



Commissariat
à la protection de
la vie privée du Canada

Les accessoires intelligents

Défis et possibilités pour la protection de la vie privée

*Rapport préparé par le Groupe de recherche du Commissariat à la
protection de la vie privée du Canada*

Table des matières

Introduction	Error! Bookmark not defined.
1. Qu'est-ce qu'un accessoire intelligent?	Error! Bookmark not defined.
2. Aperçu des répercussions sur la vie privée	Error! Bookmark not defined.
3. Les lois canadiennes sur la protection de la vie privée et les accessoires intelligents	Error! Bookmark not defined.
4. Critères de conception choisis pour les accessoires intelligents	Error! Bookmark not defined.
Conclusion.....	Error! Bookmark not defined.

Résumé

Le but du présent rapport de recherche est d'aider le Commissariat à la protection de la vie privée du Canada à mieux comprendre les répercussions de la technologie des accessoires intelligents sur la vie privée pour donner des avis éclairés au Parlement, définir des positions de principe et mener à bien les activités futures en matière de conformité. La rapidité de l'innovation technologique, la demande des consommateurs et la baisse des coûts favorisent le développement et l'adoption d'une nouvelle génération d'accessoires à porter sur soi. Ces accessoires, que l'utilisateur porte sur son corps et qui sont parfois fixés à son téléphone intelligent, peuvent accroître le risque de suivi et de profilage qui caractérise l'écosystème mobile actuel. Le présent rapport donne un aperçu des accessoires intelligents et de leurs répercussions sur la vie privée. Après une analyse de l'application des lois fédérales en matière de protection de la vie privée dans cet environnement, le rapport expose certaines considérations concernant la conception des accessoires intelligents dans le but de renforcer les protections de la vie privée intégrées. En conclusion, il fait état de certaines mesures à venir éventuelles.

Introduction

Le nombre d'accessoires intelligents à porter sur soi actuellement offerts sur le marché de la consommation est limité, mais de nombreux autres seront probablement lancés prochainement. Les accessoires intelligents sont appelés à devenir un aspect beaucoup plus important de notre vie. Lorsque le Commissariat s'est penché sur la question des capteurs dans son document d'orientation à l'intention des concepteurs d'applications mobiles, il a parlé de capteurs permettant la géolocalisation qui, associés à des données sur nos faits et gestes, brossent notre portrait intime. Les accessoires intelligents *animent* ce portrait¹.

Le présent rapport de recherche met l'accent sur les caméras et les technologies à porter sur soi, mais le Commissariat a également examiné la capacité de surveillance inhérente à d'autres technologies mobiles, par exemple les véhicules aériens sans pilote², qui commencent à faire partie de notre environnement. L'avènement des accessoires à porter sur soi complique et accroît le risque d'atteinte à la vie privée dans l'environnement mobile en recueillant des renseignements personnels supplémentaires qui dévoilent l'intimité. Certes, les différences entre un téléphone intelligent et de nombreux accessoires intelligents sont davantage une question de degré que de nature, mais elles n'en sont pas moins importantes du point de vue de la protection de la vie privée. Nombre de ces accessoires constituent une extension des capacités actuelles des téléphones intelligents. Combinés avec d'autres données, les renseignements que l'utilisateur peut communiquer activement constituent une précieuse ressource. De nombreux types de capteurs possèdent des capacités différentes. Par exemple, certains permettent de recueillir, en temps réel, de l'information sur :

- le corps de l'utilisateur : son humeur, ses habitudes, ses activités physiques, son état de santé, la vitesse à laquelle il se déplace et sa mobilité;
- l'environnement de l'utilisateur : les images, les sons, la température, l'humidité, le lieu, l'environnement social ainsi que les données générées par ordinateur pour influencer sur l'expérience de l'utilisateur dans le monde qui l'entoure.

Une caméra ne peut capter que quelques-uns de ces éléments, mais la fonction caméra est à l'origine de nombreuses préoccupations actuelles concernant le respect de la vie privée³. C'est la capacité de ces accessoires de faire des enregistrements, possiblement en continu et secrètement, qui soulève de nombreuses préoccupations. Fait intéressant, les caméras personnelles, qui font toujours face au côté opposé

à celui qui les porte, ne peuvent en fait pas capter d'image de l'utilisateur contrairement aux téléphones intelligents équipés de caméras réversibles, qui permettent d'intégrer aisément l'utilisateur aux images. La grande disponibilité récente de nombreux accessoires intelligents attrayants sur le marché de la consommation à des prix accessibles fait ressortir l'urgence de parvenir à une compréhension plus nuancée de leurs conséquences sur le plan de la vie privée. Les concepteurs sont en voie de surmonter plusieurs obstacles qui ont freiné l'adoption des premiers accessoires intelligents, par exemple la durée de vie des piles, l'esthétisme et la convivialité⁴, et nous pouvons nous attendre à ce que les cycles de développement dans ce créneau soient aussi rapides que dans l'écosystème des applications mobiles.

Nous savons que la communication d'information pertinente sur les choix en matière de protection de la vie privée représente un défi particulier dans l'espace mobile, où l'écran est petit et l'attention de l'utilisateur intermittente. Comme nous l'avons souligné dans notre document d'information à l'intention des concepteurs d'applications mobiles⁵, en raison de ces caractéristiques de conception, il est encore plus difficile de communiquer aux utilisateurs la bonne information sur leur droit à la vie privée, sous une forme qu'ils peuvent comprendre et au bon moment, pour qu'ils puissent faire des choix éclairés.

Dans le cas des accessoires intelligents, il est encore plus difficile de joindre l'utilisateur. Qui plus est, ces accessoires amplifient la difficulté de protéger la vie privée des non-utilisateurs, qui pourraient faire l'objet d'enregistrements audio et vidéo. Le présent rapport porte principalement sur les accessoires dotés d'une caméra, car ils sont actuellement au cœur du débat public. La recherche présentée ici est fondée sur notre connaissance de l'environnement et des technologies à porter sur soi à l'heure actuelle. Elle pourra être mise à jour au besoin en fonction des changements observés dans l'écosystème des accessoires intelligents et dans l'environnement technologique et social dans son ensemble.

1. Qu'est-ce qu'un accessoire intelligent?

Un accessoire intelligent est un ordinateur miniature que l'on porte sur soi ou un capteur que l'on fixe sur ou sous un vêtement ou qui y est intégré⁶. La conception actuelle des accessoires intelligents vise une interaction constante entre l'utilisateur et l'ordinateur, où l'ordinateur « apprend » de l'expérience de l'utilisateur, au moment où ce dernier vit cette expérience et l'associe à des renseignements supplémentaires.

D'après une étude de marché réalisée en 2013⁷, le marché des technologies à porter sur soi se divise actuellement en quatre grands segments :

- applications en lien avec la condition physique, le bien-être et le suivi vital (p. ex. vêtement intelligent, lunettes de sport intelligentes, moniteur d'activité ou capteur de sommeil) susceptibles de plaire à des consommateurs qui ont tendance à suivre de près de nombreux aspects de leur vie⁸;
- applications d'infodivertissements (p. ex. montre intelligente, casque de réalité virtuelle ou lunettes intelligentes);
- applications sanitaires et médicales (p. ex. glucomètre permanent ou ensemble timbre et biocapteur⁹);
- applications industrielles, policières et militaires (p. ex. terminal à porter sur la main, caméra à porter sur soi, casque de réalité virtuelle).

Il est peut-être utile de classer les accessoires intelligents par catégories de cette façon, mais on risque ainsi de négliger des façons créatives de les utiliser dans différents domaines. Ces accessoires offrent en effet un large



Source : Shutterstock

éventail de capacités. Les innovations abondent dans différents aspects des accessoires intelligents à porter sur soi et nous ne pouvons tous les couvrir ici.

a) Caractéristiques des accessoires intelligents

De nombreuses technologies à porter sur soi en développement à l'heure actuelle ou déjà sur le marché comportent des caractéristiques attrayantes¹⁰ qui pourraient inciter les consommateurs à les adopter à grande échelle. Par exemple :

- elles ont une facture visuelle attrayante¹¹;
- elles peuvent s'intégrer parfaitement aux vêtements ou au corps l'utilisateur ou à un téléphone intelligent;
- elles peuvent être personnalisées et adaptées aux besoins de l'utilisateur et donner de la rétroaction;
- elles peuvent compléter les capacités physiques ou mentales de l'utilisateur;
- elles offrent un bon rapport coûts-avantages;
- elles sont polyvalentes et se prêtent à toute une gamme d'applications dans la vie personnelle ou au travail;
- elles ont une configuration et un mode de fonctionnement relativement simples.

Compte tenu de ces caractéristiques possibles, même un observateur occasionnel peut voir l'aspect attrayant des accessoires intelligents à porter sur soi.

b) Différences entre les accessoires intelligents et l'informatique mobile

Nombre d'accessoires à porter sur soi peuvent être déployés et utilisés en tout temps, tandis que l'on garde souvent son téléphone intelligent à la main, dans sa poche ou dans un sac. Cette distinction pourrait bien s'estomper avec les nouvelles façons de porter le téléphone intelligent sur le corps. Toutefois, pour le moment, certains accessoires à porter sur soi pourraient accroître le risque d'atteinte à la vie privée dans l'environnement mobile en recueillant des images ainsi que des enregistrements audio et vidéo de façon discrète, voire secrète, et en permettant de recueillir ces renseignements personnels dans des situations où un accessoire comportant une caméra visible serait inacceptable sur le plan social.

c) Prévisions de croissance du marché et éléments militant en faveur de l'adoption des accessoires intelligents

Les prévisions actuelles concernant l'adoption des accessoires intelligents sur le marché varient, mais elles indiquent toutes une croissance appréciable. D'après Juniper Research, l'année 2014 devrait être décisive pour les accessoires à porter sur soi¹². IMS Research prévoyait en 2012 que 171 millions de ces accessoires seraient livrés d'ici 2016¹³. ABI Research a prévu que le marché connaîtrait une croissance formidable pour atteindre le chiffre astronomique de 485 millions d'accessoires intelligents livrés annuellement d'ici 2018¹⁴. BI Intelligence entrevoit une croissance plus modeste, qui ferait passer le nombre d'accessoires livrés de 100 millions en 2014 à 300 millions d'ici cinq ans¹⁵.

