Dangers of Social Media and Phone Apps

Ofc. Chad Andersen

Anthony Ln COP Officer

262-619-2511

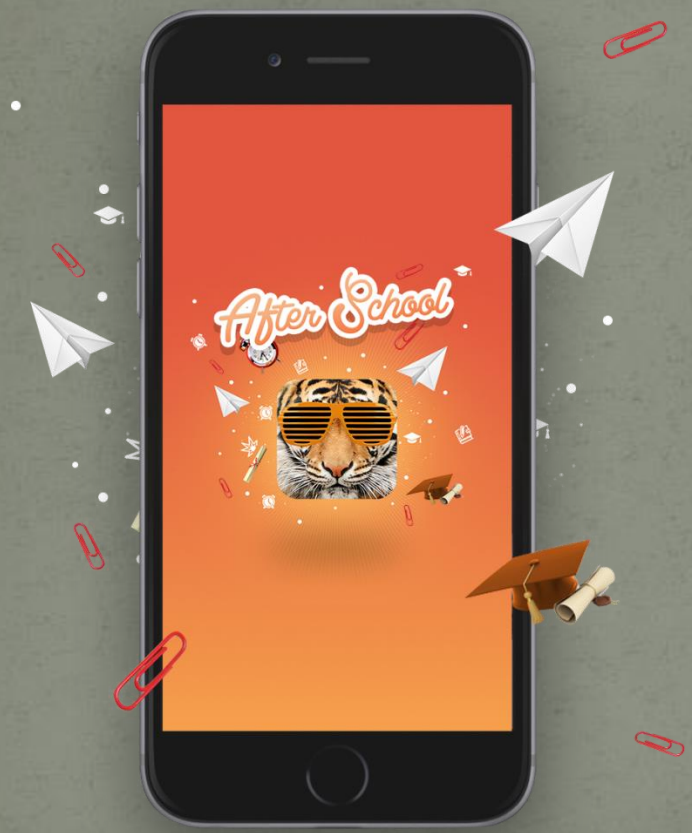
Dangers of Social Media to discuss with your children

- "Stranger Danger" - It's no longer just talking to your children about dangers on the playground
- Oversharing Information – Don't reveal too much
- Hidden geographical info in photos – Photos contain EXIF data, which is data that can be used to pull the exact geographical location of where the photo was taken
- Information on social media will stay forever
- Cyberbulling – Will others get hurt?

Phone Apps

- After School
- Ask FM
- Badoo
- BurnBook
- Calculator% Private Photo
- Chat Roulette
- Cyber Dust
- Dubsmath
- Find my Friends
- Fit Bit App
- Free Full Screen Private Browsing
- Kik Messenger
- Omegle
- Periscope
- Phhhoto
- Secret Calculator
- Snapchat
- Tinder
- TikTok
- Whisper
- Wishbone
- Yeti
- Yodel
- You now
- Youtube

AfterSchool App



- AfterSchool App is an anonymous app that creates a separate chat group for every school. It has been removed twice from the AppStore because of threats and arrests.
- Messages often include bullying/threats, pornography, and alcohol and/or drug references.
- Does have parental control that allows parents to password protect access to the app.
- All posts go through a moderation process before being posted, but moderation does not eliminate all posts.

Ask.fm

- Over 150M users
- Ask questions to any friend – anonymously or not
- Follow friends to see all the questions they've answered
- View everyone that has liked your answers to questions.
- Promoted as "A safe environment where you can express yourself freely, however, Ask.fm is one of the godfathers of cyber bullying apps. It encourages students to set up a public profile and allow anonymous people to ask them questions. This encourages bullying and can really hurt their feelings. Students often reveal too much personal information, to which cyberbullying is very prevalent.

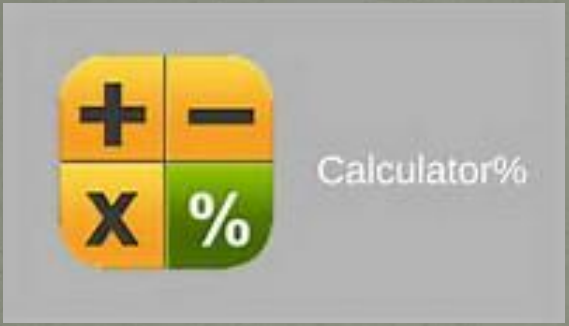
Badoo – Meet New People, Chat, Socialize

- Badoo is the App that shows you the people nearby, and even better, the people you've bumped into in real life.
- Badoo is a dating-focused social networking service/app, with it's headquarters in London.
- In 2009, Badoo was given the lowest score for privacy amoung 45 social networking sites examined.

