Robbinsville Internet Safety Night

Internet Safety for Children

Definitions and Goals of this Session

What is the Internet?

- The most important communication break through of the 20th Century
- It is a **tool** designed to be used by all people
  - It is important to be familiar enough with the Internet to be safe
- The Information Super Highway
- It serves as the backbone for all the primary forms of digital communication your children will interact with throughout their lives

Where is the Internet in Our Homes?

Everywhere!

Defining Risks by Age Group

Age Groups Risks (Young Children)

- Risks for children 8 year old and younger
- Content risks:
- *This might include pornography, images of cruelty to animals, and real or simulated violence.*
- Contact risks:
- *These risks include children coming into contact with people they don't know or with adults posing as children online.*
- Child might be persuaded to meet someone he doesn't know, share personal information with strangers, or provide contact details after clicking on pop-up messages.
- Conduct risks
- *These risks include children acting in ways that might hurt others, or being the victim of this kind of behavior.*
- *A child might destroy a game her friend or sibling has created.*
- *Another conduct risk is accidentally making in-app purchases.*

Age Group Risks (Pre-teen)

- Risk for Pre-teen kids
- Pre-teens tend to use the internet independently. They can come across more risks than younger children.
- Internet safety risks for pre-teens include content, contact and conduct risks.
- **Content risks:**
- Things that are designed to shock or scare
- Harmful user-generated content, like sites about drug use, self-harm, suicide or negative body image.
- **Contact risks** (Same as Previous Slide)
- **Conduct risks**
- Cyberbullying
- Sexting
- Impersonating others online
- Creating content that reveals information about other people
- Buying something without permission
- Having trouble regulating online time

Age Group Risks (Teen)

- Your child needs to keep building skills and knowledge to identify and manage internet safety risks independently.
- **Content Risks:**
- Hate sites
- Terrorist sites
- Harmful user-generated content like sites about drug use, self-harm, suicide or negative body image
- **Conduct Risks**:
  - Misusing people's passwords and impersonating people online
  - Making unauthorized purchases using other people's financial details
  - Creating content that reveals information about other people

How to Protect and Teach Your Children to Use the Internet Safely

Protection Strategies

Secure, Equip, & Education

- Access Control
  - Good for younger kids, first line of defense for all age groups

Empower your kids to protect themselves

- At some point your kids will have seemingly ubiquitous access to the Internet
  - “Our kids are digital natives, and we’re digital immigrants” *Deborah Gilboa*
- They will need to know how to safely navigate the Internet

Communication

- Establish trust and a relationship with your child where you can talk freely

General Best Practices

- Stay Current yourself
- There is no “lock it and forget it” protection strategy
- Avoid creating any online accounts of any kind in your child’s name
- Limit screen time for younger children
- Help your child learn to manage Internet safety risks by being a role model, and talking with your child about online content and activities
- Taking an interest in your child’s online activities builds trust and encourages your child to talk to you about online worries
- Do not share your passwords with your children
- Do not let your children access a computer that is logged on as you

Understanding Privacy and Tracking

Corporate Tracking

- This is the practice of corporations gathering and selling your data for marketing and other reasons
- This is the primary business model for social media

Identity Theft

- The risk to the children of this is reasonably low

What is the Dark Web?

- The **Dark Web** is a term that refers specifically to a collection of websites that exist on an encrypted network and cannot be found by using traditional search engines or visited by using traditional browsers. Almost all sites on the so-called **Dark Web** hide their identity using the Tor encryption tool

Protecting Younger Children

- Establish Trust:
  - Show them what to do and explain why you are doing it.
- Lay Ground Rules:
  - Define rules for screen time
  - Set the precedent that their on line activity is not private and that you will be checking it regularly
- Never provide their personal details without your permission:
  - Name; home address
  - Email address
  - School
  - Photo
  - Hobbies

Access Control & Content Filtering

Make sure that you spend the time to secure every new device as it comes into the home.

- Check that the settings are still in place often.
- Set the correct content filtering settings on all accounts.
- If you do not have a generic Gmail account, get one.

Have good password and Internet Security habits.

There is no substitute for you supervising your children’s activity.

Content Context Filters

It is important to enable logging into and setting content filters for all devices.

- Logging on to Youtube on all devices, including all your TV’s, Firesticks, etc. and setting content filters
  - *Besides letting you set content restrictions and see history of what is being viewed*

There are limits to content filters, especially for younger children.

Other Context Concerns

There are a lot of services where it is next to impossible to regulate the content and the context of the content e.g. Gaming Consoles (on-line gaming).

