Am I smart enough to live in a smart world? Privacy and security for Internet of Things

Smart technology is meant to make our lives easier, more efficient, and more effective. Energy efficient smart lightbulbs will save us more money, remote door locks can easily let in guests when we're not home, and wearable technology can monitor our health while also keeping us updated with the latest social media post. As consumers adopt smart technology, there is a growing concern over the privacy and security of smart technology. For survivors of domestic violence, sexual assault, and stalking, their worries of smart technology include whether they might be controlled, monitored, or harassed by an abuser via these devices.

What makes it smart?

Smart devices are everyday items that are smarter and more efficient because it is connected to the internet. Because smart devices are generally connected to the internet – and that's what facilitates it's "smartness" – these devices are often referred to as the Internet of Things.

Ironically, what makes smart technology vulnerable and a concern is the same thing that makes it useful: it's access to networks, the internet, and other devices. For example, a smart plug that's connected to the internet allows you to turn off the plug remotely because you can access the internet (and, therefore, the plug) from your smartphone, tablet, or computer.

This access and connection turn every day objects into multiple forms of usefulness: Google Home is basically a speaker with artificial intelligence that's connected to the internet (and your Google account, smartphone, and apps) and lets you verbally perform Google searches, read your email, turn on apps such as Spotify and Netflix, as well as a wide range of other things.

For most consumers, there are two areas of concern with Internet of Things: (1) the security of the device, and therefore the security of your information that is stored and shared through those devices, and (2) the privacy of your information when it is shared or collected by the companies of these smart devices. For survivors of abuse, there is a third area of concern – (3) the abusive person's access to survivor's information and devices because they can access it remotely via the internet.

Security Concerns

Insecure devices

The major concern over smart devices is the inherent lack of security on some of the devices. Stories in the news and researcher and hacker demonstrations have shown how easily smart devices can be "hacked." The most well-known is the Cayla Doll, which was banned in Germany after it was shown how easily someone can connect with Cayla via Bluetooth and how hackers could take over the doll and speak directly to whoever is playing with Cayla.

Insecure internet connection

Another security concern is the vulnerability of the Internet. Because it is the internet connection that permits the communication and effectiveness of smart devices, if that connection is not encrypted, someone with the right skills could eavesdrop on the information being shared. The information could include usernames, passwords, and other sensitive information.

Insecure network

Moreover, if the internet router that the device is connected to isn't secure, someone with the right skills could hack the router and gain access to the insecure devices connected to that network. This concern is exacerbated since many smart devices are for home use, and home Wi-Fi network and routers may not have been set up with the appropriate security and encryption.

Privacy Concerns

The other area of concern is privacy. For smart devices to be "smart," it needs a wide range of information about the user. Not only is a smart TV connected to the Internet, it has the ability to remember what you watched so it can suggest TV shows and movies you might enjoy. For it to do this, the information of what you watched, along with other information, such as dates, times, voice commands, and other TV activity is saved somewhere – either in your tv, account, or with the company. Who can access this information depends on where this information is stored. If your TV activity information is saved in your account, anyone with access to your account will know what you watched. If the information is stored with the company, that company could share that information with advertisers or other 3rd parties.

Smart devices collect, store, and share different types of information, and it depends on what the smart device does. For example, some devices may be constantly "listening" and will record all surrounding sounds, including conversations. Some devices may record and store verbal information only after a certain command, such as "Hey, Siri" or "OK, Google." This information can be stored in your account or with the company.

Access Concerns

For survivors of abuse, there is a third area of concern with smart devices: the abuser's access to the survivor's smart devices if they have access to the account or remote access to the device. Obviously, abusers can gain access to all of a survivor's devices if they have access to accounts, services, and technology (e.g., email, bank account, and smartphone, respectively). However, the unique difference with smart devices is that the technology is generally every-day objects: TVs, plugs, door locks, wearable devices (such as fitbits or Apple watch), lightbulbs, refrigerators, and toys. Control over these objects can permit the abusive person to cause havoc for the victim, from just using it to monitor and for surveillance to gas lighting or making her think she's going crazy.

The goal of an abusive person is to gain power and control over the survivor, usually through harassment, intimidation, inducing fear, and limiting their ability to live their daily life. An abusive person can do this by having control over a survivor's technology and everyday things – whether it

is by preventing those devices from working or gathering information from those items to facilitate controlling and abusive behaviour.

What can you do?
Privacy and safety while using IOT

Rejecting smart devices isn't necessarily the answer. Instead, be aware of the risks when you use a smart device and learn what you can do to increase privacy and security. Although each smart device will be different, here are some general tips.

1. Know how your smart device works

Although it may be tempting to plug it in, turn it on, and forget it, the first step to staying on top of your privacy, security, and safety when using a smart device is to understand how it works. Smart devices are mostly about connections and information sharing. When you set up a smart device, you will either create an account for that device, attach an email to that device, or connect that device to a network (usually your home Wi-Fi network) – or perhaps all the above. Having a general idea of how your smart device works and what it's connected to will help you determine what information is shared and how it is accessed, which will help you identify potential risks so you can minimise those risks.

2. Limit connections to your smart device

Smart devices are all about connections. Review how and what it is connected to. If it's connected via Wi-Fi, turn it off when you're not using it. If you can't turn it off, disconnect it from the internet. If it has other types of access, such as Bluetooth, turn off the connection access. If it's turned off or not connected, it will not be possible for someone to access the device remotely.

3. Limit personal information shared from your smart device

Information about you are stored either on the device, in an account, or with the company. If you are worried about someone gaining access to your information, determine whether you can limit personal information stored or shared via the device. This can include turning off the device when not in use, turning off cameras or microphones, or reviewing the device's settings and limit how much information the company can gather about you. Read the company's privacy policy to learn about how they share your personal data.

4. Secure the account associated with your device

Some devices require you to set it up with an account, where you create a username or password. Create a username and password that someone else (including the abusive person) can't guess. Some accounts may offer 2-step verification, in which if someone were to try to access your account from a different device or location, they will require an additional verification code (generally in the form of an SMS code).

If the device doesn't require a username/password to access, know how it connects and whether someone else would be able to connect to it.

5. Increase the security of your home network router

Because smart devices are mostly connected to a home Wi-Fi network, make sure that your home router is secure. There are many things you can do to increase your home router's security, including the following:

- Put a passcode on your home Wi-Fi network
- Change the router's username/password from the default
- Use WPA2 encryption
- Turn off remote management on the router

Read our article on "Securing Your Home Wi-Fi Network" for more information.