CLASSESAFFAIRES
ACTUALITÉS · SÉMINAIRES · PERSPECTIVES

Blakes

Internet des objets : réduire les risques liés à la sécurité et à la protection de la vie privée dans un monde interrelié

Wendy Mee et Kristin Ali

Consultez nos mesures pratiques visant à créer un Internet des objets plus sécuritaire où les renseignements personnels sont mieux protégés.

Votre imprimante. Le refroidisseur d'eau. Le thermostat. Qu'est-ce que ces appareils ont en commun? Ils peuvent tous être connectés à l'Internet des objets (l'« IdO »).

L'Internet des objets poursuivant son ascension fulgurante en 2017, une vaste gamme d'appareils peut désormais être connectée aux différents réseaux à travers le monde. La société de recherche technologique Gartner Inc. prédit que plus de 20 milliards d'appareils feront partie de l'IdO d'ici 2020 et le cabinet d'intelligence International Data Corporation estime que la valeur du marché canadien de l'IdO s'élèvera à plus de 4,9 G$ US en 2018.

L'IdO a, et continuera d'avoir, une incidence majeure sur les affaires des organisations de l'ensemble des secteurs. Les entreprises qui ne préparent pas leur environnement numérique à intégrer l'IdO ratent une occasion de tirer parti de la quantité phénoménale de données qu'il génère et risquent de perdre des parts de marché au profit de leurs concurrents qui ont adopté cette nouvelle technologie.

Cisco a calculé que les appareils connectés à l'IdO créeront 500 Zo de données d'ici 2019 (un zettaoctet équivaut à plus d'un billion de gigaoctets). Les organisations peuvent utiliser ces mégadonnées pour cerner des tendances importantes et recueillir de précieux renseignements au moyen de l'analytique avancée, ce qui les aide à analyser les résultats antérieurs, à prévoir les tendances futures et, du même coup, à améliorer leur efficacité opérationnelle et leurs prises de décisions.

Dans le secteur du commerce de détail, par exemple, les données combinées provenant d'appareils de l'IdO peuvent fournir des profils détaillés des modes de vie, des préférences et des habitudes des consommateurs, permettant ainsi aux spécialistes du marketing d'influencer plus efficacement les décisions des consommateurs et de personnaliser davantage les expériences clients. Par ailleurs, les consommateurs veulent de plus en plus profiter de la convivialité et des fonctionnalités que procurent ces appareils, ce qui signifie que les organisations qui ne tirent pas parti de cette technologie pourraient perdre des clients et des ventes.

Bien que l'IdO se trouve encore à un stade précoce et que les entreprises tâtonnent encore pour extraire du contenu pertinent à partir des quantités phénoménales de données générées, il promet des avantages importants pour les entreprises qui auront mis en place une stratégie axée sur cette nouvelle technologie.

Évidemment, ces avantages ne viennent pas sans risques. Lorsque les mégadonnées recueillies par des appareils de l'IdO sont associées à des utilisateurs identifiés ou identifiables, elles constituent des renseignements personnels et, par conséquent, la collecte, l'utilisation, la communication ou tout autre traitement de ces renseignements doivent être conformes aux lois sur la protection de la vie privée. Il faut notamment obtenir le consentement éclairé des utilisateurs et limiter la collecte, l'utilisation et la conservation des renseignements personnels à ce qui est raisonnable et nécessaire, de même que donner aux utilisateurs le droit d'accéder à leurs données et de les corriger, ainsi que la capacité de retirer leur consentement.

Il peut être difficile de se conformer à ces exigences dans l'environnement de l'IdO. En particulier, le fait d'avoir à se conformer aux principes de limitation de la collecte et de la conservation des données peut influer sur l'utilité des renseignements obtenus à partir d'appareils de l'IdO. Puisque les principes en matière de protection de la vie privée s'appliquent uniquement aux renseignements personnels et non aux données ne permettant pas d'identifier une personne, les organisations qui souhaitent maximiser la valeur tirée de ces mégadonnées devraient faire appel à des experts en matière d'anonymisation.

Les lois canadiennes sur la protection de la vie privée exigent que les renseignements personnels soient protégés au moyen de mesures de sécurité appropriées, étant donné la nature délicate de ces renseignements. Même si les données recueillies par les appareils de l'IdO ne sont pas sensibles par nature, le volume impressionnant de renseignements obtenus – permettant de créer des profils individuels des utilisateurs très détaillés – peut signifier que ces données doivent être considérées comme très sensibles et protégées au moyen de mesures de sécurité proportionnellement robustes.

Les mégadonnées sont une cible attrayante pour les cybercriminels, et les appareils et les réseaux de l'IdO peuvent être piratés de la même façon que tout autre dispositif pouvant se connecter à l'Internet. Dans cet environnement où les appareils, les applications et les réseaux sont interreliés, le choix des cibles d'attaques est beaucoup plus vaste.