À l'heure actuelle, les sports et le suivi de l'activité sont les domaines qui présentent le plus fort potentiel de croissance, mais le marché des accessoires intelligents à porter sur soi pourrait bien ne pas atteindre sa pleine mesure avant que la technologie ne soit parfaitement intégrée à nos vêtements, qu'elle ne devienne transparente et invisible¹⁶ et que nous n'ayons plus à tendre la main pour prendre notre téléphone. L'hypothèse selon laquelle Apple offrirait d'autres technologies à porter sur soi tout aussi révolutionnaires que le iPhone au moment de son lancement en 2007¹⁷ va grandissant, alimentée par différentes rumeurs faisant état de demandes de brevet pour une « iWatch »¹⁸ et l'embauche récente d'un spécialiste du prêt-à-porter de luxe¹⁹. L'adoption généralisée du téléphone intelligent est un autre élément qui accroît la probabilité que les gens achètent des accessoires à porter sur soi attachés à ces téléphones.

Les nouveaux modèles d'affaires qui stimulent l'adoption des accessoires intelligents à porter sur soi seront importants pour surveiller et comprendre la situation. Par exemple, les entreprises qui vendent des accessoires pour le suivi de la condition physique peuvent s'attacher à faire valoir auprès des consommateurs que les produits améliorant la condition physique, mais elles pourraient aussi souhaiter utiliser cette information pour cibler et personnaliser la publicité.

d) Des aides visuelles à réalité adaptée

Historiquement, tout comme le passage de la montre de poche à la montre-bracelet²⁰, les exemples d'accessoires intelligents à porter sur soi montrent comment la relation entre la personne et la machine a évolué pour répondre à des questions ou résoudre des problèmes en particulier. En outre, les technologies d'assistance à porter sur soi existent depuis des siècles. Par exemple, les technologies d'assistance pour la vision sont passées de la loupe aux lunettes puis aux lentilles cornéennes²¹. La Federal Drug Administration des États-Unis a récemment approuvé des implants rétiniens²² qui, associés à des lunettes et à un ordinateur leur envoyant un signal, peuvent aider des patients aveugles à acquérir une certaine capacité visuelle.



Source : Shutterstock

Certains accessoires à porter sur soi associent des sons, des images, des graphiques ou des renseignements relatifs à la géolocalisation à ce que voit l'utilisateur. Par exemple, les lunettes OrCam9F²³ offertes sur le marché permettent d'identifier des personnes ou des objets pointés par l'utilisateur et utilisent ensuite une technologie de conduction osseuse pour communiquer cette information à l'utilisateur, et ce, à un coût similaire à celui d'une prothèse auditive²⁴. Innovega a développé un système de réalité amplifiée appelé « iOptik », qui projette un affichage frontal sur des lentilles cornéennes à partir de lunettes spéciales²⁵. Les accessoires à porter sur soi à réalité amplifiée peuvent superposer des sons, des images, des graphiques ou des données GPS²⁶. Steve Mann, inventeur canadien et pionnier des accessoires intelligents à porter sur soi, a aussi développé plusieurs accessoires visuels à réalité « diminuée » permettant de *réduire* ou de simplifier de façon sélective l'information que voit l'utilisateur. Une application commerciale de cette technologie serait un casque vidéo communiquant en temps réel aux soudeurs des renseignements détaillés et exacts sur la flamme, tout en leur protégeant les yeux²⁷. Le filtrage de la lumière constitue une application, mais les accessoires intelligents à porter sur soi pourraient filtrer d'autres façons l'expérience de l'utilisateur. Nous y reviendrons de façon plus approfondie dans la conclusion du présent rapport.

e) Applications des accessoires intelligents

Les accessoires intelligents à porter sur soi pourraient bien révolutionner plusieurs secteurs en réduisant les obstacles matériels aux interactions avec le monde numérique²⁸. Nous présentons ci-après certains produits actuellement offerts sur le marché de la technologie auxquels se sont intéressés les médias l'an dernier. On observe des points communs intéressants dans les applications technologiques pour les différents marchés comme les activités de loisir, les milieux de travail industriels et les soins aux patients. Par exemple, un assistant numérique à commande vocale développé par Kopin appelé « Golden-i », qui aide à établir l'ordre de priorité des activités et à filtrer l'information, pourrait avoir de nombreuses applications variées²⁹. Des assistants numériques intelligents de nouvelle génération, comme la technologie de superordinateur Watson de questions-réponses d'IBM que l'on commence à intégrer aux téléphones intelligents³⁰, seront développés pour les accessoires à porter sur soi dans l'avenir.

Condition physique, bien-être et suivi des fonctions vitales

Si l'individu était considéré à une certaine époque comme un simple sujet sur lequel on accumulait des données, les accessoires intelligents à porter sur soi lui offrent désormais la possibilité de participer activement à la collecte, à l'utilisation et à la communication de très grandes quantités de données sur lui-même et ceux qui l'entourent. Par exemple, le minuscule accessoire photo Narrative, que l'utilisateur porte autour du cou, lui permet de capter des moments de la vie quotidienne en se déclenchant toutes les 30 secondes pour documenter ses activités tout au long de la journée³¹.

Selon une estimation, le marché des accessoires de surveillance sans fil pour le sport et la santé atteindra près de 170 millions d'accessoires d'ici 2017³². Dans la catégorie condition physique et bien-être, on trouve une panoplie de « bracelets vitaux », comme le Nike+ FuelBand³³, le Fitbit 28F³⁴, le Bodymedia³⁵ et le Jawbone UP30F³⁶, qui mesurent le niveau d'activité quotidien et calculent les calories brûlées. Qui plus est, ce type d'accessoire se sert du téléphone intelligent de l'utilisateur pour établir une liaison avec une application infonuagique qui évalue les données, lui donne des conseils et lui permet de communiquer les résultats aux membres de son groupe. En outre, une mini-oreillette de nouvelle génération diffuse de la musique, tout en mesurant les données biométriques et physiologiques en temps réel et en les transmettant au téléphone intelligent de l'utilisateur³⁷. Le suiveur d'activité Shine est un bon exemple d'accessoire petit, léger et attrayant associé au téléphone intelligent de l'utilisateur. On trouve aussi une variété de montres intelligentes, par exemple la Pebble³⁸ et la Galaxy Gear³⁹ de Samsung, qui établissent une connexion sans fil avec le téléphone intelligent de l'utilisateur.



Source : Shutterstock

Accessoires d'infodivertissement (et activités connexes)

Les caméras GoPro sont devenues très populaires auprès des amateurs de sport pour enregistrer des vidéos ou prendre des photos d'eux-mêmes, mais l'aspect pratique, les fonctions et le coût relativement modique de ces accessoires favorisent leur adoption dans d'autres activités ou domaines⁴⁰.

Les Google Glass⁴¹, en fait un ordinateur porté sur la tête, ont retenu l'attention des autorités internationales de protection de la vie privée⁴². Parmi plusieurs accessoires à porter sur soi comportant des capacités similaires, cet accessoire se distingue peut-être par le vaste potentiel d'intégration avec les autres produits de Google issus de la créativité des concepteurs d'applications à porter sur soi. Par exemple, les Vuzix Smart Glasses M100⁴³, un écran de téléphone intelligent mains libres doté de capteurs intégrés et d'une connectivité Internet, ont été lancées en décembre 2013. Pour leur part, les lunettes Recon Jet, produites par l'entreprise vancouveroise Recon Instruments à l'intention des sportifs, disposent de fonctions autonomes d'un téléphone intelligent. Leur mise en marché est prévue en mars 2014⁴⁴.

La promesse d'expériences de réalité virtuelle se rapproche également avec les avancées dans le domaine de la visualisation immersive. La visière de réalité virtuelle Oculus Rift⁴⁵ pour jeux immersifs, qui est en développement à l'heure actuelle, a aussi des applications pour la formation dans plusieurs domaines à risque élevé. La technologie de stimulation musculaire, actuellement utilisée dans le traitement de la paralysie, pourrait aussi rendre plus intense l'expérience des jeux sur un téléphone intelligent⁴⁶. En utilisant un téléphone mobile, des chercheurs ont connecté leur accessoire à des électrodes placées sur l'avant-bras de l'utilisateur qui font se contracter les muscles du joueur et lui donnent l'impression d'exercer une force en lien avec le jeu⁴⁷.

Les avancées dans le domaine des commandes gestuelles évitent la difficulté de s'en remettre aux commandes vocales et aux caméras. Les Thalmic Labs de Waterloo ont développé le bracelet Bluetooth MYO, qui génère des commandes numériques à partir de capteurs détectant les mouvements dans les muscles de l'avant-bras de l'utilisateur⁴⁸. Vingt-cinq mille de ces bracelets ont été commandés à l'avance au prix de 149 \$ chacun et devraient être livrés en 2014⁴⁹. De plus, une version à porter sur soi du détecteur de mouvements de Microsoft pour le Kinect du Xbox, appelé « Digits », est en développement⁵⁰. Digits peut reproduire sur l'écran les mouvements des bras et des doigts ou permettre de contrôler l'interface d'un jeu d'ordinateur complexe⁵¹. Pour sa part, Leap Motion a déjà lancé un détecteur de mouvements assorti d'une variété d'applications qui permet à l'utilisateur de communiquer avec l'ordinateur en utilisant des gestes de la main⁵².