- Verbal Communication with others including unknown people is possible.
- Recommend that for kids of this age group that on-line gaming should be avoided.
  - *It is important that if your kids do play games that you play with them on a semi-regular basis to establish a behavior pattern that you will be part of this activity*

Pre-Teen Children

- Never open or reply to emails that are sent from people they don't know
- Never respond to bullying or hurtful messages anywhere, including emails, texts or social media
- Never "talk" to strangers online or agree to meet anyone in-person
- Texting and Social Media
- You should friend your children on all social networks they belong to

Social Networking

Social Networking and messaging often have blurry lines.

For the purposes of this discussion we will look at Social Media as a 1 to many publication and texting and messaging as 1 to 1 or 1 to a few publications.

Social Media
Social networking sites, chat rooms, virtual worlds, and blogs are how teens and tweens socialize online; it's important to help your child learn how to navigate these spaces safely. Among the pitfalls that come with online socializing are sharing too much information or posting comments, photos, or videos that can damage a reputation or hurt someone's feelings.

Messaging

Most Social Media sites have a direct messaging feature. On top of that there are also applications that are pure messaging applications.

Facebook messenger (adult and kids versions), WhatsApp, SMS, KIK, Snapchat, Google Hangouts, Twitter, etc.

Teenagers

- All of the risks that exist for pre-teens exist for teens as well, however as they mature their usage of the Internet these risks increase with their increased autonomy
- Participate in on line activities with your children
- Play on-line games with your children to observe the content and decide if that environment is appropriate for your child

Cyber Bullying

Bullying is not new and it is a behavior.

The Internet, specifically Social Networking, increases the visibility of the actions.

Agreeing on clear rules about when your child can use her mobile phone, computer or tablet can help her avoid cyberbullying. For example, cyberbullying often happens at night through text messages and shared images.

Cyber Bullying Description

- Posting or sending messages that threaten people or put people down
- Leaving people out of online games or social forums
- Spreading nasty rumors online about people
- Setting up unkind or unpleasant fake social media accounts using real photos and contact details
- Trolling or stalking people online
- Sharing or forwarding people’s personal information
- Posting insulting or embarrassing photos or videos of people
- Harassing other people in virtual environments or online games

Cyber Bullying: Spotting the Signs

General Behavior Changes

- refuses to go to school
- starts getting lower marks than usual
- doesn’t want to see friends
- doesn’t want to take part in her usual sports and other activities
- avoids group gatherings

Technology use

- is upset during or after using the internet
- spends much longer than usual online, or refuses to use the computer or mobile phone at all
- stops what he’s doing on the computer if you go past

Emotions and behavior

- Is more moody than usual
- shows obvious changes in behavior, sleep or appetite
- gets unusually angry at home
- feels sick or complains of frequent headaches or stomach aches

Texting: Acronyms parents should know

FWB	Friends with benefits
FYEO	For your eyes only
GAL	Get a life
GB	Goodbye
GLHF	Good luck, have fun
GNOC	Get Naked on Cam
GTG	Got to go
GYPO	Get your pants off
HAK	Hugs and kisses
HAND	Have a nice day
HTH	Hope this helps / Happy to help

8	Oral Sex
1337	Elite or leet or 1,337
143	or 459 I love you
182	I hate you
420	Marijuana
1174	Nude Club
2DAY	Today
4EAE	For ever and ever
ADN	Any day now
ADR	Address
AEAP	As early as possible
AFAIK	As far as I know
AFK	Away from keyboard
ALAP	As late as possible
ASL	Age/sex/location
ATM	At the moment
BFN	Bye for now
BOL	Be on later
BRB	Be right back

Protecting against On-Line Predators

The Online Predator:

1. Blends into society
2. Is typically clean-cut and outwardly law abiding
3. Is usually white, middle-aged or younger, and male
4. Uses position in society to throw off suspicion
5. Can rise to be a pillar of society while actively pursuing children
6. Often engages in activities involving children
7. Appears trusting to both parents and child

What Fuels Online Predators?

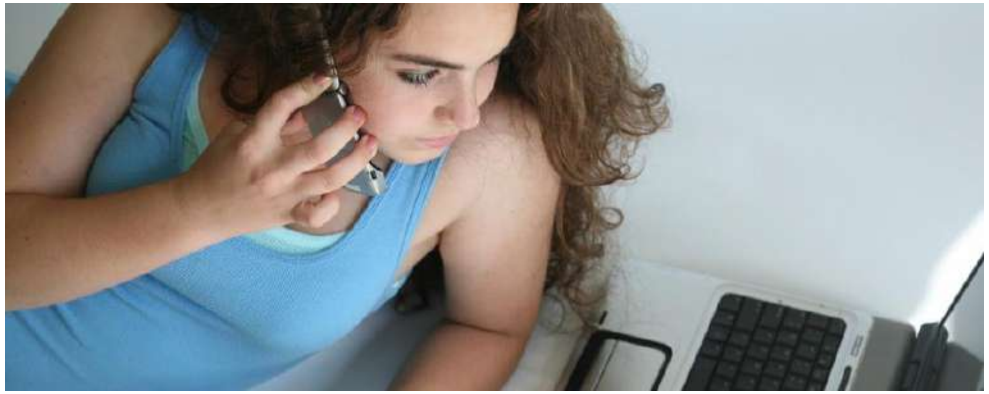
- Easy and anonymous access to children
- Risky online behavior
- Virtual validation (communication with other pedophiles via chatrooms, etc.)
- Law enforcement challenges
- Easy access to “a la carte” child pornography

Protecting against On-Line Predators

Understanding Grooming

What is "Grooming"?