BurnBook App

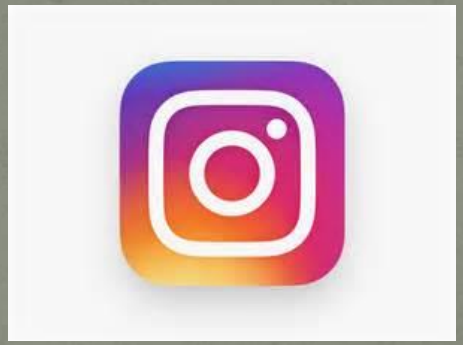
- BurnBook is an anonymous app for posting text, photos, and audio rumor messages about others. The app compiles messages by school, so **the app requires access to your location (GPS).** It encourages students to screen shot the rumors and save them to their phone, which causes cyber bullying issues.
- BurnBook gives you points if you capture screen shot rumors and save them to your phone.
- BurnBook *treats cyber bullying as a game.*

Calculator Vault – Hide Pictures and Videos



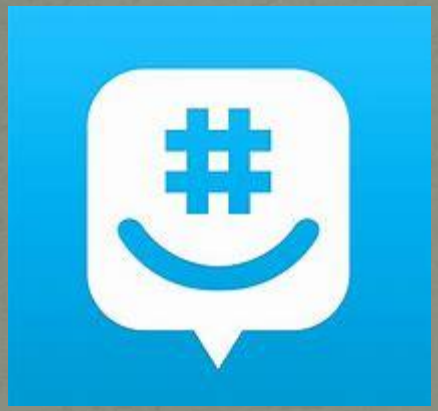
- Developed by stating, “Don’t risk your private pictures, secret videos or photo albums falling into the wrong hands or being deleted.” (Hmmm…could this be parents?)
- The Private photo (Calculator%) is designed to help students hide photos and videos behind an innocent looking calculator app that is password protected.

Facebook/Instagram



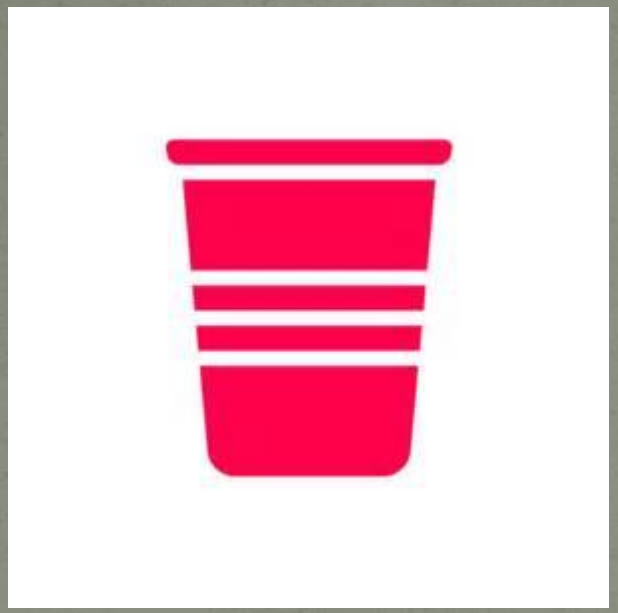
- The issue with Facebook and Instagram is that many students are in competition with each other to see how many "likes" they can obtain. Not only does this cause users to leave their profiles on "public privacy," but it also allows predators to easily access their info and know exactly what to say to them based on their interests and posting patterns. Based on the student's settings, both of these have location services that will potentially tell the world exactly where your child is posting from. Students will create more than one profile to access other people, interests, contacts for illegal activity, etc, but will show the parents "their profile."

GroupMe



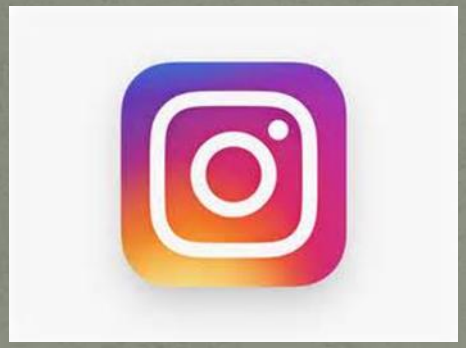
- Used for students to discuss homework, but obviously topic of discussion can change very easily (ie house parties, gossip, bullying, etc)
- Once downloaded, anyone can start a group chat, which is done by adding phone numbers. Once a phone number is added only one time, others will have that info. Predators can obtain child's info very easily. Now, the predator can directly contact your child via text messaging.
- Accessibility to sexual images is an issue, as there is no parental control.
- Cyberbullying is an issue as others in the group chat can gang up on one person.
- You can't delete previous chats.