Applications sanitaires et médicales

Selon une étude menée récemment par PricewaterhouseCoopers, plus du tiers des Canadiens estiment que les applications mobiles dans le domaine de la santé amélioreront l'aspect pratique des soins de santé au cours des trois prochaines années. Près de 80 % des répondants seraient à l'aise d'utiliser un service de surveillance virtuelle pour gérer un problème de santé chronique⁵³. Cette information vient compléter les résultats du Canadian Telehealth Report de 2013, selon lequel les gouvernements provinciaux reconnaissent le potentiel des périphériques médicaux, par exemple les stéthoscopes et caméras numériques, et envisagent d'en introduire l'usage ou d'accroître leur utilisation en télémédecine au cours des prochaines années⁵⁴.

Outre les accessoires qui surveillent la pression artérielle de l'utilisateur pour détecter les signes de crise cardiaque et d'accident vasculaire cérébral, on observe certaines avancées plus révolutionnaires dans le secteur de la santé. Par exemple, le X lab de Google développe actuellement une lentille cornéenne pour aider les diabétiques à surveiller leur taux de glycémie⁵⁵. Proteus Digital Health⁵⁶ développe pour sa part une nouvelle catégorie de produits et de services qu'elle appelle « médicaments numériques ». Il est en effet possible d'ajouter aux médicaments une micropuce digestible de la taille d'un grain de sable déjà approuvée pour certains usages aux États-Unis⁵⁷. Lorsqu'elle réagit aux sucs gastriques, cette micropuce envoie un signal à un timbre sur la peau du patient, qui relaie l'information à un téléphone intelligent qui la relaie à son tour au cabinet du médecin⁵⁸. On peut ainsi communiquer de l'information aux patients eux-mêmes, aux membres de leur famille, au personnel soignant et aux chercheurs afin qu'ils sachent si le patient a pris son médicament et quels effets il a sur lui⁵⁹.

Applications industrielles, policières et militaires

Le système Aviation Warrior de Ratheyon est un casque de pilote équipé d'un écran oculaire rabattable pour montrer une carte, des relevés de géolocalisation et d'autres données de capteurs émises par des indicateurs dans le poste de pilotage lorsque le pilote se trouve loin de l'appareil pour lui donner une idée exacte de la situation en temps réel⁶⁰. Un accessoire est intégré au casque et un téléphone intelligent est attaché au poignet du pilote.

Grâce au Golden-i⁶¹ de Kopin en développement à l'heure actuelle, les préposés à l'entretien et aux réparations, les policiers, les ambulanciers paramédicaux et les pompiers devraient avoir accès à la lecture vidéo en direct, l'accès à Internet mobile, la navigation GPS et des commandes mains libres. En outre, le casque-ordinateur HC1⁶² de Motorola a été conçu pour être utilisé dans le domaine de la mécanique industrielle ou militaire ainsi que par les techniciens des entreprises de services publics, les travailleurs du secteur de la fabrication et les ingénieurs⁶³.

Au Canada, certains corps de police ont mené des projets pilotes portant sur divers types de caméras personnelles, notamment à Victoria en 2009⁶⁴ et à Edmonton en 2012⁶⁵.

2. Aperçu des répercussions sur la vie privée

Dans un récent sondage d'opinion financé par l'industrie et portant sur les répercussions sociales des accessoires intelligents à porter sur soi au Royaume-Uni et aux États-Unis, 51 % des répondants ont cité la protection de la vie privée comme obstacle à l'adoption de ces accessoires. Soixante-deux pour cent estiment que les Google Glass et les autres accessoires intelligents à porter sur soi devraient faire l'objet d'une quelconque réglementation, tandis que 20 % préconisent leur interdiction pure et simple⁶⁶. Forrester Research en conclut que la promesse des accessoires intelligents ne pourra être livrée que si l'on donne aux utilisateurs la maîtrise de leurs propres renseignements, par exemple pour ce qui est de choisir de les communiquer ou non⁶⁷.

a) Difficultés inhérentes au mode de consentement actuel

Les capteurs intégrés à des objets interconnectés, que l'individu les porte sur lui ou qu'il les transporte, peuvent générer une quantité impressionnante de renseignements qu'il est possible de combiner et d'analyser et auxquels on peut donner suite sans la transparence ou la responsabilité appropriées ou sans le consentement explicite des intéressés.

Ces avancées présentent des difficultés considérables pour les cadres de protection de la vie privée existants à l'échelle planétaire. Par exemple, dans un monde où les accessoires informatiques et mobiles sont omniprésents, il devient de plus en plus difficile d'appliquer le principe de limitation de la collecte de renseignements personnels sous réserve du consentement donné à des fins déterminées. De plus, comme le Commissariat à la protection de la vie privée l'a indiqué dans son document d'orientation à l'intention des concepteurs d'applications, il demeure difficile d'obtenir un consentement valable au moyen d'un appareil mobile⁶⁸. Il faut faire davantage pour montrer aux utilisateurs, de manière créative et intelligible, à quoi servent réellement leurs renseignements personnels.

b) Nouvelles options en matière de surveillance

Comme nous l'avons vu, certains accessoires intelligents à porter sur soi prennent des photos et enregistrent des vidéos, des sons, des données de géolocalisation ou l'environnement général autour de l'accessoire, y compris les personnes et les autres accessoires se trouvant à proximité. La caméra intégrée à plusieurs accessoires suscite une foule de préoccupations concernant le respect de la vie privée⁶⁹. Des produits polyvalents et bon marché d'utilisation courante en vente au Canada, par exemple des casquettes de baseball⁷⁰, des lecteurs de musique MP3⁷¹ et des boutons de chemise⁷², sont munis d'une caméra cachée de style James Bond⁷³. Nombre de ces accessoires permettent de faire des enregistrements secrètement en continu.

Toutefois, au-delà des caméras, la nouvelle génération de technologies de suivi de la condition physique devrait ouvrir de nouvelles perspectives aux compagnies d'assurance-maladie et aux employeurs concernant notre état de santé et nos comportements. Ainsi, la Fondation des maladies du cœur et de l'AVC s'est associée avec Desjardins Assurances pour lancer une série d'outils numériques visant à aider les utilisateurs à réduire les risques d'accident vasculaire cérébral (AVC)⁷⁴. Dans le monde du travail, les spécialistes du marketing font la promotion des accessoires intelligents auprès des employeurs comme moyen de réduire les coûts liés à la santé mentale et physique du personnel. L'entreprise canadienne Sprout cite plusieurs clients canadiens pour son programme de suivi de l'activité des employés à l'appui des initiatives des entreprises en matière de santé et de bien-être⁷⁵. Aux États-Unis, la vidéo publicitaire d'Empatica⁷⁶ explique que son accessoire de surveillance des émotions est utilisé dans le cadre de programmes de mieux-être au travail du pays : un bracelet capte en temps réel de l'information sur la pression artérielle de l'utilisateur, sa conduction cutanée, sa température

corporelle et les mouvements de son corps⁷⁷. Il faut ensuite recueillir cette information au moyen du téléphone intelligent de l'utilisateur, puis l'analyser pour déterminer les activités qui induisent un stress et les endroits où cela se produit.

Nous pouvons nous attendre à d'autres avancées de cette nature. Le domaine émergent de la « physiolytique » fera le lien entre les accessoires à porter sur soi et l'analyse des mégadonnées afin de créer un système de rétroaction et de suggestions pour modifier les comportements⁷⁸.

c) Regroupement des données recueillies par les accessoires intelligents

Comme nous l'avons vu dans la recherche du Commissariat sur l'analyse prédictive⁷⁹, nous sommes aux prises avec des défis d'un nouveau genre en matière de protection de la vie privée découlant de la combinaison d'éléments d'information personnels en apparence anodins et non sensibles qui aboutit à un profilage des personnes. D'entrée de jeu, il est difficile pour les individus de prendre une décision éclairée quant à savoir s'ils devraient communiquer des renseignements personnels du fait qu'ils ne sont pas en mesure de pleinement comprendre comment ces renseignements pourront être combinés et utilisés dans l'avenir. Nul doute que les accessoires intelligents qui recueillent, traitent et envoient des données en continu compliqueront encore le problème⁸⁰.

Les accessoires intelligents à porter sur soi pourraient également amener les organisations à modifier leur approche concernant l'expansion de leur clientèle. Par exemple, d'après Forrester Research, les spécialistes du marketing auraient intérêt à éviter d'utiliser ce type d'accessoires pour joindre les nouveaux clients et à s'en servir plutôt pour fidéliser leurs clients actuels. Forrester ajoute que ces spécialistes doivent utiliser de façon responsable l'information recueillie au moyen de capteurs dans le cadre des initiatives constantes qu'ils déploient pour prévoir l'humeur et les besoins des clients et y donner suite avant même que ceux-ci les aient exprimés⁸¹.



Source : Shutterstock

d) Accélération de « l'effondrement du contexte »

Les gens tentent généralement de compartimenter les différentes sphères de leur vie, que ce soit entre les cercles sociaux dont ils font partie ou simplement entre le travail et la vie personnelle. De façon générale, les réseaux sociaux et l'environnement en ligne limitent notre capacité à faire des distinctions nettes entre ces sphères. L'atténuation de ces distinctions, que les spécialistes des sciences sociales désignent par l'expression « effondrement du contexte »⁸², pourrait être exagérée et accélérée étant donné que les capteurs sont toujours activés et en interaction avec le corps de l'utilisateur et avec d'autres accessoires dans son environnement.

e) Possibilité d'accroître l'autonomie et la maîtrise

Certaines avancées prometteuses dans le paysage des accessoires intelligents à porter sur soi peuvent toutefois aider à accroître l'autonomie si on les fait valoir à l'étape de la conception. Par exemple, la possibilité d'éliminer grâce à l'accessoire certains éléments de son environnement pourrait accroître l'autonomie de l'utilisateur⁸³. En filtrant la publicité pour conserver uniquement les annonces que l'utilisateur souhaite voir et de la manière qu'il souhaite les recevoir, les accessoires intelligents pourraient créer un environnement plus confortable conçu et maîtrisé par l'utilisateur lui-même. Par exemple, on pourrait avoir recours à des programmes pour « effacer » en temps réel des objets se trouvant dans l'image d'une caméra afin d'enlever la publicité de l'information que communique l'accessoire⁸⁴. Des lunettes pourraient remplacer les annonces indésirables par des renseignements utiles et souhaitables pour l'utilisateur, par exemple un itinéraire⁸⁵.

f) Nouvelles méthodes d'authentification de l'identité, nouveaux renseignements personnels

Il est possible de configurer les accessoires intelligents à porter sur soi pour gérer les renseignements personnels d'une manière qui protège la vie privée et la sécurité. Par exemple, des chercheurs s'efforcent actuellement de trouver des façons de combiner les renseignements générés par les capteurs des téléphones intelligents de la génération actuelle pour identifier les utilisateurs et authentifier leur identité au moyen de leur téléphone, pendant que ces individus vaquent à leurs occupations quotidiennes, sans qu'ils aient à sortir cet accessoire de leur poche⁸⁶.