Online grooming is a process in which a predator uses seemingly casual or innocent information with the goal of establishing a relationship to gain a child's trust. It may start with something as simple as a popular music group, sports team, or clothing trend.



During the "Grooming" process, predators will:

- Affirm feelings and choices of child
- Exploit natural sexual curiosities of child
- Ease inhibitions by gradually introducing sex into conversations or exposing them to pornography
- Flatter and compliment the child excessively, send gifts, and invest time, money, and energy to groom child
- Develop an online relationship that is romantic, controlling, and upon which the child becomes dependent
- Drive a wedge between the child and his or her parents and friends
- Make promises of an exciting, stress-free life, tailored to the youth's desires
- Make threats, and often will use child pornography featuring their victims to blackmail them into silence

WHY ARE THEY SEXTING?

- To be funny
- To impress a crush
- Peer pressure or threats
- Experimenting with relationships, sexual behavior, and boundaries

Talking to you Kids about Sexting

Ask questions to make it clear you're comfortable discussing it.

- Has anyone ever asked or pressured you to sext?
- Have you ever received a sexy picture from someone?"

Discuss what characterizes a healthy relationship.

- Any person pressuring to sext isn't someone you should trust.
- Boyfriends and girlfriends come and go, but a sexual image of you can stay around forever.

Explain how quickly images can spread.

Emphasize the importance of not forwarding image follows them for a long sexts they receive.

- You do not have to decide who should see someone else's body.
- Forwarding images is a major violation trust and exposes the person in the picture to potential ridicule.

Risks of Sexting

Teens who take, send or forward sexting images may face:

- Embarrassment if their picture is shown to family, friends, classmates and even strangers.
- Trouble with the police. In extreme cases, kids can be charged for sending or forwarding nude images of minors.
- Bullying or harassment from peers who judge them for sexting.
- Teens have been kicked off of athletic teams or suspended.

What if your Child has Sexted

This is one of the best ways to stop your image from spreading if it is on a website/app or being shared without your consent.

REPORT IT:

To the website or app. Trustworthy websites/apps work hard to keep off sexual images of minors and will remove them if notified. You can also report anyone who is posting or sharing images of you. For more information about reporting to popular websites/apps, visit **https://needhelpnow.ca/removing_pictures**.

To CyberTipline.org. This tipline can connect you with the experts best suited to work on your case. They may contact the website or the police, or reach out to you for more details. You can report without sharing your name and can even make a report for a friend if they need help.

To the police. They can help stop your image from spreading by working with websites/apps and talking to the people sharing it. You should know if the police get involved, you could face some consequences, too. It's illegal to share sexual images of minors even if they are of you. You may not be charged with a crime, but you may have to attend classes or complete community service.

To an administrator. If your pictures are being shared around school, your teachers and school administrators can help stop it by making clear there are consequences for sharing them.

What if your child is being blackmailed?

Blackmail is when someone tries to threaten or scare you into doing something. For example, teens may share sexual images with people they trust, only to have those people turn on them. They may threaten to send the images to teens' families unless the teens share more images.

If you're being blackmailed, you may feel helpless or guilty. You may think you don't have the right to say "no" because you shared the first image willingly. WRONG! Blackmail is illegal and you don't have to take it.

YOU SHOULD:

Stop any communications with blackmailers. They'll try to use your conversations to threaten and manipulate you – don't give them the chance. Even if you have already started communicating with them, it's never too late to stop and report it.

Block or remove the blackmailer from your contact list. If you decide to deactivate your accounts, contact the websites/apps for help.

Make a report to the police and CyberTipline.org right away. Seriously. They can help. They may want to see any messages you've received from the blackmailer.

Summary

As parents, what can we do to help keep our kids safe online?

Talk With Your Kids. Begin early conversations about online safety using vocabulary/language that is meaningful to children based on their age. Ensure that this is an ongoing dialogue so that communication is open and regular.

Educate Yourself and Your Kids. Educate children about the importance of keeping their personal information safe (name, address, phone number, passwords). Understand how the apps and games your kids are using work by trying them out.

Keep the Lines of Communication Open. Emphasize the importance of telling a parent/caregiver if any online interaction makes him/her feel sad, scared, or confused.

Be Active and Involved. Know the sites your kids spend time on and who they are talking to. Join them by watching videos with them or playing games with them.