Du point de vue de la sécurité, les appareils de l'IdO posent des défis uniques puisque de nombreuses mesures de sécurité traditionnelles ne peuvent pas, dans bien des cas, s'y appliquer (dont celles utilisées pour protéger les réseaux). De plus, la sécurité des appareils ne concerne pas seulement la sécurité des données. Vu le nombre important d'appareils visés (voitures connectées, dispositifs médicaux connectés, systèmes de sécurité résidentiels connectés, etc.), une défaillance de la sécurité de certains d'entre eux peut également causer la perte ou le vol d'un bien, ainsi que des lésions corporelles ou même la mort.

Ces risques liés à la sécurité et à la protection de la vie privée ne sont pas passés sous le radar des organismes de réglementation. Au Canada et aux États-Unis, ceux-ci ont émis des avertissements et des directives sur les risques que posent les appareils de l'IdO à la sécurité et à la protection de la vie privée.

PROTECTION DE LA VIE PRIVÉE

Les préoccupations liées à la protection de la vie privée que suscite l'IdO sont une priorité importante du Commissariat à la protection de la vie privée du Canada (le « CPVPC »). Dans son Rapport annuel au Parlement 2016-2017 concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*, le CPVPC a indiqué que des directives supplémentaires ou des mises à jour seraient émises relativement à l'IdO, aux mégadonnées, aux voitures connectées et aux maisons intelligentes, entre autres.

Ces directives nouvelles ou modifiées s'ajoutent au travail déjà accompli par le CPVPC au sujet de cette nouvelle technologie. En 2016, le CPVPC a participé au ratissage du Global Privacy Enforcement Network consacré à l'IdO. Il s'est concentré sur les dispositifs de santé connectés tels que les moniteurs d'activité physique, les thermomètres et les moniteurs de fréquence cardiaque. L'un des principaux problèmes mis en évidence dans le cadre du ratissage est la médiocrité des énoncés sur la protection de la vie privée. Le CPVPC a constaté que les appareils recueillent une quantité impressionnante de données sensibles, mais que les communications aux utilisateurs sur les renseignements personnels sont génériques et qu'elles n'informent pas adéquatement ceux-ci sur la nature des renseignements personnels qui sont recueillis par l'appareil et sur la façon dont ils seront utilisés.

« Avec l'essor de l'Internet des objets, les activités, comportements et préférences des individus sont mesurés, enregistrés et analysés de plus en plus régulièrement. Cette technologie prend de l'expansion et il faut absolument que les entreprises expliquent mieux leurs pratiques en matière de traitement des renseignements personnels », a déclaré Daniel Therrien, commissaire du CPVPC.

Parmi les autres enjeux notés, on retrouve le manque de renseignements sur la façon dont l'information est conservée, l'absence de directives claires quant à la manière de supprimer les données et les cas où l'utilisateur devait fournir davantage de renseignements personnels que ceux raisonnablement requis compte tenu des fonctions de l'appareil. Toutefois, sur une note positive, le CPVPC a constaté qu'un certain nombre d'appareils fournissaient des avis en temps réel sur la collecte de certains éléments d'information.

SÉCURITÉ

Les cyberattaques facilitées par des appareils de l'IdO mal sécurisés ont fait les manchettes récemment. La plus notoire étant celle visant Dyn Inc., survenue en octobre 2016, où des pirates informatiques ont lancé une cyberattaque massive contre d'importants sites Web à l'intention des consommateurs, qui a compromis des centaines de milliers d'appareils de l'IdO dont la sécurité était déficiente. À l'aide d'un logiciel malveillant, les pirates ont infecté des enregistreurs vidéo numériques, des caméras Web et des caméras connectés à Internet en exploitant des failles comme des micrologiciels désuets ou non actualisables et des noms d'utilisateurs et des mots de passe par défaut qui n'avaient jamais été changés par les utilisateurs finaux. Les pirates ont ensuite utilisé les appareils infectés de l'IdO afin d'attaquer les serveurs de Dyn, une société qui contrôle une bonne partie de l'infrastructure du système des noms de domaine. Cet assaut a été suffisamment puissant pour fermer de nombreux sites Web importants, dont Twitter, Netflix, Spotify et Amazon. La cyberattaque contre Dyn n'est pas un « cygne noir »

(événement isolé). Stroz Friedberg, un chef de file de la gestion des risques associés à la cybersécurité, prédit que les cyberattaques visant les appareils de l'IdO continueront de constituer une menace grave.

Aux États-Unis, la Federal Trade Commission (la « FTC ») a exhorté les fabricants d'appareils de l'IdO à protéger davantage les consommateurs, à la fois durant et après le cycle de vie des produits, et a émis des lignes directrices détaillées dans ses rapports de 2015 intitulés *Internet of Things: Privacy & Security in a Connected World* et *Careful Connections: Building Security in the Internet of Things*.