Houseparty



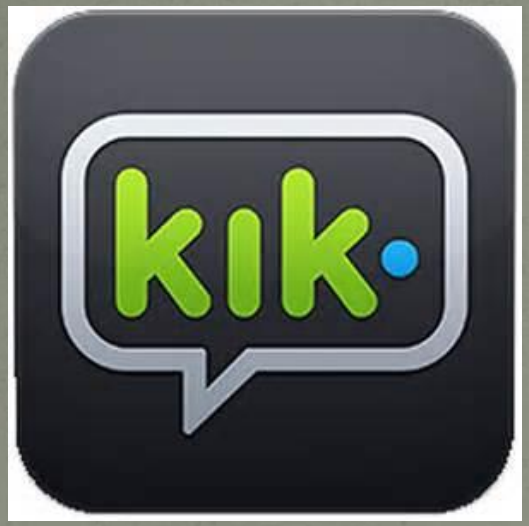
- This app is a way for people to be together even when they're apart. Students get together through the app and "live chill" from anywhere, including the comfort of their bedrooms.
- Students can live chat and see each other in REAL TIME.
- Be aware of who your children are "live chilling" with and if they are people you'd want them to chill with in real life.

Instagram



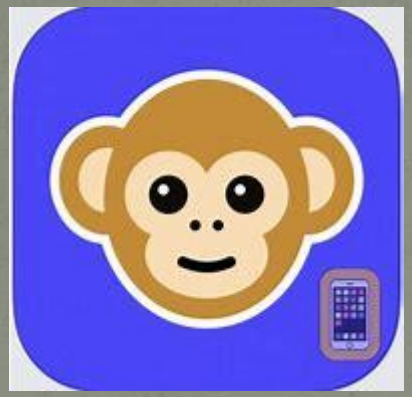
- A favorite social media forum for teens that focuses primarily on perfect photos and/or videos. Users can share selfies, memes, gifs, and other items that allows others to comment on.
- Instagram has “followers.” Find out who your child is following and equally important, who is following your child. You must check on your child’s followers very frequently. Sit with them and have them explain who each and every person is. This may not be a quick process as students may have 100’s or even 1000’s of followers.
- Instagram does have some filters/parental control.
- Finsta – slang term for fake Instagram account.

Kik Messenger



- This app is referred to as Kik and is a free instant messaging service similar to text messaging. This app is very popular for cyber bullying as anyone can create an account and send messages, photos, and videos completely anonymously to either one person or as a group message.
- App not based in the U.S.
- Some adults have used this app to pretend they are teens, thus making them a predator.
- Reported 40% of students with smart phones use this app.
- Users of Kik can come across online predators who target them either for immediate exploitation (attempts at sexting, exposing them to graphic imagery, etc.), or the more insidious practice of grooming (deliberately earning their trust in order to leverage them to do things such as provide personal information, images, or even to meet offline).
- NO PARENTAL CONTROL PROTECTION

Monkey



- Monkey's own description: "Monkey is a place to have fun chats with new people from all over the world." (Or right in your own neighborhood.) "Meet people in trees that match your interests and add people you like to your friends list."
- The picture of the app looks fun and innocent. Young children may download app based on this picture.
- Because sexual predators know this, they can easily create a fake profile and start talking with your young children.

MyLOL Dating App

- #1 teen dating app in the US, UK, and Canada and is designed for students 13-19 yrs old
- Encourages users to send private messages to complete strangers
- Like other apps, user can manipulate their DOB so it shows they are under 19 yrs old
- MyLOL directs the user to upload a picture from another social media source
- Vote on members if they are attractive or not (self-esteem issues??) and receive points
- Generally vulgar, sexual in nature, and not appropriate for teens
- All profiles are made public

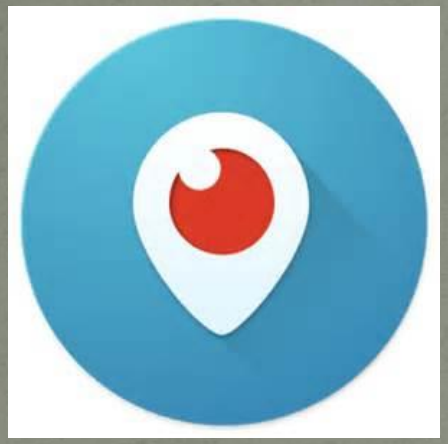
Ogle

- Ogle is an anonymous app that automatically searches your location for nearby schools when downloaded.
- Users of Ogle post photos, videos, thoughts, questions, comments, etc, anonymously!
- Cyberbullies and predators can manipulate their registration information so it gives the perception that they are students or friends.