Set Ground Rules. Establish limits. This could include limits on the amount of time a child spends online, which websites they are visiting online, or where they access the internet (at home in a central location v. on their phone at a friend's house).

Use Parental Controls. Apps like Verizon Smart Family can help you monitor and set limits on the content your kids are engaging with. Set time limits and filter content using the app.

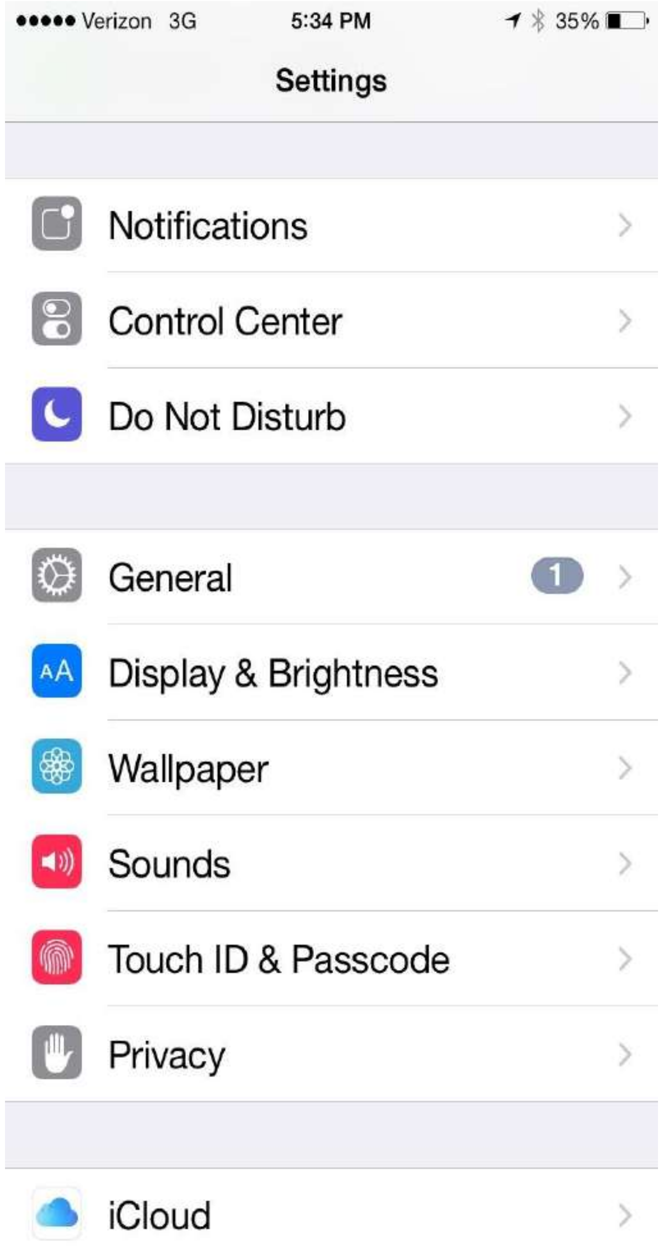
Role Model Good Digital Behavior. Consider device-free meals and avoid texting while driving. Kids are more attentive to what their parents do versus what they say.

Questions

Tools & References

- PCMAG list of child safety tools
- https://www.commonsensemedia.org/reviews
- Robbinsville Curriculum K-4
- Robbinsville Curriculum 8'th Grade
- Secure your Devices
- https://internetsafety101.org
- https://rockinmama.net/internet-safety-for-kids/
- https://www.safety.com/internet-safety/
- https://www.consumer.ftc.gov/features/feature-0002-parents