Ainsi, il suffirait qu'un utilisateur marche ou fasse son jogging ou bien qu'il monte ou descende un escalier en ayant un téléphone intelligent dans sa poche pour créer sa signature biométrique. Cette fonction permettrait certes d'améliorer la sécurité grâce à l'authentification de l'identité de l'utilisateur, mais elle créerait aussi par ailleurs de nouveaux risques d'atteinte à la vie privée.

3. Les lois canadiennes sur la protection de la vie privée et les accessoires intelligents

L'information en temps réel concernant l'humeur, la condition physique et l'état de santé d'une personne répond vraisemblablement à la définition de « renseignements personnels ». Nous savons que la combinaison d'éléments d'information hétéroclites tirés de plusieurs sources peut finir par broser un portrait permettant d'identifier une personne. Selon un jugement de la Cour fédérale⁸⁷, un renseignement concerne un individu identifiable lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles. Le Commissariat a par ailleurs fait valoir que l'information sur les abonnés peut révéler des renseignements très éloquentes sur une personne⁸⁸ et cette analyse fait ressortir certains points importants qui donnent matière à réflexion au moment de se pencher sur l'environnement des ordinateurs à porter sur soi.

a) Les accessoires intelligents et la Loi sur la protection des renseignements personnels

En vertu de la *Loi sur la protection des renseignements personnels*, une institution fédérale peut recueillir uniquement les renseignements personnels qui ont un lien direct avec ses programmes ou ses activités. Elle ne peut utiliser ces renseignements qu'aux fins auxquelles ils ont été recueillis ou pour des usages compatibles avec ces fins. Mis à part certaines exceptions limitées et précises, le consentement de l'individu est exigé pour toute autre utilisation des renseignements recueillis au moyen d'un accessoire porté sur soi.

Chaque fois qu'un ministère fédéral a l'intention d'utiliser ce type d'accessoires pour recueillir des renseignements personnels, il doit s'assurer que ses activités de programme sont conformes à la *Loi sur la protection des renseignements personnels*, effectuer une évaluation des facteurs relatifs à la vie privée (EFVP) et établir un protocole de protection de la vie privée pour la recherche, les audits et les évaluations conformément aux directives et aux politiques du Conseil du Trésor⁸⁹.

Rapport récent d'un comité parlementaire

En 2012, le Comité permanent de la sécurité publique et nationale a publié un rapport⁹⁰ sur l'efficacité de la surveillance électronique dans le domaine correctionnel et dans celui de l'immigration, sa rentabilité et son état de préparation à sa mise en œuvre. Des témoins lui ont fait part de leur opinion concernant la surveillance électronique dans ces contextes au moyen de dispositifs biométriques ainsi que de bracelets munis d'émetteurs de radiofréquences.

Dans sa réponse⁹¹ au rapport du Comité, le gouvernement a indiqué que le Service correctionnel du Canada entendait lancer en 2013 un deuxième projet pilote de surveillance électronique de portée plus étendue. La description du projet et les mesures d'atténuation des risques d'atteinte à la vie privée pour cette phase sont maintenant affichées en ligne⁹².

Dans sa réponse au rapport du Comité, le gouvernement a aussi expliqué que l'on avait recours à la surveillance électronique dans le cas de plusieurs personnes visées par un certificat de sécurité à long terme et que la Commission de l'immigration et du statut de réfugié (CISR) avait exigé la surveillance électronique pour quelques personnes en tant que condition de leur mise en liberté. Il a souligné en outre que l'Agence des services frontaliers du Canada (ASFC) entreprendrait une étude pour déterminer les risques et les avantages de la mise en œuvre d'un recours accru à la surveillance électronique dans le contexte de l'immigration en tirant des leçons de l'expérience des États-Unis et du Royaume-Uni dans le domaine. Les médias ont fait état de certains aspects de ce projet⁹³.

Réglementation des accessoires médicaux

Signalons que Santé Canada réglemente déjà de nombreux types d'accessoires médicaux, par exemple les tensiomètres, les glucomètres et les appareils auditifs, qui doivent actuellement être homologués avant d'être mis en marché au pays⁹⁴. Les nouveaux accessoires intelligents à porter sur soi qui utilisent des logiciels, des matériaux de pointe, la microélectronique et la biotechnologie⁹⁵ pourraient être régis par des aspects du régime actuel du *Règlement sur les instruments médicaux*, qui relève de la *Loi sur les aliments et drogues*. L'éventail d'accessoires à porter sur soi assujettis à ce règlement pourrait s'élargir à mesure que s'estompera la démarcation entre les accessoires médicaux de surveillance et ceux d'intervention. Il est également possible que Santé Canada ait besoin de recueillir des renseignements personnels, par exemple pour faire part des effets indésirables ou des incidents liés au matériel médical⁹⁶.

b) Les accessoires intelligents et la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

En lien avec le cadre de protection de la vie privée de la LPRPDE, les accessoires intelligents à porter sur soi peuvent poser des difficultés très similaires à celles que l'on rencontre déjà de façon générale dans les environnements mobile et en ligne. La caméra miniature dont sont équipés certains accessoires est au cœur du débat sur la question, en particulier en ce qui concerne les renseignements recueillis à des fins personnelles par les utilisateurs et portant sur d'autres individus. Dans ce contexte particulier, la *Loi* n'aura peut-être pas beaucoup de poids.

La LPRPDE précise expressément qu'elle ne s'applique pas « à un individu à l'égard des renseignements personnels qu'il recueille, utilise ou communique à des fins personnelles ou domestiques et à aucune autre fin⁹⁷ ». En vertu de cette exception, elle pourrait ne pas s'appliquer aux enregistrements audio et vidéo faits par des personnes portant sur d'autres personnes et affichés en ligne⁹⁸. Le gouvernement fédéral a récemment proposé des mesures pour régler un aspect de ce problème, soit la distribution d'une image intime d'une personne sans son consentement⁹⁹.

Il serait possible d'invoquer la LPRPDE dans les cas où des renseignements personnels provenant de l'accessoire de l'utilisateur sont transmis à des organisations qui recueillent, utilisent et communiquent des renseignements personnels dans le cadre d'activités commerciales. Par exemple, dans une lettre¹⁰⁰ récente concernant les Google Glass, les autorités de protection des données ont demandé à Google quels renseignements elle recueille au moyen des accessoires utilisés par les individus et à qui elle communique

cette information. Dans sa réponse, Google a insisté sur certains aspects de la maîtrise par l'utilisateur et sur son engagement à ne pas déployer pour le moment les applications de reconnaissance faciale sur les Google Glass¹⁰¹.

Il est possible que les employés d'organisations sous réglementation fédérale soient appelés à porter un casque virtuel dans l'exercice de leurs tâches quotidiennes. Les employeurs qui recueillent ou utilisent l'information ainsi générée par les employés pourraient contrevenir aux exigences de la LPRPDE concernant le consentement et la transparence si leur collecte de renseignements personnels auprès des individus ou des clients a une trop grande portée ou se fait à l'insu et sans le consentement des intéressés¹⁰². En outre, on pourrait configurer ces accessoires de manière à surveiller le niveau de stress et les émotions des employés et à transmettre cette information, comme le ferait le produit Empatica. En pareil cas, il y a tout lieu de croire que ces accessoires recueilleraient ainsi des renseignements personnels et seraient dès lors assujettis à plusieurs obligations prévues par la LPRPDE. Fondamentalement, il s'agit de déterminer si les renseignements sont recueillis uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

À l'issue d'une récente étude technique portant sur 43 applications axées sur la santé et la condition physique, l'organisation américaine Privacy Rights Clearinghouse a tiré certaines conclusions intéressantes, concernant la protection de la vie privée et les modèles d'affaires, qui sont pertinentes pour l'application de la LPRPDE. D'après l'étude, 72 % des applications examinées présentaient un risque d'atteinte à la vie privée modéré ou élevé et les applications payantes présentaient le risque le plus faible pour les utilisateurs. Cet état de choses est principalement attribuable au fait que l'entreprise ne s'en remet pas uniquement à la publicité en pareil cas pour faire de l'argent, ce qui atténue le risque de transmission des données à d'autres parties¹⁰³. Cette dynamique, qui sous-tend plusieurs enjeux liés à la protection de la vie privée dans les environnements mobile et en ligne, s'étendra aux défis à prévoir en lien avec les accessoires à porter sur soi. De nombreuses recommandations formulées par le Commissariat dans son document d'orientation à l'intention des concepteurs d'applications mobiles¹⁰⁴, sa fiche d'information sur les consoles de jeu¹⁰⁵ et sa position de principe sur la publicité comportementale en ligne¹⁰⁶ sont également applicables dans le contexte des accessoires intelligents.

4. Critères de conception choisis pour les accessoires intelligents

Certains principes relatifs à l'équité dans le traitement de l'information méritent une attention particulière pour protéger la vie privée dans l'environnement des accessoires intelligents à porter sur soi. Il sera important de maintenir à cet égard une approche neutre sur le plan technologique à mesure que les caractéristiques des accessoires actuels évolueront en parallèle avec l'Internet des objets.