Omegle

- Omegle is an anonymous text and video chat room that connects strangers to talk with each other. The app allows you to share personal information, and also contains inappropriate and UNMODERATED content.
- Their slogan is: “Talk to strangers!” Omegle has a video chat feature, which, again, is not moderated by administrators.

Periscope



- Owner by Twitter, which syncs the Twitter account to Periscope
- Live broadcasting
- "No content monitoring"
- ***GPS LOCATION OF THE USER IN REAL TIME. GPS monitor will direct a potential predator within 100 yards of your child***

Secret App

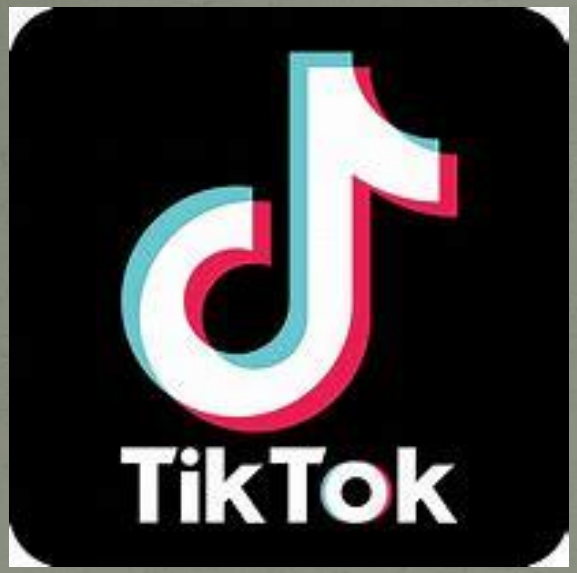
- Secret in an app that allows people to share messages anonymously within their circle of friends, friends of friends, and publicly. When a student sees a secret about them on the app, they don't know who posted it, but they do know of one of their connections that sent it. This can cause bullying and anxiety.
- Students often hide behind being anonymous when posting and forget that anonymous does not mean untraceable.

Snapchat

- Children think this app is safe because they can send info to friends & strangers that "disappear." It makes user feel secure in sending pics & videos that may not be normally sent. However, others may take a screenshot of the content that could include inappropriate pictures and/or videos, and post that screenshot at a later date without initial person ever knowing that it was sent.
- SnapMap - If a user creates a "Snap" that gives out personal information and they send it to "Our Story", it can be seen by the entire community and then possibly put on the World Snap Map with whatever personal information the user has shared. This is another tool predators can use to find their targets.
- This is a popular app as children are more drawn to social apps and networks that are based on messaging rather than news-feed style such as Facebook and/or Twitter.

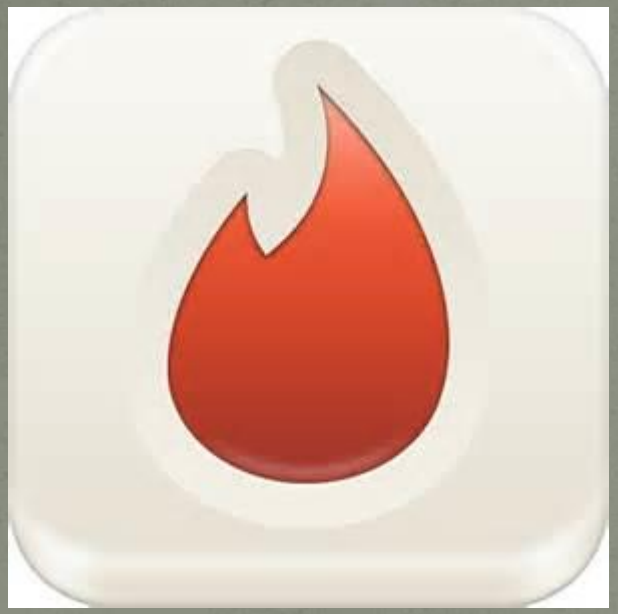
- https://www.youtube.com/watch?v=fg-LhgZLB8M