Examples /Demo



●●●●● Verizon 3G 5:34 PM 35%

Settings

Notifications

Control Center

Do Not Disturb

General 1

Display & Brightness

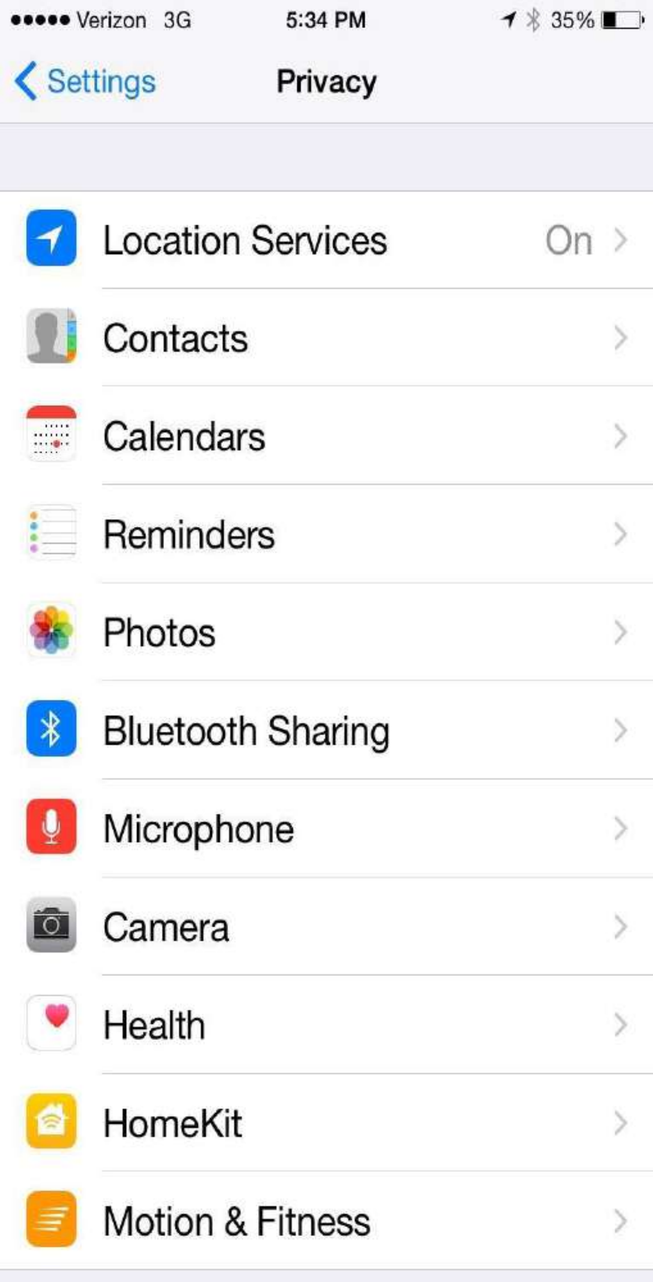
Wallpaper

Sounds

Touch ID & Passcode

Privacy

iCloud



●●●●● Verizon 3G 5:34 PM 35%

< Settings Privacy

Location Services On

Contacts

Calendars

Reminders

Photos

Bluetooth Sharing

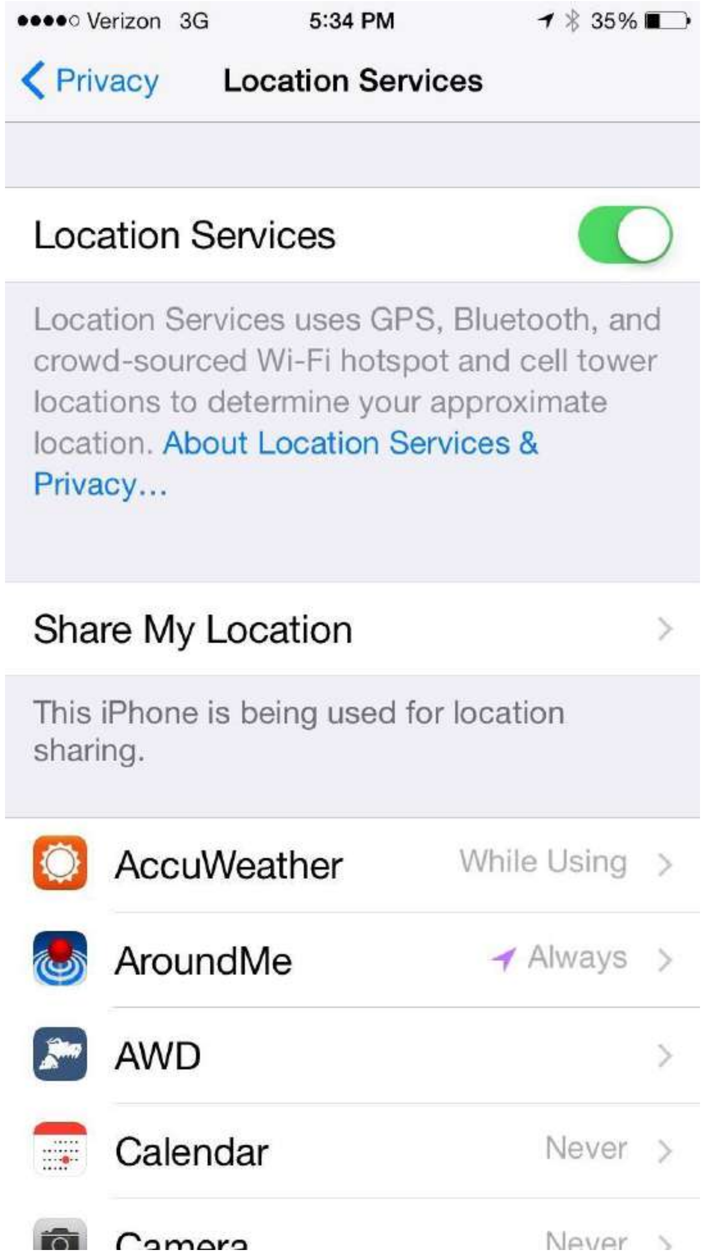
Microphone

Camera

Health

HomeKit

Motion & Fitness



●●●●○ Verizon 3G 5:34 PM 35%

< Privacy Location Services

Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy…

Share My Location

This iPhone is being used for location sharing.

