par Jay Donovan dans « Smart TVs: How Do They Work? », *TechCrunch*, 13 janvier 2012. Consulté le 2 avril 2015.
[106] Google et Apple cherchent à se positionner en tant que chefs de file de la sécurité dans la maison intelligente : Google a fait l'acquisition d'entreprises en démarrage telles que Nest Labs, entreprise de thermostats intelligents, et Dropcom, concepteur de caméras en circuit fermé, de manière à combiner les deux appareils; Apple a lancé HomeKit, un cadriciel qui peut être utilisé par des concepteurs d'applications et de matériel pour communiquer avec les accessoires connectés d'une maison et les contrôler. Pour plus de détails, voir « Smart homes: 'My home, my comfort', say readers », Open Roboethics Initiative, 28 octobre 2014. Consulté le 2 avril 2015.
[107] Rick Delgado, « From Edison to Internet: A History of Video Surveillance », 14 août 2013. Consulté le 2 avril 2015.
[108] Richard Davis, « How surveillance systems save money on insurance », 24 janvier 2014. Consulté le 2 avril 2015. Bien que nous ne sachions pas si tel est le cas au Canada, il est fort probable que les compagnies d'assurance canadiennes adopteront cette façon de faire. Voir également la fiche d'information — Conseils concernant l'assurance-maison de la Commission des services financiers de l'Ontario. Consulté le 2 avril 2015.
[109] Cette fonction est de plus en plus offerte dans de nombreuses caméras, y compris les suivantes : Vue Zone, netcams de Belkin.
[110] « Intelligent à tout moment », Le commissaire à l'environnement de l'Ontario, 15 octobre 2014. Consulté le 21 janvier 2016.
[111] Megan Wollerton, « Smart appliances, connected homes at CES 2014 », *CNET*, 10 janvier 2014. Consulté le 1er avril 2015; Keith Wagstaff, « Out of Milk? LG's New Smart Fridge Will Let You Know », *NBC News*, 7 mai 2014. Consultés le 12 mai 2015.
[112] Yohana Desta, « Why You're Not Seeing More Smart Home Appliances », 26 avril 2014. Consulté le 1er avril 2015.

[113] Morgan Brennan, « House Of The Future: How Automation Tech Is Transforming The Home », *Forbes,* 10 octobre 2013. Consulté le 1er avril 2015. Voir les images connexes.
[114] Alison Marie Kenner, « Securing the Elderly Body: Dementia, Surveillance, and the Politics of 'Aging in Place' », *Surveillance and Society*, vol. 5, no 3, Kingston (Ontario), Université Queen's, 2008. Consulté le 2 avril 2015. La surveillance de la maison intelligente est un élément du concept « vieillir chez soi ».
[115] Association canadienne des individus retraités, « Nursing Home Woes », juin 2011. Consulté le 2 avril 2015.
[116] Victoria Stunt, « Use of surveillance tech to monitor seniors at home on rise », 9 mars 2014. Consulté le 2 avril 2015.
[117] Shalene Gupta, « For the disabled, smart homes are home sweet home », *Fortune Magazine*, 1er février 2015. Consulté le 29 avril 2015.
[118] Basma M. Mohammad El-Basioni, Sherine Mohamed Abd El-Kader et Hussein S. Eissa, « Independent Living for Persons with Disabilities and Elderly People Using Smart Home Technology », *International Journal of Application or Innovation in Engineering and Management*, vol. 3, no 4, avril 2014. Consulté le 29 avril 2015.
[119] Future of Privacy Forum, « The Future of Privacy Forum Announces New Group to Develop Best Practices for Retail Location Analytics Companies », 16 juillet 2013.
[120] International Association of Privacy Professionals, *IAPP Information Privacy Certification — Glossary of Common Privacy Terminology*, 2011.
[121] Ed Felten, « Is aggregate data always private? », blogue *Tech@FTC*, 21 mai 2012.
[122] Groupe de travail Article 29 sur la protection des données, *Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things*, 14/EN WP 223, 16 septembre 2014, p. 11.
