L'essor rapide de l'Internet des Objets (l'IdO) a donné naissance à une nouvelle génération d'appareils et de services qui nous conduisent vers l'ère la plus importante sur le plan de l'innovation et de la croissance depuis le lancement d'Internet. Les solutions IdO changent la donne, offrant aux consommateurs, aux entreprises et aux gouvernements du monde entier d'innombrables avantages.

Moniteurs d'activité physique, thermostats « intelligents », jouets avec fonctionnalités en ligne, villes et services de santé connectés... Il ne fait aucun doute que la société est à l'aube d'une nouvelle ère technologique. Selon les prévisions d'analystes reconnus de l'industrie, 6,4 milliards d'appareils connectés seront utilisés dans le monde en 2016 et ce nombre pourrait atteindre 20,8 milliards d'ici 2020. Cette année, par exemple, plus de 5 millions de nouveaux appareils sont connectés chaque jour.[1]

« Un écosystème basé sur la confiance et l'innovation où des avantages pour la société et le commerce se concrétisent lorsque l'on accorde la priorité à la sécurité et à la confidentialité. »

Comme c'est le cas avec la plupart des technologies émergentes, il reste des défis à relever avant que nous puissions profiter pleinement de ces avantages. Neuf Américains sur dix considèrent qu'il serait important qu'un contrôle soit exercé sur les renseignements collectés à leur sujet. Parallèlement, les utilisateurs n'ont jamais été aussi peu convaincus que leurs données demeurent réellement sécurisées et privées.[2] En ce qui concerne l'Internet des Objets, les craintes des consommateurs en matière de sécurité et de confidentialité sont citées comme les deux principaux obstacles à l'adoption de technologies IdO.[3]

Dans de nombreux cas, ces craintes sont justifiées. Des chercheurs et des individus mal intentionnés continuent de nous montrer les différentes manières dont un appareil IdO non sécurisé peut nous nuire collectivement. Bien que la mise sur le marché d'appareils « sécurisés par défaut » soit un objectif à atteindre, de trop nombreux appareils actuels comportent des vulnérabilités qui auraient pu être évitées.[4] Si aucune mesure n'est prise à cet égard, les appareils IdO risquent de devenir des outils qui, entre de mauvaises mains, donneront lieu à des abus et à des perturbations très importantes.

Afin que les avantages économiques et sociaux que peut offrir l'IdO puissent se concrétiser, nous devons aborder toutes ces questions de sécurité, de confidentialité et de gouvernance de manière globale. Il nous faudra faire preuve d'innovation, de leadership et de collaboration. Si toutes les parties prenantes peuvent s'unir et parvenir à un consensus, les avantages seront quadruples : non seulement nous connaîtrons une croissance économique, mais nous garderons également les réglementations trop sévères à distance, accroîtrons la résilience des infrastructures critiques et

contribuerons à l'évolution de l'IdO.

L'Online Trust Alliance (OTA) estime qu'en favorisant un dialogue public-privé, nous pouvons surmonter les différents défis auxquels nous faisons face et créer un monde connecté plus sécuritaire et plus fiable. L'OTA a agi à titre d'organisme rassembleur, réunissant des développeurs, des fournisseurs et des décideurs politiques pour que ces défis soient relevés de manière proactive grâce à des meilleures pratiques, des normes et des études de référence.

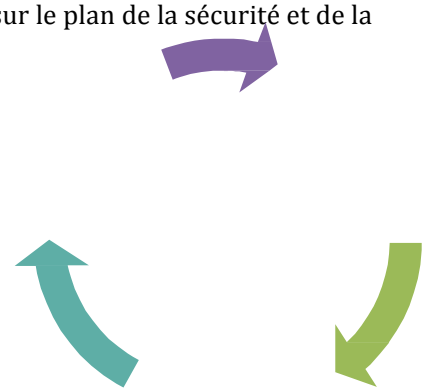
En collaborant avec toutes les parties prenantes, l'OTA s'engage à promouvoir des services en ligne porteurs d'innovation et de vitalité tout en responsabilisant les utilisateurs et en augmentant leur niveau de confiance envers l'IdO. Forte de plus d'une décennie d'expertise et d'engagement en politique publique, en gouvernance d'Internet, en normes et en « deep tech » (innovation profonde), l'OTA aide les parties prenantes à anticiper et à gérer les risques potentiels, tout en contribuant à placer la sécurité et la confidentialité au cœur de leur proposition de valeur.