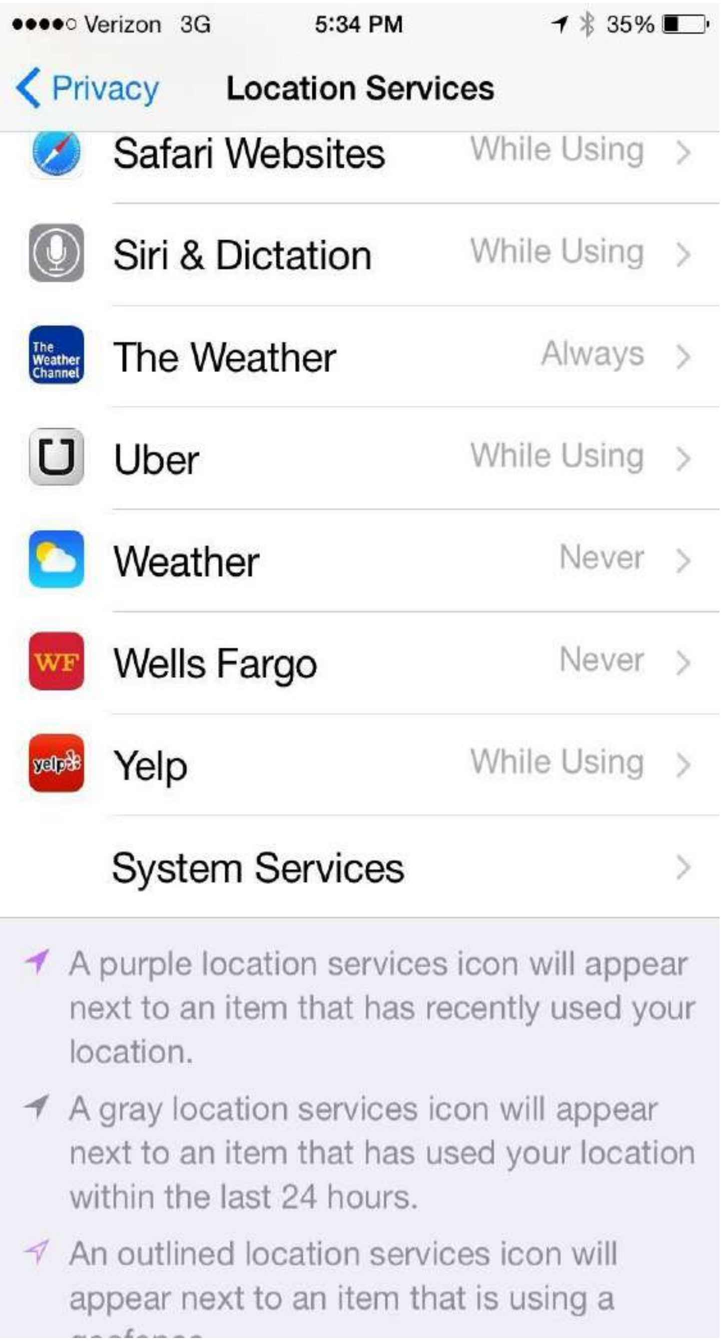
AccuWeather While Using

AroundMe Always

AWD

Calendar Never

Camera Never



●●●●○ Verizon 3G 5:34 PM 35%

Privacy **Location Services**

Safari Websites While Using

Siri & Dictation While Using

The Weather Always

Uber While Using

Weather Never

Wells Fargo Never

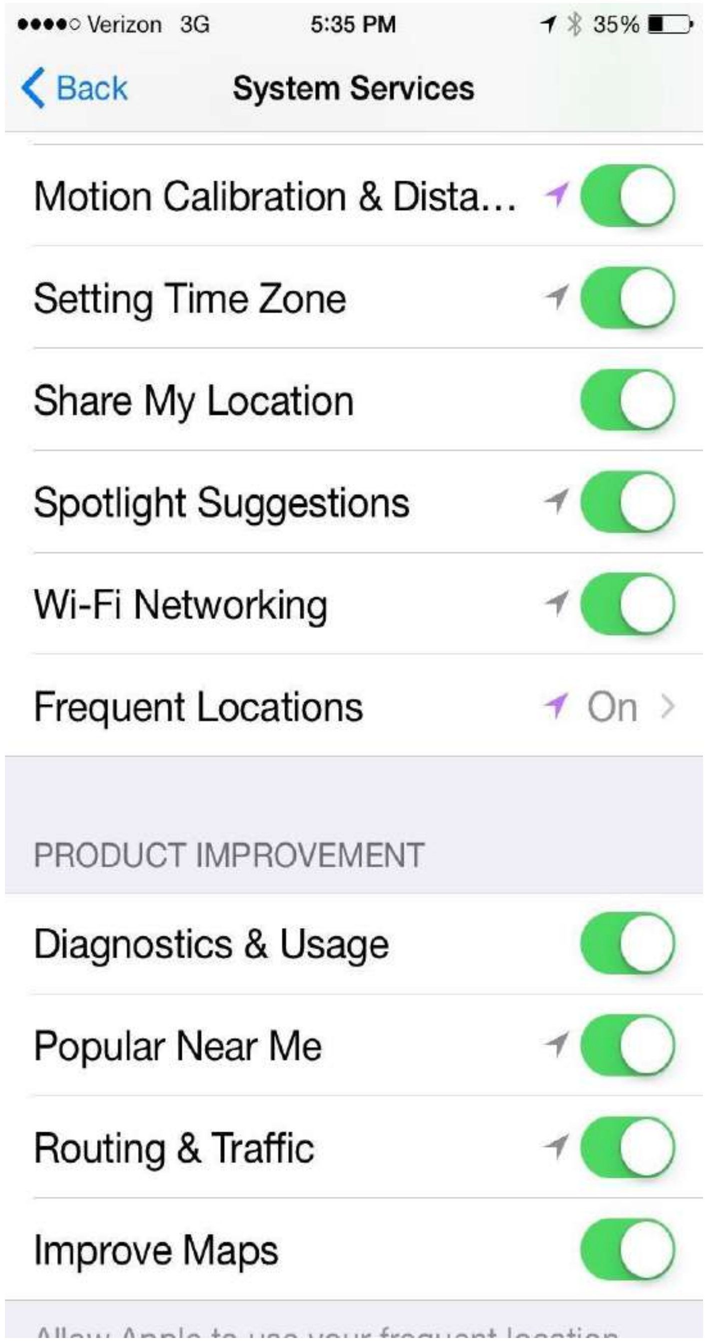
Yelp While Using

System Services

A purple location services icon will appear next to an item that has recently used your location.

A gray location services icon will appear next to an item that has used your location within the last 24 hours.