TikTok



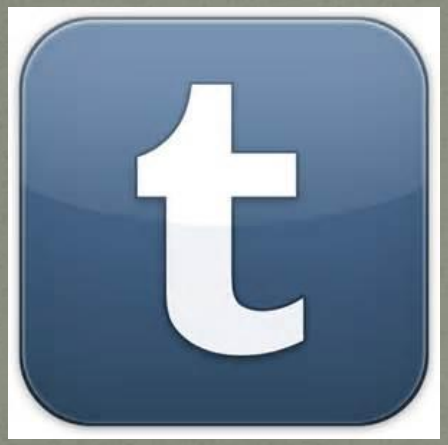
- Originally available as “musical.ly”
- 100 Million users
- Interactive world of videos that others can like, comment, and share freely
- Account is defaulted to public, not private (GPS monitoring).
- Live streaming could be an issue

Tinder App



- Tinder is a dating app, marketed to adults, that allows users to connect with other Tinder users. Despite the app increasing it's age restrictions, many parents are wondering, "What is Tinder?"
- Tinder is a dating app that uses the real-time geo-location data of nearby users to connect with one another, and for much of 2013, a vulnerability in the app allowed a user to track the exact location of another user while the app was running. When the app was closed, a user could still be tracked to the last place they used Tinder. According to Tinder, this error has been corrected, however, I ask you this, can you trust apps like this to keep your kids safe?

Tumblr



- Tumblr is one of the world's most popular blogging platforms. In 2013, Tumblr's terms of service stated they would NOT delete pornographic information (and they were OK with that sort of content). They encourage students to hide from their real identity, by creating fake usernames, email addresses, and birthdates. (It took me less than 4 minutes to create an identity).They have a huge search box at the top of the page and pornographic information can still be found very, very easily!!

Whisper App

- The rated 17+ app's motto is "Share Secrets, Express Yourself, Meet New People."
- People post messages known as whispers, and receive replies completely anonymously. People contact or respond directly to the actual post. This is a hotbed for cyberbullying because it is virtually untraceable making students feel they can do anything and post everything without any repercussions.
- Whisper lets users set up anonymous accounts.

Youtube

- Youtube isn't necessarily dangerous, but without appropriate filters and parental controls, children can quickly be exposed to inappropriate content. Enabling the Safety Mode Feature will help filter out MOST of the inappropriate videos and content, but not all.

Cyberbullying

- Students tend to use Instagram rather than Facebook. I was told by a middle school student that Facebook is for "old people."
- Approximately 34% of students report experiencing cyberbullying in their lifetime (Patchin, 2015).
- 15% of students admitted to cyberbullying others during their lifetime. (Patchin, 2015).
- Adolescent girls are more likely to have experienced cyberbullying in their lifetime (40.6% compared to 28.2%). The type of cyberbullying tends to be different among gender. Girls are more likely to post mean comments while boys are more likely to post hurtful pictures or videos (Patchin, 2015).
- Of the 60% of parents who reported checking their teen's social media profiles, 35% knew the password to one or more of their teen's social media accounts and 39% used parental controls at least once (Journal of Adolescent Health, 2017).
- Social media is associated with mental health problems, which includes depression, sleep disturbances, and eating concern (Journal of Adolescent Health, 2017).

Cyberbully continued

- According to the National Center for Education Statistics (NCES), 2013…
- 71.9% reported being cyberbullied once or twice in the school year
- 19.6% reported once or twice a month
- 5.3% reported once or twice a week
- 3.1% reported almost everyday
- 3.6% of students reported being cyberbullied with hurtful information on the internet
- 25% of teens on social media reported having an experience resulting in a face-to-face confrontation with someone
- 13% reported concern about going to school the next day
- 11% received a message from another student intended to hurt their feelings
- 8% reported having physical altercations with someone because of something that occurred on a social network site

Protect Identity

- According to Pew Internet & American Life Project, 2013, students younger than 14 yrs old…

- 91% post a photo of themselves
- 71% post their school name
- 71% post the city of town where the live
- 53% post their email address
- 20% post their cell phone number (I would venture to guess this is much higher)

- Students 14-17 yrs old…
- 94% post a photo of themselves
- 76% post their school name
- 66% their relationship status
- 23% their cell phone number (Again, I would also think this number is much higher)

- 16% of teen social media users have set up their profile to automatically include their location
- 26% of teen social media posts include false info (ie fake names, age, or location).
- 44% of youth have lied about their age to gain access to restricted websites
- 95% of all teens ages 12-17 are now online

Legal Ramification of Sexting

- What is Sexting – the sending of sexually explicit digital images, videos, text messages, or emails, usually by cell phone.