DÉFIS PARTICULIERS ET UNIQUES

Pour pouvoir assurer la sécurité de l'IdO, il est nécessaire d'avoir une compréhension nuancée de ses caractéristiques uniques. Tout d'abord, l'écosystème de l'IdO est composé de trois dimensions : l'appareil ou le capteur, les applications de prise en charge et les services dorsaux/infonuagiques.[5] En combinaison avec les chaînes logistiques individuelles de ces dimensions, chaque facette et chaque couche de données constitue un risque potentiel.[6]

Chaque dimension de l'IdO doit être sécurisée, et ce, sur plusieurs couches. Au fur et à mesure qu'ils communiquent et en viennent à dépendre les uns des autres, tous les flux de données doivent être sécurisés. Mais alors que de plus en plus de cas de violation de données, de vol d'identité et d'espionnage parrainés par certains États sont mis au jour, les consommateurs et les entreprises sont de plus en plus réticents à partager leurs données personnelles et professionnelles. Les entreprises devront prouver qu'elles accordent la priorité à la vie privée par le biais de pratiques responsables. En adoptant des principes transparents de collecte, d'utilisation, de partage et de propriété de données, nous pouvons collectivement faire en sorte que l'IdO atteigne le niveau nécessaire sur le plan de la sécurité et de la confidentialité.

Comprendre ces relations complexes et savoir qui est responsable de leur protection est essentiel lorsqu'il s'agit de sécuriser presque tous les systèmes. Ce qui rend l'IdO différent, c'est que les actions sont exécutées dans la sphère physique plutôt que la sphère numérique : les portes sont déverrouillées, les températures sont abaissées, l'insuline est injectée et les systèmes d'extinction d'incendie sont activés. Si l'intégrité de données ou d'appareils est compromise, si la connexion est interrompue ou si des fonctionnalités sont contrôlées à distance par des individus malveillants, les conséquences peuvent être catastrophiques.



DÉVELOPPEMENT DURABLE DE L'IDO

Intégrer des mesures et dispositifs visant à protéger la sécurité et la confidentialité au tout début de la conception et du développement est le moyen le plus efficace de commercialiser des appareils IdO qui sont sécurisés et de faire en sorte qu'ils le demeurent. Les processus, les technologies et les stratégies qui visent à protéger les utilisateurs requièrent une prise en charge continue tout au long du cycle de vie des appareils et des données. La prise en charge après la garantie (ce qui comprend la facilité d'utilisation, la gestion des correctifs, la propriété des données et la portabilité) doit faire partie de toute démarche. Définis par le terme « développement durable », ce sont les implications et les risques liés aux appareils sans correctifs, discontinués ou brisés qui sont essentiels à la réalisation des promesses de l'IdO. Le développement durable inclut également les problèmes de politique, de gouvernance et de réglementation liés à la propriété et à la transférabilité des appareils et des données d'utilisateurs. Étant donné que les appareils peuvent survivre à un propriétaire ou être transférés à de nouveaux acheteurs — dans le cas de maisons intelligentes, par exemple —, les consommateurs et les entreprises ont besoin de savoir que les entreprises continueront de répondre à leurs besoins après l'expiration de leur garantie traditionnelle. Parallèlement, il est important de reconnaître d'abord qu'il est impossible d'assurer de façon totale et parfaite la sécurité et la confidentialité. Ensuite, il faut reconnaître que toute technologie a une durée de vie donnée. Peu importe l'appareil concerné, le

~~soutien fourni aux utilisateurs finira par diminuer en intensité avant de cesser, tout simplement.~~

L'utilisation continue d'appareils obsolètes et abandonnés par leur fabricant fera en sorte qu'ils soient peu sécuritaires et qu'ils risquent d'être ciblés ou exploités. Le système d'opération Windows XP est un bon exemple de ce phénomène. Bien que Microsoft fournisse aux utilisateurs de Windows XP un service d'assistance gratuit depuis plus de 10 ans, des millions d'appareils fonctionnent toujours avec ce système, ce qui constitue un risque.[7] Un peu comme le fait de conduire un Modèle T de Ford sur une autoroute moderne. Limités par leur architecture matérielle, ces appareils, logiciels et systèmes ne sont plus sécuritaires sur l'autoroute numérique actuelle. Malheureusement, bien que de telles solutions puissent être sécuritaires lors de leur mise en marché, aucun correctif — aussi astucieux soit-il — ne peut résoudre les problèmes de conception liés à des menaces imprévues survenant des décennies plus tard.