An outlined location services icon will appear next to an item that is using a



●●●●○ Verizon 3G 5:35 PM 35%

Back **System Services**

Motion Calibration & Dista…

Setting Time Zone

Share My Location

Spotlight Suggestions

Wi-Fi Networking

Frequent Locations On

PRODUCT IMPROVEMENT

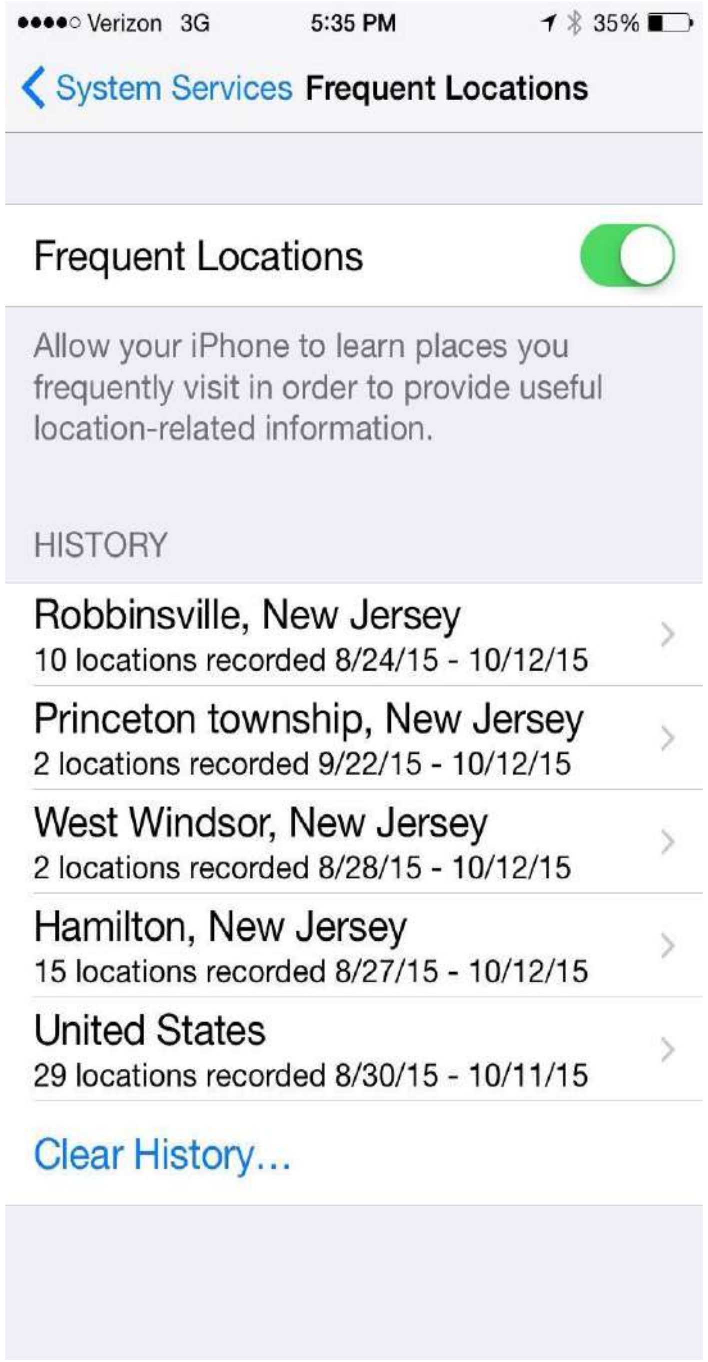
Diagnostics & Usage

Popular Near Me

Routing & Traffic

Improve Maps

Allow Apple to use your frequent location



●●●●○ Verizon 3G 5:35 PM 35%

System Services **Frequent Locations**

Frequent Locations

Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.

HISTORY

Robbinsville, New Jersey
10 locations recorded 8/24/15 - 10/12/15

