Apps

With the explosion of the tech industry and the dramatic increase in internet availability around the world over the past few decades, "apps" have become rather ubiquitous. "Apps" (or applications), are essentially computer programs that are typically found on smartphones.[1]

We have apps that tell us what the weather is like anywhere in the world, apps that allow us to hitch a ride from a driver, apps that allow us to listen to our favorite music or watch our favorite shows, and apps that enable us to video chat with loved ones thousands of miles away. Most people can agree that apps have done a lot of wonderful things for our society. But, as with all technology, they possess the potential for danger.

Here are a few of the types of apps we have seen used by predators to attempt to groom and traffick vulnerable youth:

Microblogging Apps

HOW THEY WORK:

Microblogging apps are broadcast media that provide short and frequent posts. In comparison with traditional blogging, where longer, in-depth posts are released weekly or monthly, microblogging posts are more themed around "what I am doing right now" – also known as a "status update."

These are platforms on which users create a profile, bio, and, sometimes, a miniature empire online. These pages are frequently used as social media forums where users connect with friends. For platforms that use a central server (e.g. Twitter), all posts go through that server before posting. Posting photos and videos, instant messaging, group messaging, and building an individual profile are all features common to these apps.

Other microblogging apps focus more on visuals. Tumblr is an example of a microblogging site in which reposting, or "reblogging," is the main source of content. A user's "dashboard" is an updated page of recent posts from people or tags he/she follows. Due to the nature of these sites, posts are frequently very art-based. Signing up for a Tumblr page gives you the opportunity to create an aesthetic board specific to you. There are a larger number of photos, text posts, and graphics shared/reblogged; therefore users can choose the ambiance they want their page to exude.

Microblogging sites with an emphasis on visuals and creativity (i.e. Tumblr) are different from microblogging sites where the main source of sharing is text-based and socially motivated posts (i.e. Facebook, Twitter).

POTENTIAL RISKS:

Privacy is a major issue in the use of apps since users may inadvertently broadcast sensitive, personal information to anyone who views their public feed. Due to the short, casual nature of these frequent posts, private information can be shared without a second thought. Sites that use central servers can be hacked, and the original location of the post or tweet can be traced, putting that user at risk of being located. Though that requires that the hacker have a special skill set, it is not particularly uncommon.

Risks more specific to visual microblogging apps include the visual emphasis of the site. It is easier to target insecure teens based on the info on their pages, teens who are in search of a relationship, or teens who may be having a hard time at home, since these "visually oriented" sites are meant to provide a representation of their feelings. A number of visual microblogging sites are known to host a plethora of pornographic images. Larger sites have banned porn (Tumblr), but users indicate ban enforcement has been spotty. Tumblr has become known for its NSFW (not safe for work, or explicit) content; in recent years, however, enforcing this ban (since that content was a large part of Tumblr's appeal) caused Tumblr to lose 30% of its web traffic in only two months.

Examples: **Facebook, Twitter, Tumblr, DeviantArt**

Photo and Video Sharing Apps

HOW THEY WORK:

These apps tend to center around the activity of snapping, editing, and posting photos and videos, which can be seen (and sometimes "liked") by users' friends or by the public (depending on their privacy settings).

Depending on which app is being used, these photos can remain available to view by the user's "followers" or the general public as long as the user does not delete them.

To find people with similar interests, users often place hashtags (such as "#horses") in the caption of their posted photo; this makes their photo searchable to other users with similar interests.

In some of these apps, users may "tag" the location in which they took the photo or video, which is often attached in an in-app map.

Image-sharing apps also usually have a "story" feature, which compiles posted photos or videos that can be viewed up to 24 hours after they're shared.

To communicate with others, users can either comment on someone's photo or send a private message using a direct message feature — sometimes both, depending on the app.

POTENTIAL RISKS:

What makes these apps dangerous is the trust that teens tend to put in the audience to whom they believe their information is being shown.

Traffickers can use these apps to glean information about a teen, which they can then use to relate to that teen in the grooming process.

For instance, a trafficker can learn where a teen likes to hang out, who their friends are, what their interests are, where they live, and more — all by viewing their pictures.

Unfortunately, teens can also become vulnerable to traffickers by over-sharing about their personal struggles or issues, especially if they use hashtags to express themselves.