En particulier, la FTC a recommandé aux fabricants d'intégrer dès le départ un système de sécurité à leurs appareils, de former leurs employés sur l'importance de la sécurité, d'assurer une surveillance raisonnable des pratiques en matière de sécurité des tiers fournisseurs, d'avoir recours à plusieurs niveaux de sécurité pour se défendre contre un risque particulier, d'employer des mesures pour empêcher les utilisateurs non autorisés d'accéder à l'appareil, aux données ou aux renseignements personnels d'un consommateur stockés sur le réseau, de faire un suivi des appareils connectés tout au long de leur cycle de vie prévu et de fournir des correctifs de sécurité, au besoin.

Aux États-Unis, la Food & Drug Administration (la « FDA ») est également préoccupée par la sécurité de l'IdO auquel des appareils médicaux sont connectés. Dans son rapport de 2016 intitulé *Postmarket Management of Cybersecurity in Medical Devices*, la FDA prévient que les pirates informatiques ciblent constamment des appareils médicaux et des hôpitaux. Au même titre que la FTC, la FDA a souligné que les fabricants doivent porter une attention particulière à la cybersécurité des appareils de l'IdO pendant leur cycle de vie : conception, élaboration, production, distribution, déploiement et maintenance.

D'après le rapport de la FDA, les vulnérabilités en matière de cybersécurité peuvent compromettre le fonctionnement des appareils, causer la perte de données personnelles et médicales, et exposer ces appareils à des menaces à leur sécurité provenant d'autres appareils connectés, ce qui pourrait faire en sorte qu'un patient tombe malade, se blesse ou décède.

Dans ses directives, la FDA recommande aux fabricants d'appareils de mettre en œuvre un programme structuré et complet visant à gérer les risques associés à la cybersécurité et à régler les problèmes de cybersécurité avant et après la mise en marché des appareils médicaux, de même que d'appliquer les directives du *Framework for Improving Critical Infrastructure Cybersecurity* publié par la National Institute of Standards and Technology.

Quelles sont les mesures que les entreprises peuvent prendre pour gérer les risques liés à la sécurité et à la protection de la vie privée que suscite l'IdO? Mettez en pratique les mesures concrètes ci-dessous afin de créer un IdO plus sécuritaire qui protégera mieux les renseignements personnels.

MESURES CONCRÈTES POUR GÉRER LES RISQUES LIÉS À LA SÉCURITÉ ET À LA PROTECTION DE LA VIE PRIVÉE

Préparation

- Déterminer la nature de l'information recueillie par l'appareil (son origine, son utilisation et avec qui elle est partagée et dans quels buts).
- Classer l'information selon deux catégories, soit « critique » (nécessaire au fonctionnement de l'appareil), soit « facultative » (renseignement pouvant être utile ou servir à apporter des améliorations, mais non essentiel au fonctionnement de l'appareil).
- Effectuer une évaluation des conséquences sur la protection de la vie privée afin de cerner les risques à cet égard et de songer à des moyens de les gérer et de les mitiger.
- Se familiariser avec les lois en vigueur en matière de protection des données dans les territoires où l'appareil sera utilisé.
- Évaluer si d'autres lois pourraient s'appliquer à l'appareil ou aux personnes ou aux entreprises qui l'utiliseront.
- Déterminer et comprendre les limites techniques de l'appareil qui peuvent nuire à sa sécurité.
- Connaître les menaces au sein de l'environnement actuel.

Mise en œuvre

- Restreindre la collecte, l'utilisation et la communication de renseignements personnels à ce qui est raisonnable et nécessaire au fonctionnement de l'appareil.
- S'assurer que la collecte, l'utilisation ou la communication de renseignements personnels qui ne sont pas critiques sont considérées comme facultatives.
- Décrire dans un style clair et simple les pratiques de traitement des renseignements personnels, et obtenir le consentement des utilisateurs. Utiliser des avis en temps réel et d'autres mécanismes d'obtention du consentement améliorés, au besoin.
- Mettre en œuvre des mesures de contrôle de la sécurité adéquates, en ce qui a trait à la nature de l'appareil, à la nature des renseignements recueillis, à la façon dont l'information est conservée, et aux menaces relevées.
- Conserver uniquement les renseignements personnels qui sont nécessaires au fonctionnement de l'appareil.
- Faire appel à des experts en matière d'anonymisation des renseignements personnels pour s'assurer que ce travail est effectué efficacement.

Évaluation

- Revoir régulièrement les mesures de sécurité existantes et les mettre à jour, au besoin, compte tenu des changements aux menaces ou aux normes de l'industrie, ou des expériences d'utilisation de l'appareil.
- Passer régulièrement en revue les politiques en matière de protection de la vie privée et le libellé des consentements, et chaque fois qu'un changement est apporté à l'appareil ou aux lois applicables sur la protection des données.

COMMUNIQUEZ AVEC NOUS

Sunny Handa
Associé
514-982-4008

Hélène Deschamps Marquis
Associée
514-982-4042

Wendy Mee
Associée
416-863-3161

Kristin Ali
Avocate
416-863-2678