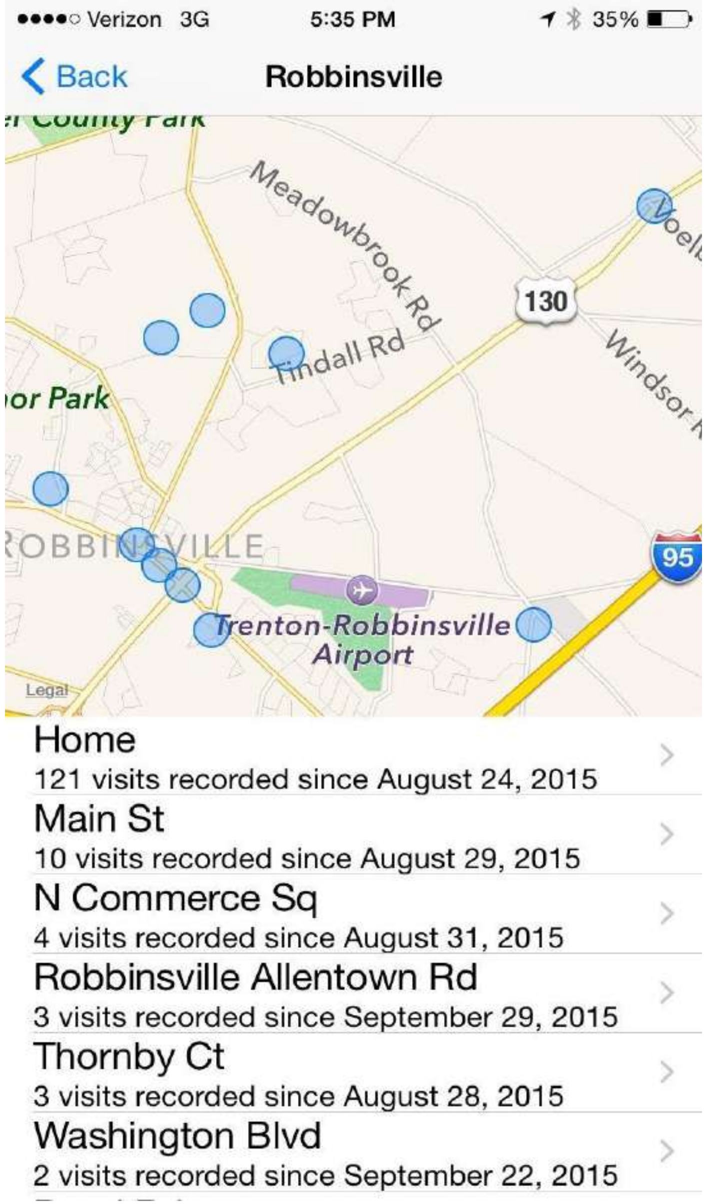
Princeton township, New Jersey
2 locations recorded 9/22/15 - 10/12/15

West Windsor, New Jersey
2 locations recorded 8/28/15 - 10/12/15

Hamilton, New Jersey
15 locations recorded 8/27/15 - 10/12/15

United States
29 locations recorded 8/30/15 - 10/11/15

Clear History…



Home
121 visits recorded since August 24, 2015

Main St
10 visits recorded since August 29, 2015

N Commerce Sq
4 visits recorded since August 31, 2015

Robbinsville Allentown Rd
3 visits recorded since September 29, 2015

Thornby Ct
3 visits recorded since August 28, 2015

Washington Blvd
2 visits recorded since September 22, 2015