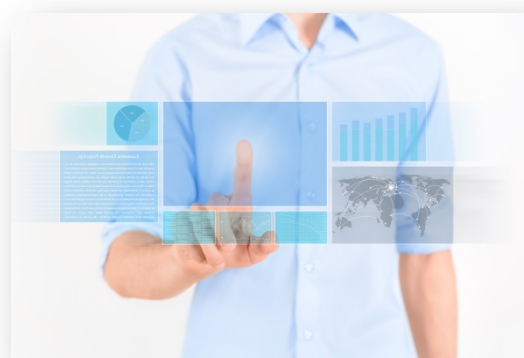
a) Maîtrise dynamique par l'utilisateur

Le consentement donné ou refusé une fois pour toutes et les définitions traditionnelles de « renseignements personnels » sont de plus en plus perçus comme étant désuets. Par exemple, l'Institut international des communications a mené en 2012 une recherche qualitative¹⁰⁷ visant à établir des modèles intellectuels sur la gestion des renseignements personnels. Son étude, qui mettait à contribution certains participants canadiens, a conclu que les politiques de gestion des renseignements personnels simplistes du type « tout ou rien » ne sont pas souples ni appropriées dans l'environnement en ligne qui évolue rapidement¹⁰⁸. Cette étude a également révélé que l'approche actuelle consistant à compartimenter l'information, selon qu'elle est visée ou non par les lois sur la protection des renseignements personnels dans la mesure où elle remplit le critère des renseignements personnels, était trop simpliste. D'après les auteurs de l'étude, il faudrait proposer à l'utilisateur un mécanisme de contrôle graduel ou progressif¹⁰⁹.

Selon le courant de pensée actuel concernant le concept de respect de la vie privée, il s'agirait d'une condition dynamique car l'environnement social et culturel de la personne évolue constamment¹¹⁰. On doit explorer une panoplie d'options créatives pour rendre le consentement plus explicite et mieux adapté aux différentes circonstances et à l'évolution des préférences ainsi que pour atténuer le fardeau décisionnel dans l'environnement des accessoires intelligents. Les options présentées ici sont le fruit d'extrapolations faites à partir des travaux de spécialistes de la vie privée comme Solove¹¹¹, Calo¹¹², Nissenbaum¹¹³, Tene¹¹⁴, Bailey¹¹⁵, Kerr¹¹⁶ et Sweeney¹¹⁷. Par exemple, il faudrait :

- élaborer des règles de protection de la vie privée calibrées de façon dynamique pour répondre aux besoins et aux attentes des individus en la matière;
- intégrer des caractéristiques de conception simples afin que les accessoires à porter sur soi puissent tenir compte des préférences de chacun au chapitre de la protection de la vie privée;
- exhorter les organisations à renforcer leurs politiques de protection de la vie privée au moyen de cartes de données dynamiques et interactives¹¹⁸ et d'outils infographiques pour montrer les relations dans l'environnement des accessoires intelligents.

Une autre caractéristique des accessoires intelligents à porter sur soi tient au fait qu'ils pourraient permettre de *réduire* de façon sélective ou de simplifier l'information que reçoit l'utilisateur en fonction de son choix. Des concepts comme celui-ci peuvent offrir une véritable possibilité de protéger la vie privée en appliquant à l'environnement des accessoires intelligents les principes du débat sur l'interdiction du suivi en ligne. Les programmes permettant d'effacer en temps réel des objets qui figurent à l'écran d'une caméra, cités en exemple précédemment, pourraient être utilisés pour retirer la publicité de l'information montrée aux individus au moyen de l'accessoire et limiter l'information autrement destinée aux tiers¹¹⁹.



Source : Shutterstock

Les chercheurs explorent actuellement d'autres modèles pour accroître la maîtrise des fonctions de reconnaissance faciale par l'utilisateur. Par exemple, d'après le Groupe de travail « Article 29 » sur la protection des données, une organisation devrait pouvoir recueillir les images numériques d'une personne pour déterminer si celle-ci l'a déjà autorisée à recueillir ses renseignements et, dans le cas contraire, être tenue de détruire l'image¹²⁰.

Les critères de conception pour l'interaction avec l'accessoire auront une incidence sur la vie privée de l'utilisateur. Par exemple, un accessoire à commande vocale crée un problème de protection de la vie privée similaire à celui qui se pose quand on a une conversation téléphonique en public. La capacité de la personne à modifier son comportement, peut-être à passer d'une conversation audio à des textos, constituerait une adaptation de la conception intéressante pour mieux protéger la vie privée.

b) Modèles de transparence en pleine évolution

Le contexte des accessoires intelligents à porter sur soi présente à la fois des possibilités et des défis sur le plan de la transparence. Par exemple, comme les accessoires faisant appel à la vision, à l'ouïe ou à d'autres sens peuvent être mieux intégrés à l'utilisateur, il pourrait être plus facile à certains égards d'obtenir son attention immédiate. On pourrait ainsi s'assurer plus aisément que le consentement et l'avis ont été prévus dès la conception dans le cas d'un accessoire intelligent que dans celui d'un téléphone intelligent¹²¹. La conception de certains accessoires ne nécessite aucun écran, si bien que de nouveaux modèles seront nécessaires pour obtenir le consentement des utilisateurs.

La protection de la vie privée de l'utilisateur est très différente de la protection de la vie privée des personnes qui l'entourent, laquelle constitue peut-être un problème plus épineux. Il est déjà difficile de savoir quand quelqu'un utilise un téléphone intelligent ou un autre accessoire pour faire un enregistrement audio ou vidéo. Toutefois, les accessoires intelligents réduisent encore plus la capacité des autres de savoir que l'on recueille des renseignements à leur sujet et de maîtriser cette collecte, car la technologie est intégrée de façon plus transparente à des objets qui passent inaperçus, par exemple la monture de lunettes ordinaires.

c) Accès aux renseignements et contestation de leur exactitude dans un processus décisionnel automatisé

La question de l'accès aux renseignements personnels est étroitement liée à celle de la transparence. Il est difficile de savoir comment les personnes pourront déterminer quelle information a été recueillie au moyen d'un accessoire à porter sur soi et laquelle a été utilisée et communiquée. Les utilisateurs devront avoir un moyen de contester les renseignements personnels recueillis et utilisés par les organisations pour prendre leurs décisions, car l'exactitude de cette information ne sera pas garantie.

Une étude récente portant sur certains accessoires à porter sur soi axés sur la condition physique a remis en question la fiabilité du suivi de la dépense énergétique associée à des activités de faible intensité comme se tenir debout ou faire le ménage¹²². Des inexactitudes dans la saisie de ce type de renseignements pourraient avoir des répercussions réelles pour les utilisateurs des accessoires. Par exemple, des erreurs de lecture à partir d'une nouvelle méthode de détection précoce de la maladie d'Alzheimer, faisant appel à une évaluation des mouvements du patient au moyen d'un accéléromètre¹²³, pourraient avoir une incidence sur le diagnostic posé et les soins prodigués au patient. Ces erreurs pourraient aussi créer des problèmes dans le milieu de travail si l'employeur s'en remettait à ce type d'accessoires pour surveiller des aspects de la productivité des employés. Une caractéristique importante inhérente à la conception des accessoires intelligents à porter sur soi consistera à s'assurer que les personnes ont la possibilité de vraiment contester l'exactitude des renseignements générés au moyen de ces accessoires ou l'analyse qui en est faite.

d) Vulnérabilités sur le plan de la sécurité

Sans systèmes de sécurité et d'authentification de l'identité appropriés, les accessoires intelligents sont vulnérables au piratage¹²⁴. Or, les accessoires piratés pourraient mettre en péril non seulement les renseignements personnels et la réputation de la personne, mais aussi sa santé. Par exemple, l'interception non autorisée et la substitution de personne dans le cas d'un accessoire assurant la régulation de l'insuline pourrait avoir des conséquences désastreuses pour la santé de l'individu¹²⁵. Comme l'a souligné un commentateur, « la sécurité des renseignements personnels d'un individu ne dépasse pas le maillon le plus faible de l'écosystème lui-même¹²⁶ ».

Conclusion

On convient généralement que les accessoires intelligents à porter sur soi sont appelés à occuper une place beaucoup plus grande dans notre vie quotidienne. Il ne fait aucun doute que six des douze technologies étudiées dans le rapport sur les technologies révolutionnaires publié en mai 2013 par le McKinsey Global Institute¹²⁷ font déjà partie intégrante de ce paysage : informatique mobile et capteurs à faible coût, systèmes logiciels intelligents, technologie de l'infonuagique, stockage de l'énergie avant-gardiste et matériaux de pointe.

Les accessoires intelligents représentent une avancée importante en soi, mais on ferait fausse route en les examinant en vase clos. Leur véritable importance dans le domaine de la protection de la vie privée sera

révélée lorsque leurs capacités seront combinées avec d'autres innovations façonnant notre monde aujourd'hui qui font aussi le suivi de nos activités, de nos mouvements, de nos comportements et de nos préférences. Cette tendance pourrait bien se répercuter sur notre vie privée, mais également sur notre milieu de travail. Par exemple, le « badge de pointage » Business Microscope¹²⁸ de Hitachi, auquel sont intégrés des capteurs infrarouges, un accéléromètre et un capteur de microphone, a pour objet de saisir les modes d'interaction dans le milieu de travail mais également la *qualité* de la collaboration des employés. La surveillance de nos émotions, de notre état de santé et de la qualité de nos interactions humaines touche au cœur même de notre moi le plus profond.