[123] Groupe de travail Article 29 sur la protection des données, *Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things*, 14/EN WP 223, 16 septembre 2014, p. 8.
[124] Ângela Guimarães Pereira, Alice Benessia, et Paula Curvelo, *Agency in the Internet of Things*, Joint Research Centre — Institute for the Protection and Security of the Citizen, Commission européenne, 2013, p. 9.
[125] Groupe de travail Article 29 sur la protection des données, *Opinion 13/2011 on Geolocation services on smart mobile devices*, 881/11/EN WP 185, 16 mai 2011, p. 6.
[126] Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, 22 octobre 2013.
[127] Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, 22 octobre 2013, p. 3.
[128] Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, 22 octobre 2013 p. 6.
[129] Future of Privacy Forum, « MAC Addresses and De-Identification », 27 mars 2014.
[130] Commissariat à la protection de la vie privée du Canada, *Tracer le chemin : Principaux développements au cours des sept premières années d'application de la* Loi sur la protection des renseignements personnels et les documents électroniques *(LPRPDE)*, 23 mai 2008, p. 31.
[131] Electronic Frontier Foundation, « Mobile Tracking Code of Conduct Falls Short of Protecting Consumers », 26 octobre 2013.
[132] Commissariat à la protection de la vie privée du Canada, *Rapport des conclusions en vertu de la LPRPDE no 2013-001*.
[133] Ed Felten, « Does Hashing Make Data "Anonymous"? », blogue *Tech@FTC,* 22 avril 2012.
[134] Jim Rennie, « Data Anonymization », *TRUSTe Blog*, 16 avril 2013.
[135] *Gordon c. Canada* (Santé), 2008 CF 258 (CanLII). Consulté le 12 mai 2015.
[136] Déclaration du commissaire à la protection de la vie privée du Canada concernant le jugement de la Cour suprême dans *R. c. Spencer*, 13 juin 2014.

[137] « Une déclaration des droits numérique : Commentaires à la conférence juridique de l'Association du Barreau canadien », allocution prononcée par Patricia Kosseim, avocate générale principale, Commissariat à la protection de la vie privée du Canada, 15 août 2014.
[138] Commissariat à la protection de la vie privée du Canada, *Ce qu'une adresse IP peut révéler à votre sujet : Rapport préparé par la Direction de l'analyse des technologies du Commissariat à la protection de la vie privée du Canada*, mai 2013.
[139] Commissariat à la protection de la vie privée du Canada, *Métadonnées et vie privée : Un aperçu technique et juridique*, octobre 2014.
[140] Commissariat à la protection de la vie privée du Canada, *L'ère de l'analyse prédictive : des tendances aux prédictions*, rapport préparé par le groupe de recherche du Commissariat à la protection de la vie privée du Canada, août 2012.
[141] *Comments of the Electronic Privacy Information Center to the Federal Trade Commission On the Privacy and Security Implications of the Internet of Things*, 1er juin 2013. Consulté le 12 mai 2015.
[142] Commissariat à la protection de la vie privée du Canada, *Rapport de conclusions en vertu de la LPRPDE n° 2013-017*.
[143] Robert Lee Hotz, « Metadata Can Expose Person's Identity Even Without Name », *The Wall Street Journal*, 29 janvier 2015.
[144] Dans son opinion sur l'Internet des objets, le groupe de travail Article 29 sur la protection des données a formulé des recommandations à ce chapitre, notamment en attribuant des responsabilités précises à ces intervenants. Voir Groupe de travail Article 29 sur la protection des données, *Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things*, 14/EN WP 223, 16 septembre 2014. Consulté le 12 mai 2015.
[145] Voir, par exemple, les ressources de l'Electronic Privacy Information Center sur la transparence de l'algorithme. Consulté le 15 juillet 2015; voir également *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, document d'orientation conjoint élaboré par le Commissariat à la protection de la vie privée du Canada et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, avril 2012.
[146] Voir, par exemple, David S. Kemp, « Autonomous Cars and Surgical Robots: A Discussion of Ethical and Legal Responsibility », *Verdict*, 19 novembre 2012; James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson et Alex Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, p. 59, mai 2013. Consultés le 14 avril 2015.