- First and foremost, sexual images (sexting) of minors is illegal everywhere, even if these pictures were taken by a minor. Secondly, in many jurisdictions, it is illegal for a minor to distribute these images, even if they are the one in the image.

- There have been cases in which minors have been charged with possession and/or distribution of child pornography after sharing and receiving pictures with other minors. This is a serious charge and can have lifelong ramifications they certainly won't want following them through their lives and professional careers. As a reminder, children don't realize the consequences of their actions. Not only may the consequences be dealt with right away, but these consequences can be dealt with for their entire lives (school, professional, personal).

Texting Abbreviations, Acronyms and other lingo

8 - Oral Sex
9 - Parent is Watching
99 - Parent no longer watching
143 - I love you
182 - I hate you
459 - I love you
831 - I love you
1174 - Nude club
420 - Marijuana
4Q - F*** you
ADR - Address
AITR - Adult in the room
ASL - Age/Sex/Location
Banana - Penis
BJ - Blow job
BOB - Battery operated boyfriend
CBF - Can't be f***ed
CBJ - Covered blow job
CYT - See you tomorrow
DURS - Damn you're sexy
DUM - Do you masterbate
DUSL - Do you scream loud
F2F - Face to Face
FAH - F***ing a hottie
FB - F*** buddy
FBI - Female body inspector
FILF - Father I'd like to F***
FMLTWIA - F*** me like the whore I am
FMUTA - F*** me in the a**
FO - F*** off
FOL - Fond of leather

Texting Abbreviations, Acronyms and other lingo continued

FWB - Friends with benefits
GAP - Got a pic
GNOC - Get naked on cam
GYPO - Get your pants off
1&1 - Intercourse and inebriation
F-1B - In the front of in the back
IIT - Is it tight?
ILF/MD - I love female/male dominance
IMEZRU - I am easy, are you?
IWSN - I want sex now
ILU - I love you
IPN - I'm posting nude
ITS - Intense text sex
JAFO - Just another F***ing onlooker
J/O - Jerking off
JEOMK - Just ejaculated on my keyboard
KFY or K4Y - Kiss for you
Kitty - Vagina
KPC - Keeping parents clueless
KWSTA - Kiss with serious tongue action
LB?W/C - Like bondage? Whips & Chains?
LF - Let's F***
LHOS - Let's have online sex
LKITR - Little kid in the room
LMIRL - Let's meet in real life
LY* or LU* - forms of I love you
M4C - Meet for coffee
M or F - Male or Female
MOOS - Member of the opposite sex
MILF - Mother I'd like to F***
MIRL - Meet in real life
MPFB - My personal F*** buddy

Texting Abbreviations, Acronyms and other lingo continued

MSNUW - Miniskirt or no underwear
MA - Mature audience
NIFOC - Nude in front of computer
NSFW - Not safe for work
OLL - Online love
PAL - Parents are listening
PAW - Parents are watching
PIR - Parent in room
PBB - Parent behind back
PLOS - Parents looking over shoulder
POM - Parent over my shoulder
POS - Parent over shoulder/Piece of S***
PRW - Parents are watching
PRON - Porn
Q2C - Quick to cum
RU/18 - Are you over 18
RYO - Roll your own
S2R - Send to receive (photo)
S or G - Straight or gay
STM - Spank the monkey
TAW - Teachers are watching
TTA - Tap the A**
WYFM - Would you F*** me?
WYRN - Will you call me?
WUF - Where you from?
XTC - Ecstasy

So now what?

- Parents…you MUST check your child's phone, emails, contacts, text messages, social media accounts. Have the sometimes uncomfortable conversation with your child about what's on their phone
- Turn off GPS monitoring/permission to use location services on social media
- Parental controls on child's phone, social media, app downloads, etc
- Install monitoring apps such as Bark, Dinner Time, Mobicip Parental Controls, Kidslox, WebWatcher, Google Family Link, Porn Blocker Plus, etc.
- Subscribe to web pages such as SmartSocial.com (I personally recommend this particular site. They provide a free webinar and will email updates to help you as the parent stay informed with the latest and greatest threats to our children's safety).