Autrefois de l'ordre de la science-fiction, l'intégration de caméras et de capteurs *dans* le corps semble également vraisemblable, en particulier dans les cas où il faut compléter ou augmenter des fonctions humaines. Par exemple, des chercheurs de l'Université de Princeton ont utilisé des imprimantes 3D pour combiner l'électronique avec un tissu afin de créer une oreille fonctionnelle qui peut « entendre » les radiofréquences beaucoup mieux que l'oreille humaine¹²⁹. Dans le domaine de l'électronique épidermique¹³⁰, des chercheurs travaillent au développement d'accessoires de surveillance de l'état de santé fixés sur la peau de l'individu, comme des tatouages temporaires, pour poser des diagnostics et assurer de façon peu invasive un suivi d'anomalies telles que l'arythmie cardiaque ou les troubles du sommeil. La US Navy explore les biomonteurs de prochaine génération, sous forme de tatouages temporaires, pour surveiller les indicateurs de stress chez les militaires, par exemple le rythme cardiaque, la température ou la réaction bioélectrique dans diverses situations d'entraînement¹³¹.

Ce type d'exemple montre à quel point les technologies à porter sur soi pourraient devenir intégrées dans notre corps et notre esprit. Or, elles modifient en profondeur les façons dont les autres peuvent nous surveiller et nous évaluer. Les technologies d'accessoires intelligents à porter sur soi pourraient améliorer la vie de nombreuses personnes, mais le risque de bouleversement social et de surveillance n'est pas négligeable.

Défis au chapitre de la protection de la vie privée découlant de la technologie à porter sur soi

Compte tenu de la possibilité omniprésente mais quasi imperceptible de surveillance, le besoin de transparence est plus grand que jamais auparavant. Les individus posent des questions et remettent en question la surveillance dont ils connaissent ou soupçonnent l'existence. Cependant, lorsque les capteurs à porter sur soi sont minuscules, silencieux et intégrés dans des produits d'usage courants, comme les vêtements¹³², il n'y a aucune raison évidente de poser des questions ou de faire des remises en question.

Si la transparence en ce qui concerne le suivi assuré au moyen d'accessoires intelligents à porter sur soi est importante pour nos relations avec le secteur privé, elle l'est tout autant pour nos relations avec le gouvernement. Les révélations sur le front de la sécurité nationale¹³³ montrent que les renseignements personnels recueillis par le secteur privé jouent un rôle crucial dans l'écosystème de surveillance. Il ne faut pas s'étonner que la quantité de renseignements obtenus grâce à ce type d'accessoires puisse attirer les organismes de renseignement et les gouvernements.

Les accessoires intelligents à porter sur soi marquent le début d'une toute nouvelle génération de risques d'atteinte à la vie privée, mais ils offrent par ailleurs une formidable possibilité de renforcer la protection de la vie privée et l'autonomie des utilisateurs. Des façons créatives de mettre davantage à contribution nos sens pourraient offrir aux utilisateurs de nouveaux moyens de donner de la rétroaction et de faire des choix concernant leurs préférences en matière de protection de la vie privée; il serait bénéfique d'alléger le fardeau décisionnel caractéristique des politiques de confidentialité actuelles fondées sur des textes et des pratiques de consentement statiques du tout ou rien.

Les défis au chapitre de la protection de la vie privée émanant à la fois des secteurs public et privé s'intensifieront forcément au cours des années à venir. Ces technologies peuvent toutes être bénéfiques pour la société, mais les risques d'atteinte à la vie privée demeurent sérieux et difficiles à prédire, même à court terme. Toutes les études de marché prévoient une plus grande adoption par les consommateurs. Une transparence accrue, des solutions technologiques novatrices et une mobilisation dynamique du public sur ces enjeux s'imposent afin que la protection de la vie privée suive le rythme de la révolution des accessoires intelligents et qu'elle en fasse partie intégrante.

Notes

¹ La portée du présent rapport de recherche se limite aux accessoires intelligents portés à l'extérieur du corps. Elle exclut les implants, car ils posent une foule de défis supplémentaires sur le plan de la vie privée. Certains mots-clés : accessoire intelligent, assistant numérique intelligent, Aviation Warrior de Raytheon, BodyMedia FIT, bracelet MYO, bracelet vital, Digits, effondrement du contexte, électronique épidermique, Empatica, FitBit, FuelBand, Golden-i de Kopin, Google Glass, GoPro, Leap Motion, HC1, HealthPatch de Vital Connect, iOptik d'Innovega, iWatch, Jawbone UP, LifeBoard, marketing d'anticipation, médicament numérique, Memoto, montre espion DVR Tieex, Oculus Rift, OrCam, Pebble, physiolytique, Proteus Digital Health, Recon Jet, Shine, Steve Mann, Thalmic Labs, technologie d'assistance, télescope implantable et Vuzix Smart Glasses M100.

² Commissariat à la protection de la vie privée du Canada. [Les véhicules aériens sans pilote au Canada : L'utilisation croissante de véhicules aériens sans pilote dans l'espace aérien canadien suscitera-t-elle de nouvelles inquiétudes pour la protection de la vie privée?](#), mars 2013.

³ Donald Melanson et Michael Gorman. « [Our augmented selves: The promise of wearable computing](#) », *Engadget*, 12 décembre 2012. Consulté le 8 juillet 2013.

⁴ Marcelo Ballvé. « [Wearable Computing: A New Mobile Market Takes Shape](#) », *BI Intelligence*, 2013.

⁵ 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.

⁶ Steve Mann. « Smart Clothing: The Shift to Wearable Computing », dans *Communications of the ACM*, 39 (8), 1996a, p. 23-24. Voir Steve Mann. « [Wearable Computing](#) », dans Mads Soegaard et Rikke Friis Dam (éditeurs). *The Encyclopedia of Human-Computer Interaction*, 2^e éd., Aarhus, Danemark, The Interaction Design Foundation, 2013. Consulté le 14 juin 2013.

⁷ « [Wearable Technology Market — Global Scenario, Trends, Industry Analysis, Size, Share And Forecast, 2012-2018](#) », *Market Research Reports Biz*, janvier 2013. Consulté le 13 juin 2013.

⁸ Emily Waltz. « [How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives?](#) », *IEEE Spectrum*, 30 août 2012. Cité dans Steve Mann. « [Steve Mann: My "Augmediated" Life](#) », *IEEE Spectrum*, 1^{er} mars 2013. Consulté le 14 juin 2013.

⁹ Voir Vital Connect. [HealthPatch](#). Consulté le 6 janvier 2014.

¹⁰ Tom Ryan, « [Will tech wearables go mainstream?](#) », *RetailWire*, 14 janvier 2014. Consulté le 22 avril 2014.

¹¹ Par exemple, voir [Misfit Wearables](#), cité par Jennifer Darmour dans « [3 Ways To Make Wearable Tech Actually Wearable](#) », *Fast Company*, 15 mars 2013. Consulté le 12 juin 2013.

¹² « [Smart Glasses and Other Wearable Devices to be worth over \\$1.5bn by 2014, finds Juniper](#) », communiqué de Juniper Research, 31 octobre 2012. Consulté le 17 juillet 2013.

¹³ [World Market for Wearable Technology – A Quantitative Market Assessment – 2012](#), IMS Research, août 2012, analysé dans [Wearable Computing Devices, Like Apple's iWatch, Will Exceed 485 Million Annual Shipments by 2018](#), ABI Research, 21 février 2013. Consulté le 10 juillet 2013.

¹⁴ [Wearable Computing Devices, Like Apple's iWatch, Will Exceed 485 Million Annual Shipments by 2018](#), ABI Research, 21 février 2013. Consulté le 10 juillet 2013.

-
- ¹⁵ Marcelo Ballvé. [Wearable Computing: A New Mobile Market Takes Shape](#), *BI Intelligence*, avril 2013. Consulté le 10 juillet 2013.
- ¹⁶ Donald Melanson et Michael Gorman. « [Our augmented selves: The promise of wearable computing](#) », *Engadget*, 12 décembre 2012. Consulté le 8 juillet 2013.
- ¹⁷ Christina Warren. « [Why the iPhone Was Truly a Disruptive Product](#) », *Mashable*, 29 juin 2012. Consulté le 16 juillet 2013.
- ¹⁸ Charles Arthur. « [Apple applies for iWatch trademark](#) », *The Guardian*, 1^{er} juillet 2013. Consulté le 16 juillet 2013.
- ¹⁹ « [Apple hires Yves Saint Laurent CEO, stoking rumours of wearable device](#) », *CBC News*, 3 juillet 2013. Consulté le 16 juillet 2013.
- ²⁰ Steve Mann. « [Wearable Computing](#) », dans Mads Soegaard et Rikke Friis Dam (éditeurs). *The Encyclopedia of Human-Computer Interaction*, 2^e éd., Aarhus, Danemark, The Interaction Design Foundation, 2013.
- ²¹ Bien que les aides visuelles implantables offertes sur le marché, par exemple le « télescope implantable » pour les personnes atteintes de dégénérescence maculaire liée à l'âge, ne relèvent pas de la portée du présent document, il est important de reconnaître la portée beaucoup plus vaste d'autres formes de technologies d'assistance pour les déficiences visuelles. « [Implantable Telescope Lens to Treat Macular Degeneration Available at Johns Hopkins](#) », communiqué de presse, *Johns Hopkins Medicine*, 21 mars 2013. Consulté le 12 juin 2013.
- ²² Sunir Garg. « [Retinal Prostheses Offer Hope to Blind Patients](#) », *Review of Ophthalmology*, 15 mars 2013. Consulté le 14 juin 2013.
- ²³ [Site Web du capteur Orcam](#).
- ²⁴ John Markoff. « [Device From Israeli Start-Up Gives the Visually Impaired a Way to Read](#) », *The New York Times*, 3 juin 2013. Consulté le 13 juin 2013.
- ²⁵ « [iOptik augmented reality contact lens prototype to be unveiled at CES](#) », *Gizmag*, 6 janvier 2014. Consulté le 7 janvier 2014.
- ²⁶ Steve Mann travaille depuis 35 ans au développement de ce type de lunettes intelligentes. Steve Mann. « [Steve Mann: My "Augmediated" Life](#) », *IEEE Spectrum*, 1^{er} mars 2013. Consulté le 14 juin 2013.
- ²⁷ Steve Mann, Raymond Chun Hing Lo, Kalin Ovtcharov, Shixiang Gu, David Dai, Calvin Ngan et Tao Ai. [Realtime HDR \(High Dynamic Range\) Video for EyeTap Wearable Computers, FPGA-based Seeing Aids, and Glasses \(EyeTaps\)](#), 25^e conférence canadienne de génie électrique et informatique de l'IEEE, 2012. Consulté le 24 juin 2013.
- ²⁸ Michael W. Boyce et P.A. Hancock. « [The Interpenetration of Mind and Machine](#) », *Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting*, 56: 178, 2012. Consulté le 11 juin 2013.
- ²⁹ [LifeBoard for Gi-OS](#). Consulté le 24 juin 2013.
- ³⁰ « [IBM's Watson Now A Customer Service Agent, Coming To Smartphones Soon](#) », *Forbes*, 21 mai 2013. Consulté le 15 juillet 2013.
- ³¹ [Narrative Clip](#).
- ³² Valencell. [PerformTek® Precision Biometrics: Engaging the Burgeoning Mobile Health and Fitness Market](#), livre blanc, janvier 2013. Consulté le 17 juin 2013.
- ³³ [Nike+ FuelBand](#).
- ³⁴ [Fitbit](#) ne fait pas encore de livraison au Canada.
- ³⁵ [BodyMedia FIT](#) — le site Web indique que ce produit peut être livré au Canada.
- ³⁶ [Jawbone UP](#).
- ³⁷ [PerformTek® Sensor Technology](#) et Bryon Moyer, « [You Put That Where?](#) », blogue de l'*Electrical Engineering Journal*, 5 février 2013. Consulté le 17 juin 2013.
- ³⁸ [Pebble](#).
- ³⁹ [Galaxy Gear](#).