[147] Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, 22 octobre 2013, p. 1-2.
[148] Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, 22 octobre 2013.
[149] Communiqué de la Federal Trade Commission, « Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices », 23 avril 2015.
[150] Communiqué de la Federal Trade Commission, « Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices », 23 avril 2015.
[151] Communiqué de la Federal Trade Commission, « Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices », 23 avril 2015.
[152] Commissariat à la protection de la vie privée du Canada, *Les accessoires intelligents — Défis et possibilités pour la protection de la vie privée*, rapport de recherche, janvier 2014.
[153] Liste des fichiers de renseignements personnels Info Source du gouvernement du Canada. Consulté le 13 avril 2015.
[154] *Personal Data Management: The User's Perspective*, International Institute of Communications, 22 novembre 2012, p. 9.

[155] Si les appareils peuvent apprendre et exécuter les règles automatisées que nous établissons concernant ce que nous voulons communiquer dans des circonstances, des lieux et des endroits donnés — puis fermer le robinet — la protection de la vie privée pourrait être renforcée. Voir Jared Allen, Quang Duong et Craig Thompson, « Natural Language Service for Controlling Robots and Other Agents », KIMAS 2005, 18-21 avril 2005. Consulté le 12 mai 2015.
[156] « Gestural Interfaces: Controlling Computers with our Bodies », *MIT Technology Review*, mai-juin 2011. Consulté le 12 mai 2015.
[157] Bruce Schneier, « The Internet of Things Is Wildly Insecure—And Often Unpatchable », *Wired*, 6 janvier 2014. Consulté le 14 avril 2015.
[158] Stacey Higginbotham, « The internet of things needs a new security model. Which one will win? », Gigaom, 22 janvier 2014. Consulté le 12 mai 2015.
[159] Wade Trappe, Richard Howard et Robert S. Moore, « Low-Energy Security: Limits and Opportunities in the Internet of Things », *IEEE Security & Privacy*, vol. 13, n° 1, p. 14-21, janvier-février 2015.
[160] Earl Perkins (vice-président de Gartner Research), « Securing The Internet of Things— Some Not-So-Obvious Concerns », 20 janvier 2014. Consulté le 12 mai 2015.
[161] « Possible cybersecurity flaws in medical devices probed », *CBC News*, 22 octobre 2014. Consulté le 12 mai 2015.
[162] Voir, par exemple, les recommandations sur la sécurité à l'étape de la conception dans le mot d'ouverture de la présidente de la FTC, Edith Ramirez, « Privacy and the IoT: Navigating Policy Issues », International Consumer Electronics Show, Las Vegas, Nevada, 6 janvier 2015. Consulté le 14 avril 2015.
[163] *Supra*, note 4, p. 17-18.
[164] Larry Dignan, « Internet of things big security worry, says HP », *ZDNet*, 29 juillet 2014. Consulté le 2 avril 2015.
[165] L'authentification à deux facteurs est une mesure de sécurité dans le cadre de laquelle l'utilisateur doit s'identifier de deux façons. En général, il s'agit d'une authentification physique, par exemple au moyen d'une carte, et d'une autre qui est généralement mémorisée, par exemple un code de sécurité. Ces deux facteurs sont parfois connus comme étant *quelque chose que l'on possède* et *quelque chose que l'on sait*. Voir TechTarget, « two-factor authentication (2FA) definition ». Consulté le 29 juin 2015.
[166] « HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems » 10 février 2015. Consulté le 2 avril 2015.
[167] Ces lettres se trouvent sur le site Web du Commissariat : Lettre aux 10 fabricants de caméras Web au Canada et aux États-Unis et Lettre aux opérateurs du site diffusant des images de caméras Web.
[168] Commissariat à la protection de la vie privée du Canada, *Les accessoires intelligents — Défis et possibilités pour la protection de la vie privée*, rapport de recherche, janvier 2014.
[169] Chris Baraniuk, « Surveillance: The hidden ways you're tracked », BBC, 27 octobre 2014. Consulté le 2 avril 2015.