BC Society of Transition Houses

Smart Cars and Driverless Vehicles: Safety and Privacy Concerns

While driverless vehicles get all the headlines, more and more passenger cars come off the lot already "connected," allowing parents to monitor and control teen drivers and employers to monitor employee driving habits. In addition, small gadgets can be attached to a car to allow for remote monitoring, and in some cases remote control.

WHAT IS "IoT"?

The Internet of Things (IoT) refers to devices connected to each other and to a device or app that can control them. These devices may be connected through the Internet, Bluetooth, or other means. Unfortunately, these devices or systems can provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten or harm women. At the same time, they can also offer potential tools women can use to strategically increase their safety.

SELF-DRIVING CARS

A few car-makers, rideshare services, and cargo delivery businesses are touting the future of self-driving cars. These cars combine a wide variety of sensors and systems that navigate a vehicle through city traffic, and on long stretches of highway. In almost all cases, the cars still require a person to be present in the driver's seat to take over if there is a problem. Many cars on the road today already include features basic computer-assisted features, where a computer assists the driver with a function, such as automatically engaging the brakes.

CONNECTED CARS

A number of services on the market today are designed to monitor and control the driving decisions of employees and teen drivers. The services are used to track driving habits and location and then deliver the information via an electronic report or with real-time updates. Options to control a car remotely or through pre-set limits include limiting speed, volume, and blocking texts or app alerts from reaching a teen's phone while driving. These could also be misused by a perpetrator to control a woman's vehicle.

A limited number of vehicles come with these services built-in, while many others work by plugging in a small device to the on-board diagnostics (OBD) port. The OBD system is a part of the car that many drivers aren't aware of – it's a computer that can monitor emissions, mileage, speed, and other data.

Some available apps also bypass the need for a plug-in device by using the driver's smartphone to gather and send information, and to block incoming messages.

SAFETY AND PRIVACY RISKS

The primary safety risk with connected cars is the possibility of remote control of the car. The most extreme risk would be crashing a car by taking over control of steering, braking or acceleration. Other serious risks include control of the stereo volume, lights, horn, windshield wipers, and other features. Hackers have demonstrated that it is possible to hijack control of all of those features in cars currently on the streets.

Privacy risks stem from tracking and sharing information about driving habits and location. Built-in, plug-in, and smartphone apps can all share information with someone remotely, providing the opportunity for monitoring and control. Manufacturers also store information collected from the vehicles, which can pose a privacy risk for unauthorized access.

BENEFITS OF CONNECTED & SMART DEVICES

While the risks of connected cars are deeply troubling, there are ways that the technology can be used strategically to increase safety. A woman who is concerned about the location of a car or its passengers could use these features for reassurance or to direct emergency services in case of a theft or abduction. A woman could choose to share location with trusted friends or family. Finally, a perpetrator's movements or driving habits could be used as evidence.

QUESTIONS ABOUT IoT DEVICES

When considering purchasing connected cars, devices to plug into cars, or apps, there are a few questions to consider:

- Does that particular device need to be "smart" or "connected"?
- Do the benefits outweigh the risks?
- How secure is the device and the app that runs it?
- Are there features that allow the user to individualize and increase privacy and security?

BC Society of Transition Houses

STRATEGIES TO INCREASE PRIVACY AND SAFETY

Steps to increase the privacy and safety include learning about the built-in security options, turning it off features when not in use, and changing the default passwords or other security settings.

If a woman suspects they are being tracked or monitored via their vehicle, they can begin to document the incidents. Our technology abuse log is one way to document each occurrence. These logs can be helpful in revealing patterns, determining next steps, and may potentially be useful in building a case if a woman chooses to involve the legal system.

Women might also try to access evidence through the device, or the app or website that controls it. They can also try to reach out to the manufacturer to try to regain control over a device or the account associated with it. With these devices and others, it is also important to take steps to increase network and WiFi security. For more information, see our handout on WiFi security.

Adapted from and in cooperation with the Safety Net Technology Project at the National Network to End Domestic Violence, United States