Dans une optique de développement durable, les entreprises envisagent de plus en plus un modèle de service ou d'abonnement pour fournir du soutien, des mises à jour de sécurité et des mises à jour fonctionnelles pour toute la durée de vie d'un produit — après une période initiale de soutien gratuit. Offrir du soutien de façon continue permettra aux entreprises d'incorporer le développement durable dans leurs modèles commerciaux et de démontrer leur engagement à long terme envers la sécurité et la confidentialité des données des utilisateurs. Et bien entendu, cela leur donnera l'occasion d'offrir des fonctionnalités, des services et une compatibilité supplémentaires.

Il n'y a pas de solution unique; la portée et l'engagement en matière de développement durable sont des éléments que chaque entreprise doit évaluer et à propos desquels elle doit prendre des décisions. L'anticipation de ces besoins et de ces coûts est essentielle pour le modèle financier d'une entreprise et sa capacité à soutenir ses clients au fil des ans. Une entreprise qui communique avec précision cet engagement à sa clientèle avant un achat nourrit des attentes réalistes et protège sa marque et sa réputation : c'est tout simplement un bon modèle d'affaires. Bien que tous les intervenants doivent aujourd'hui faire face à ces problèmes de sécurité et de confidentialité, ces derniers peuvent facilement être résolus. Si nous travaillons ensemble et prenons les devants en matière de transparence, de sécurité et de confidentialité, nous pouvons nous assurer que les utilisateurs aient une confiance suffisante envers le système pour que l'IdO atteigne son véritable potentiel.

Cadre de confiance de l'IdO

La confiance des utilisateurs dans la capacité des différentes entités à préserver la sécurité et la confidentialité des données diminue, ce qui fait en sorte qu'il est de plus en plus difficile de convaincre les utilisateurs de partager leurs renseignements. Ironiquement, dans de nombreux cas, ce sont ces mêmes données qui donnent leur valeur aux solutions IdO. Des échanges équitables et ouverts entre les entreprises et les consommateurs nous aideront à comprendre les avantages et les obligations liés à l'IdO.

Si les particuliers et les entreprises ne peuvent pas croire que leurs données personnelles et propriétaires seront conservées de manière sécurisée et privée, l'adoption à grande échelle de l'IdO ne sera pas réalisée et les appels à une législation réglementaire augmenteront. Déjà, les législateurs de l'Union européenne envisagent des règles qui pourraient obliger les entreprises à passer par un processus de certification pour se conformer aux nouvelles normes de sécurité et garantir la confidentialité des données des utilisateurs.[8]

Pour résoudre ces problèmes combinés, l'OTA a établi un groupe de travail intersectoriel chargé de créer un cadre de confiance pour l'IdO, un modèle volontaire d'autorégulation.[9] Grâce à un processus de 18 mois axé sur l'atteinte de consensus et impliquant plus de 100 parties prenantes, l'OTA a identifié 31 critères initialement centrés sur les technologies liées aux maisons, aux bureaux et aux technologies portables connectés. Servant de code de conduite volontaire, ce cadre de confiance sert aujourd'hui de base à plusieurs programmes de certification et d'évaluation des risques de l'IdO qui, selon les

prévisions, serviront à leur tour de base à de futures initiatives « Safe Harbor » (sphère de sécurité).[10]

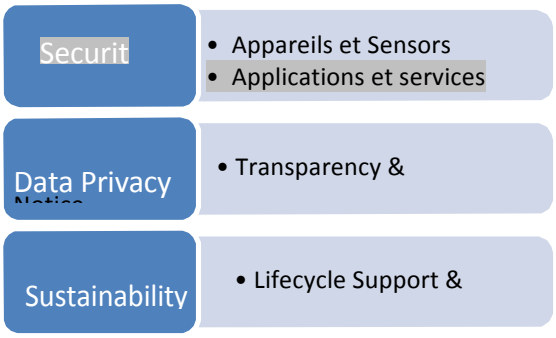
Ces critères mesurables aident les entreprises à évaluer les risques auxquels elles sont exposées et à s'attaquer aux questions de sécurité et de confidentialité en devenant des intendants et des défenseurs des éléments critiques de l'IdO pour les utilisateurs. En exploitant ce cadre de confiance et autres ressources de l'OTA, les entreprises peuvent démontrer qu'elles s'engagent à contribuer à un avenir sûr et fiable pour l'IdO.