- ⁴⁰ « [GoPro's video revolution](#) », *60 Minutes*, 10 novembre 2013.
- ⁴¹ [Google Glass](#).
- ⁴² « [Les autorités chargées de la protection des données exhortent Google à donner suite aux préoccupations concernant Google Glass](#) », communiqué de presse, Commissariat à la protection de la vie privée du Canada, 18 juin 2013. Consulté le 24 juin 2013.
- ⁴³ « [Vuzix M100 Production Model Shipping to Developers and Available for General Pre-Order](#) », communiqué de presse. Consulté le 30 décembre 2013.
- ⁴⁴ [Recon Instruments](#). Consulté le 30 décembre 2013.
- ⁴⁵ [Oculus Rift](#).
- ⁴⁶ Paul Marks. « [Muscle-zapper forces gamers' own hands against them](#) », *New Scientist*, n° 2902, 31 janvier 2013. Consulté le 11 juin 2013.
- ⁴⁷ P. Lopes et P. Baudisch. « [Muscle-Propelled Force Feedback: Bringing Force Feedback to Mobile Devices](#) », *CHI 2013: Changing Perspectives*, Paris, France. CHI 13, du 27 avril au 2 mai 2013. Consulté le 11 juin 2013.
- ⁴⁸ Sarah Mitroff. « [Your Next Computer Will Live on Your Arm](#) », *WIRED*, 25 février 2013. Consulté le 8 juillet 2013.
- ⁴⁹ Voir « [The Hottest Global Startups Of 2013](#) », *Forbes*, 16 décembre 2013 et [Thalnic Labs](#). Consulté le 6 janvier 2014.
- ⁵⁰ [Digits](#) de Microsoft Research. Consulté le 6 janvier 2014.
- ⁵¹ Will Knight. « [What Comes After the Touch Screen](#) », *MIT Technology Review*, 11 octobre 2012. Consulté le 7 juillet 2013.
- ⁵² Voir le site Web de [Leap Motion](#).
- ⁵³ « [Health apps, virtual visits and remote monitoring – Canadians looking to manage their health one click at a time: PwC report](#) », communiqué de presse de PwC, 4 juin 2013, Consulté le 19 juillet 2013.
- ⁵⁴ [2013 Canadian Telehealth Report](#) (basé sur l'enquête canadienne sur la télésanté de 2012), mis à jour en juin 2013. Consulté le 30 décembre 2013.
- ⁵⁵ « [Introducing our smart contact lens project](#) », *Google Official Blog*, 16 janvier 2014. Consulté le 24 janvier 2014.
- ⁵⁶ [Proteus Digital Health](#).
- ⁵⁷ Erin Kim. « [Digital pill' with chip inside gets FDA green light](#) », *CNNMoney*, 3 août 2012. Consulté le 17 juillet 2013.
- ⁵⁸ [Digital Health Feedback System](#) de Proteus.
- ⁵⁹ Voir le sommaire de [How Wireless Therapy Will Change Health Care Delivery](#) dans la page des publications de Proteus.
- ⁶⁰ [Aviation Warrior](#) de Raytheon. Donna Tam. « [Pilot of the Future: U.S. Army gets wearable tech for the battlefield](#) », *CNET News*, 8 juillet 2012. Consulté le 24 juin 2013.
- ⁶¹ [Site Web de Golden-i](#) de la société Kopin.
- ⁶² [Specification Sheet](#), fiche technique du casque virtuel HC1 de Motorola. Consulté le 24 juin 2013.
- ⁶³ Voir aussi [Hands-Free Mobile Computing: Increase Productivity with Motorola Solutions Wearable Portfolio](#) de Motorola. Consulté le 27 juin 2013.
- ⁶⁴ [BCCLA Says Police "Body-Worn" Video Cameras Not About Police Accountability](#), British Columbia Civil Liberties Association, 30 juin 2009. Consulté le 9 juillet 2013.
- ⁶⁵ « [Edmonton police to test body cameras](#) », *CBC News Edmonton*, 9 octobre 2012. Consulté le 9 juillet 2013.
- ⁶⁶ [The Human Cloud: Wearable Technology from Novelty to Productivity](#), rapport commandé par Rackspace en association avec le Centre for Creative and Social Technology (CAST) à Goldsmiths, Université de Londres, 5 juin 2013. Consulté le 12 juin 2013.
- ⁶⁷ Sarah Rotman Epps. « [Smart Body, Smart World: The Next Phase of Personal Computing](#) », *All Things D*, 29 octobre 2012, Consulté le 12 juin 2013.

- ⁶⁸ 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](#), document d'orientation, octobre 2012.
- ⁶⁹ Donald Melanson et Michael Gorman. « [Our augmented selves: The promise of wearable computing](#) », *Engadget*, 12 décembre 2012. Consulté le 8 juillet 2013.
- ⁷⁰ Voir la [description](#) de la caméra intégrée dans une casquette de baseball.
- ⁷¹ Voir la [description](#) de la caméra cachée dans un lecteur MP3.
- ⁷² Voir la [description](#) de la caméra cachée dans un bouton.
- ⁷³ Dans une cause récente jugée au Royaume-Uni, une caméra cachée dans une montre-bracelet a été utilisée pour enregistrer les examens médicaux de patientes. D'après les reportages médiatiques, le médecin a utilisé une montre espion DVR HD étanche Tieex de 4 GB, qui ressemble à n'importe quelle autre montre de sport pour homme. « [12 years for GP who filmed sex assaults on female patients with James Bond-style watch](#) », *London Evening Standard*, 23 mai 2012. Consulté le 10 juin 2013.
- ⁷⁴ [Heart & Stroke eTools](#), analysé dans « [How insurers are turning to fitness apps to decide your health coverage](#) », *The Globe and Mail*, 19 décembre 2013.
- ⁷⁵ [Sprout](#). Consulté le 3 janvier 2014.
- ⁷⁶ [Empatica](#). Consulté le 3 janvier 2014.
- ⁷⁷ Amir Muaremi, Bert Arnrich et Gerhard Tröster. « [Towards Measuring Stress with Smartphones and Wearable Devices During Workday and Sleep](#) », *BioNanoScience*, 8 mai 2013, p. 182. Consulté le 17 juin 2013.
- ⁷⁸ H. James Wilson. « [Wearables in the Workplace](#) », *Harvard Business Review*, septembre 2013.
- ⁷⁹ Paul M. Schwartz. [Data Protection Law and the Ethical Use of Analytics](#), The Centre for Information Policy Leadership Hunton & Williams LLP 2010, cité dans Erin Courtland. [L'ère de l'analyse prédictive : des tendances aux prédictions](#), SGDDI n° 350219, août 2012.
- ⁸⁰ Daniel J. Solove, [Privacy Self-Management and the Consent Dilemma](#), 4 novembre 2012. *Harvard Law Review* 1880 (2013), vol. 126; GWU Legal Studies Research Paper No. 2012-141; GWU Law School Public Law Research Paper No. 2012-141. Consulté le 19 juin 2013.
- ⁸¹ Sarah Rotman Epps. « [Smart Marketing In A Sensor-Laden World](#) », *Forbes*, 18 avril 2013. Consulté le 12 juin 2013.
- ⁸² Voir, par exemple, Alice Marwick et danah boyd. « [I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience](#) », *New Media & Society*, vol. 13, n° 1, février 2011, p. 114-133 et Carolyn Marvin. « [Your smart phones are hot pockets to us: Context collapse in a mobilized age](#) », *Mobile Media & Communication*, 1: 153, 2013. Consulté le 22 août 2013.
- ⁸³ En outre, tous les contrôles imposés en vertu de la gestion des droits numériques et des accords de licence d'utilisateur pour les accessoires intelligents à porter sur soi pourraient diminuer la maîtrise par le particulier et son autonomie. Jane Bailey et Ian Kerr. « [Seizing Control?: The Experience Capture Experiments of Ringley & Mann](#) », *Ethics & Information Technology*, vol. 9, n° 2, 2007, p. 129-139.
- ⁸⁴ Paul Miller. « [Project Glass and the epic history of wearable computers: How we've tried to become more than human](#) », *The Verge*, 26 juin 2012. Consulté le 24 juin 2013.
- ⁸⁵ Steve Mann. « [Wearable Computing](#) », dans Mads Soegaard et Rikke Friis Dam (éditeurs). *The Encyclopedia of Human-Computer Interaction*, 2^e éd., Aarhus, Danemark, The Interaction Design Foundation, 2013.
- ⁸⁶ Jennifer R. Kwapisz, Gary M. Weiss et Samuel A. Moore. « [Cell Phone-Based Biometric Identification](#) », *Biometrics: Theory Applications and Systems (BTAS)*, 2010 Fourth IEEE International Conference, du 27 au 29 septembre 2010.
- ⁸⁷ [Gordon c. Canada](#) (Santé), 2008 CF 258 (CanLII). Consulté le 22 juillet 2013.
- ⁸⁸ 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. Consulté le 24 juin 2013.

