Sécurité technologique Canada

Voitures connectées et véhicules sans conducteur: Problèmes de sécurité et de confidentialité

Une note sur la langue

Dans cette trousse, nous utiliserons parfois le mot femme et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif de la violence facilitée par la technologie sur les femmes et les filles. Nous reconnaissons que la VFGFT a également un impact sur les personnes trans, non binaires et bispirituelles. Nous espérons que toutes les personnes touchées par la VFGFT trouveront ces documents utiles.

Si les véhicules sans conducteur n'ont pas encore fait leur apparition sur les routes canadiennes, de plus en plus de voitures sont livrées déjà «connectées», ce qui permet notamment aux parents de surveiller les habitudes de conduite des jeunes et aux employeurs celles de leur personnel. En outre, de petits gadgets peuvent être fixés à une voiture pour permettre une surveillance à distance et, dans certains cas, un contrôle à distance.

Pour plus d'informations et de conseils généraux sur l'Internet des objets et les appareils intelligents ou connectés, consultez notre document de présentation.

Voitures sans conducteur

Certains fabricants automobiles, services de covoiturage et entreprises de livraison de marchandises font l'apologie des voitures sans conducteur. Ces voitures combinent une grande variété de capteurs et de systèmes qui permettent de diriger un véhicule dans le trafic urbain et sur de longs tronçons d'autoroute. Dans presque tous les cas, les voitures nécessitent la présence d'une personne sur le siège du conducteur pour prendre le relais en cas de problème. De nombreuses voitures en circulation aujourd'hui sont déjà dotées de fonctions de base d'assistance par ordinateur qui aide le conducteur à effectuer une tâche, par exemple à actionner automatiquement les freins.

Voitures connectées

Aujourd'hui, plusieurs services sur le marché sont conçus pour surveiller et contrôler les décisions de conduite du personnel des entreprises et des jeunes au volant. Ces services permettent de surveiller les habitudes de conduite et de repérer la localisation, puis de fournir un rapport électronique ou des mises à jour en temps réel. Les options permettant de contrôler une voiture à distance ou en fixant des limites prédéfinies comprennent les limites de vitesse et du volume audio, ou le blocage des SMS ou des alertes d'applis sur le téléphone de l'adolescent·e. Ces options peuvent également être utilisées par un auteur de violence pour contrôler le véhicule d'une femme.

Un nombre limité de véhicules sont équipés de ces services, tandis que de nombreux autres fonctionnent en branchant un petit appareil sur la prise de diagnostic de bord (OBD). Le système OBD est une partie de la voiture qui passe souvent inaperçue. Il s'agit d'un ordinateur qui peut suivre les émissions, le kilométrage, la vitesse et d'autres données. Certaines applis permettent également de recourir directement à l'appareil mobile du conducteur pour recueillir et envoyer des informations et bloquer les messages entrants.

Risques pour la sécurité et la confidentialité

Le principal risque de sécurité des voitures connectées concerne la possibilité de les contrôler à distance. Le plus grave serait de provoquer un accident en prenant le contrôle de la direction, du freinage ou de l'accélération. Parmi les autres risques, citons la prise de contrôle du volume du système de son, de l'éclairage, du klaxon, des essuie-glaces et d'autres fonctions susceptibles de distraire ou de perturber, risquant ainsi de provoquer des accidents. Des pirates informatiques ont démontré qu'il était possible de prendre le contrôle de toutes ces fonctions dans les voitures actuellement en circulation.

Les risques pour la confidentialité découlent de la surveillance et du partage des informations sur les habitudes de conduite et la localisation. Les fonctions intégrées, celles nécessitant une connexion physique, ainsi que les applis pour appareil mobile, peuvent partager des informations à distance, offrant ainsi une possibilité de surveillance et de contrôle. Les fabricants stockent également les informations recueillies sur les véhicules, ce qui peut poser un risque d'accès non autorisé.

Avantages des appareils connectés et intelligents

Si les risques liés aux voitures connectées sont très inquiétants, il existe des moyens d'utiliser cette technologie de manière stratégique pour accroître la sécurité. Une femme qui souhaite localiser un véhicule ou ses passagers, se rassurer ou diriger les services d'urgence en cas de vol ou d'enlèvement peut partager sa position. Une femme peut également

choisir de partager sa position avec des proches ou des membres de sa famille. Enfin, les déplacements ou les habitudes de conduite d'un auteur de violence peuvent être utilisés comme preuves.

Questions sur l'IdO

Voici quelques questions à se poser lorsqu'on envisage l'achat de voitures connectées, d'équipements à brancher sur les voitures ou d'applis:

- Cet appareil particulier doit-il absolument être «intelligent» ou «connecté»?
- Est-ce que les avantages l'emportent sur les risques?
- Quel est le niveau de sécurité de l'appareil et de l'appli qui le fait fonctionner?
- Existe-t-il des fonctionnalités qui permettent de personnaliser et d'accroître la sécurité et la confidentialité?

Stratégies pour accroître la sécurité et la confidentialité

Pour améliorer la sécurité et la confidentialité, il faut notamment se renseigner sur les options de sécurité intégrées, désactiver ces fonctions lorsqu'elles ne sont pas utilisées et modifier les mots de passe ou autres paramètres de sécurité par défaut.

Si vous soupçonnez qu'un appareil est utilisé à mauvais escient, documentez les incidents sans plus attendre. Notre journal de la violence facilitée par la technologie est un outil pour documenter chaque événement. Ces journaux peuvent être utiles pour révéler des schémas et déterminer les prochaines étapes, et peuvent éventuellement servir à constituer un dossier si vous choisissez d'intenter des poursuites.

Vous pouvez également tenter d'accéder à des preuves par le biais de l'appareil ou de son appli ou compte. Vous pouvez également essayer d'entrer en contact avec le fabricant pour reprendre le contrôle d'un appareil ou de son compte. Avec ces appareils, il est également important de prendre des mesures pour renforcer la sécurité du réseau et du Wi-Fi. Pour plus d'informations, consultez notre document sur la sécurité Wi-Fi.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Safety Net Project du NNEDV, d'après leur ressource Connected Cars and Driverless Vehicles Safety and Privacy Concerns.

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).

Femmes et Égalité des genres Canada Women and Gender Equality Canada Canada