Le cadre de confiance fournit une voie vers une autorégulation significative. Si le secteur privé peut démontrer son engagement en matière de sécurité et de respect de la vie privée, les gouvernements se sentiront moins obligés de réglementer l'IdO et l'innovation aura le champ libre. Après tout, des réglementations imposées de l'extérieur — plutôt que des meilleures pratiques et des normes générées suite au consensus des parties prenantes — peuvent conduire à une culture de conformité inefficace et insuffisante pour tout le monde.

TRAVAILLER ENSEMBLE POUR STIMULER LA CONFIANCE ET L'INNOVATION

L'avenir de l'IdO est certes prometteur, mais il ne pourra être réalisé si nous n'abordons pas simultanément les questions de sécurité et de confidentialité. Au cours de la prochaine décennie, ces deux éléments deviendront des critères clés que les consommateurs, les entreprises, l'industrie et le gouvernement exigeront. Sécuriser et protéger les éléments les plus importants — nos systèmes, nos données et notre vie privée — est une responsabilité partagée.

Bien que l'industrie évolue et adopte déjà des normes concernant l'interopérabilité et les différentes plateformes, elle doit également intégrer dans la pratique des principes de base en matière de confiance. De tels principes ne peuvent pas être abordés à mi-chemin; ils doivent être conçus dès le départ. Créer de façon transparente une culture de sécurité, de vie privée et de développement durable aura de nombreux avantages à long terme pour la société.



L'OTA fournit un forum où les parties prenantes peuvent discuter en toute confiance d'idées, de politiques, de technologies et de pratiques afin que tous ensemble, nous puissions en arriver à un consensus en fonction duquel l'industrie pourra — et devra — fonctionner. Grâce au processus de consultation de l'OTA, nous pouvons aider nos membres à développer les meilleures pratiques et à promouvoir des politiques publiques équilibrées. Et par le biais de groupes de travail et de relations stratégiques avec des spécialistes du marketing interactif et de la publicité, de la technologie, de la vie privée et des politiques publiques, l'OTA fournit une vision et des renseignements stratégiques à nos membres pour les aider à prospérer et à innover en évitant les nombreux nids-de-poule et obstacles en cours de route.

L'OTA est une initiative de l'Internet Society (ISOC), une organisation caritative à but non lucratif 501c3 dont l'objectif est d'assurer l'évolution, l'utilisation et le développement ouverts d'Internet au profit de tous les peuples du monde. La mission de l'OTA : accroître le niveau de confiance de la population envers Internet, promouvoir la responsabilisation des utilisateurs et encourager l'innovation. Les méthodes privilégiées : organiser des initiatives multipartites, ainsi que développer et faire la promotion de meilleures pratiques, de pratiques éthiques en matière de confidentialité et de la gouvernance des données. Pour en savoir plus, consultez le https://otalliance.org et le https://www.internetsociety.org/.

© 2017 Online Trust Alliance. Tous droits réservés.

[3] Accenture 2016 Consumer Survey https://www.accenture.com

[1] Gartner IoT Forecast http://www.gartner.com/newsroom/id/3165317

[2] Pew Research Center. (2015). Americans' attitudes about privacy, security and surveillance http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

/us-en/insight-ignite-growth-consumer-technology

[4] Recherche de l'ORA, 8 septembre 2016 https://otalliance.org/IoTvulnerabilities

[5] National Institute for Standards & Technology "Networks of "Things." http://doi.org/doi:10.6028/NIST.SP.800-183 [6] Symantec Internet Security Threat Report, avril 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[7] La fin du support de Windows XP https://support.microsoft.com/fr-ca/help/14223/windows-xp-end-of-support

[8] Commission de l'UE https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/

[9] OTA announced IoT Working Group May 2015 https://otalliance.org/oTWGannounce

[10] RSA Conference Framework Release March 2, 2016 https://otalliance.org/IoTFW-release r10-25