⁸⁹ Secrétariat du Conseil du Trésor. [Directive sur l'évaluation des facteurs relatifs à la vie privée](#) et [Politique sur la protection de la vie privée](#).

⁹⁰ [Une étude sur la surveillance électronique dans les domaines correctionnel et de l'immigration](#), sixième rapport du Comité permanent de la sécurité publique et nationale, septembre 2012. Consulté le 23 août 2013.

⁹¹ [Réponse du gouvernement aux recommandations formulées dans le sixième rapport du Comité permanent de la sécurité publique et nationale intitulé Une étude sur la surveillance électronique dans les domaines correctionnel et de l'immigration](#), Vic Toews, ministre de la Sécurité publique, 28 janvier 2013. Consulté le 23 août 2013.

⁹² Service correctionnel du Canada. [Projet pilote de surveillance électronique II \(SE-PPII\)](#). Consulté le 2 janvier 2014.

⁹³ « [Canada looks to put GPS bracelets on more migrants](#) », *Globe and Mail* en ligne, 27 juin 2013. Consulté le 3 janvier 2014.

⁹⁴ Santé Canada, [Achat de matériel médical sur Internet : Votre santé et vous](#), fiche d'information. Consulté le 24 juin 2013.

⁹⁵ Industrie Canada. [Profil de l'industrie des appareils médicaux 2013](#). Consulté le 2 janvier 2014.

⁹⁶ Santé Canada. [Déclaration des effets indésirables ou des incidents liés aux matériels médicaux](#). Consulté le 19 juillet 2013.

⁹⁷ Voir l'[alinéa 4\(2\)b](#) de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

⁹⁸ Teresa Scassa. « [Google Glass and the Privacy Gap](#) », blogue, 19 juin 2013. Consulté le 19 juin 2013.

⁹⁹ [Projet de loi C-13, Loi sur la protection des Canadiens contre la cybercriminalité](#). Consulté le 2 janvier 2014.

¹⁰⁰ Commissariat à la protection de la vie privée du Canada et 36 de ses homologues provinciaux et internationaux. « [Les autorités chargées de la protection des données exhortent Google à donner suite aux préoccupations concernant Google Glass](#) », communiqué de presse concernant la lettre à Google, 18 juin 2013.

¹⁰¹ Peter Fleischer. [Réponse de Google aux autorités chargées de la protection des données au sujet de Google Glass](#), conseiller en matière de protection de la vie privée à l'échelle mondiale, Google, 27 juin 2013.

¹⁰² Commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, Commission d'accès à l'information du Québec et Commissariat à la protection de la vie privée du Canada. [Vous êtes photographiés : La technologie de l'imagerie à l'échelle de la rue, Internet et vous](#), fiche d'information.

¹⁰³ « [Privacy Rights Clearinghouse Releases Study: Mobile Health and Fitness Apps: What Are the Privacy Risks?](#) », communiqué de presse affiché le 15 juillet 2013. Consulté le 17 juillet 2013.

¹⁰⁴ 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](#), document d'orientation, octobre 2012.

¹⁰⁵ Commissariat à la protection de la vie privée du Canada. [Consoles de jeu et renseignements personnels : la vie privée en jeu](#), document d'orientation, novembre 2012.

¹⁰⁶ Commissariat à la protection de la vie privée du Canada. [Position de principe sur la publicité comportementale en ligne](#), juin 2012.

¹⁰⁷ Institut international des communications. [Personal Data Management: The User's Perspective](#), recherche commandée à IPSOS UU par l'Institut, réalisée entre mars et août 2012 et financée par la société Microsoft Corporation, 22 novembre 2012, p. 9. Consulté le 17 juin 2013.

¹⁰⁸ Institut international des communications, [Personal Data Management: The User's Perspective](#), 22 novembre 2012, p. 9. Consulté le 17 juin 2013.

¹⁰⁹ Institut international des communications, [Personal Data Management: The User's Perspective](#), 22 novembre 2012, p. 37. Consulté le 17 juin 2013.

¹¹⁰ Julie E. Cohen. « [What Privacy Is For](#) », *Harvard Law Review*, vol. 126, 2013, p. 1906.

- ¹¹¹ Daniel J. Solove, [Privacy Self-Management and the Consent Dilemma](#), 4 novembre 2012. *Harvard Law Review* 1880 (2013), vol. 126; GWU Legal Studies Research Paper No. 2012-141; GWU Law School Public Law Research Paper No. 2012-141. Consulté le 19 juin 2013.
- ¹¹² M. Ryan Calo. « [Against Notice Skepticism in Privacy \(and Elsewhere\)](#) », *Notre Dame Law Review*, 1027, vol. 87, 2012, p. 1033.
- ¹¹³ Helen Nissenbaum. *Privacy In Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.
- ¹¹⁴ Omer Tene. « [Privacy: The New Generations](#) », *International Data Protection Law*, 2010.
- ¹¹⁵ Jane Bailey et Ian Kerr. « [Seizing Control?: The Experience Capture Experiments of Ringley & Mann](#) », *Ethics & Information Technology*, vol. 9, n° 2, 2007, p. 129-139.
- ¹¹⁶ Jane Bailey et Ian Kerr. « [Seizing Control?: The Experience Capture Experiments of Ringley & Mann](#) », *Ethics & Information Technology*, vol. 9, no 2, 2007, p. 129-139.
- ¹¹⁷ Projet [DataMap](#) en ligne.
- ¹¹⁸ Voir, par exemple, le portail en ligne [theDataMap](#).
- ¹¹⁹ Paul Miller. « [Project Glass and the epic history of wearable computers: How we've tried to become more than human](#) », *The Verge*, 26 juin 2012. Consulté le 24 juin 2013.
- ¹²⁰ Voir la recommandation n° 5 du Groupe de travail « Article 29 » sur la protection des données. [Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles](#), 00727/12/FR WP 192. Consulté le 16 juillet 2013.
- ¹²¹ M. Ryan Calo. « [Against Notice Skepticism in Privacy \(and Elsewhere\)](#) », *Notre Dame Law Review*, 1027, vol. 87, 2012, p. 1033.
- ¹²² K.L. Dannecker, N.A. Sazonova, E.L. Melanson, E.S. Sazonov et R.C. Browning. « [A Comparison of Energy Expenditure Estimation of Several Physical Activity Monitors](#) », *Medicine & Science in Sports & Exercise*, 10 mai 2013, analysé dans Gretchen Reynolds. « [How Accurate Are Fitness Trackers?](#) », *The New York Times*, 12 juin 2013. Consulté le 12 juin 2013.
- ¹²³ Thomas Kirste, André Hoffmeyer, Philipp Koldrack, Alexandra Bauer, Susanne Schubert, Stefan Schröder et Stefan Teipel. « [Detecting the Effect of Alzheimer's Disease on Everyday Motion Behavior](#) », *Journal of Alzheimer's Disease*, vol. 38, n° 1, 2014.
- ¹²⁴ La Federal Drug Administration des États-Unis a publié en 2005 un document d'orientation sur la cybersécurité en lien avec les appareils médicaux en réseau utilisant des logiciels commerciaux. Voir Federal Drug Administration des États-Unis. [Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf \(OTS\) Software](#), 14 janvier 2005. Consulté le 19 juillet 2013.
- ¹²⁵ Li Chunxiao, Anand Raghunathan et Niraj K. Jha. « [Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System](#) », 2011 IEEE Conference on e-Health Networking, Applications and Services.
- ¹²⁶ Michael Carney. « [You are your data: The scary future of the quantified self movement](#) », *PandoDaily*, 20 mai 2013. Consulté le 10 juin 2013.
- ¹²⁷ 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. Consulté le 16 juillet 2013.
- ¹²⁸ [Business Microscope](#), Hitachi. Consulté le 13 février 2014. Voir aussi « [Wearable Gadgets Transform How Companies Do Business](#) », *The Wall Street Journal*, 20 octobre 2013.
- ¹²⁹ John Sullivan. « [Printable 'bionic' ear melds electronics and biology](#) », *News at Princeton*, 8 mai 2013, Consulté le 13 juin 2013.
- ¹³⁰ Woon-Hong Yeo, Yun-Soung Kim, Jongwoo Lee, Abid Ameen, Luke Shi, Ming Li, Shuodao Wang, Rui Ma, Sung Hun Jin, Zhan Kang, Yonggang Huang et John A. Rogers. « [Multifunctional Epidermal Electronics Printed Directly Onto the Skin](#) », *Advanced Materials*, 25, 2013, p. 2773–2778.

¹³¹ Nick Stockton. « [Pentagon's Mad Scientists Want a Tattoo That Tracks Troops' Vitals](#) », *WIRED*, 27 mars 2013.

¹³² Voir, par exemple, [Cityzen Sciences](#). Des tissus intelligents auxquels sont intégrés des microcapteurs leur permettant de surveiller la température, le rythme cardiaque, la vitesse et l'accélération ainsi que la géolocalisation.

¹³³ Commissariat à la protection de la vie privée du Canada. [Rapport spécial au Parlement – Mesures de vérification et de contrôle : Renforcer la protection de la vie privée et la supervision des activités du secteur canadien du renseignement à l'ère de la cybersurveillance](#), 28 janvier 2014.