For instance, traffickers can search #depressed or #sexy to find teens with vulnerabilities, and then reach out to them via direct message with sympathy or advice.

On some of these apps, images posted on stories seem to disappear after 24 hours, which gives teens a false sense of safety. Teens may then post more risky photos or opinions thinking they will disappear. Unfortunately, users can screenshot anything, and the app can also save any image posted — so in reality, the photo or video can potentially be available for much longer than 24 hours.

Examples: **Instagram, Facebook, Snapchat, TikTok**

WIFI-Based Messaging Apps

HOW THEY WORK:

These apps allow their users to "text" one another using WiFi instead of cellular data, enabling users to message any other user, regardless of geographical location, without additional fees and, sometimes, without the need to even exchange phone numbers, thus maintaining whatever level of anonymity the user desires.

Although originally designed for private individual and group messaging, most WiFi-based instant-messaging apps also have a public groups feature, comprised of public, themed "chat rooms." Users who interact with one another in public groups can typically send private messages to individual users, where they can chat via text or video message and send pictures, videos, and GIFs (animated pictures).

POTENTIAL RISKS:

This type of app is used by traffickers who target themed chat rooms in order to identify and meet teens who are vulnerable to trafficking.

Once a trafficker identifies an at-risk teen, it's easy to begin the grooming process, gleaning information about the teen's vulnerabilities, sending and receiving explicit pictures, etc.

These apps have also been used to buy, share, and trade images of child sexual exploitation (or ICSE, formerly known as "child pornography").[2]

Traffickers tend to gravitate toward communicating with their victims through WiFi-based messaging apps (rather than through traditional texting) due to these apps' anonymous nature, which makes it harder for law enforcement to track them — and which makes teens more comfortable with sharing personal information.

In addition, traffickers prefer this method of communication because it can be accessed on any device with WiFi connectivity, including tablets, laptops, even deactivated and "burner" cell phones.

Examples: **Kik, WhatsApp, Facebook Messenger, WeChat, Viber, GroupMe**

Dating Apps

HOW THEY WORK:

Although each dating app will advertise its own niche or way of operating, they all tend to work in a very similar manner: They allow users to review strangers' dating profiles, which tend to consist mostly of pictures, along with some basic information about their general location, age, height, education, occupation, etc.

Although some apps operate on a "like" or "dislike" basis, more and more apps are switching over to a swiping method, in which users swipe their device screen to the right if they're interested in getting to know the user whose profile they're viewing, and swipe left if they're not interested.

If two users have swiped right on or "liked" each other's profiles, they're matched and given the opportunity to chat with one another via a private messaging feature.

Although most dating apps are created for users 18 and older, age requirements are easy to bypass by simply entering the incorrect age when creating a profile.

POTENTIAL RISKS:

Even though these apps were originally designed for (and are still used for) finding a serious romantic partner, they have also become known to many as "hookup" apps.

Perhaps because of the appearance-based nature of the matching process, teens and adults have been known to use this type of app to find a casual sexual partner, or "friend with benefits."

Along with shaping modern dating culture as one where it is normal to "hook up" (or have sexual relations with a stranger), these dating apps are also a place where traffickers can find teens in search of love and/or physical affection.

Examples: **Yubo, Tinder, Bumble, Hinge, Tagged, Grindr, Plenty of Fish (or POF), Coffee Meets Bagel, Badoo, SKOUT, MeetMe**

Vault Apps

HOW THEY WORK:

These apps are designed to act as a secret virtual vault for media such as photos, notes, files, contacts, passwords, and internet browsing.

However, Vault apps often appear to have a different purpose than they actually do. For instance, many appear and function as a calculator, yet they're set up so that if a certain predetermined code is typed into the calculator keypad, the "vault" unlocks and the secret contents become accessible.

Even though users often must pay a small fee to use all of these features in an unlimited capacity, these apps typically have a free version where users may still store some photos, notes, contacts, etc.

POTENTIAL RISKS:

Although vault apps are not used to recruit teens into being trafficked, these apps still frequently appear in trafficking cases. When traffickers are first grooming a teen online, they often encourage the youth to get a vault app so their correspondence — the sexual images (photos and videos) they might have exchanged, and the pornography that they have been sent — can be kept secret from anyone who might access their phone.

Examples: **Fake Calculator, Calculator+, Secret Photo Vault, Private Photo Vault**

PLEASE REMEMBER:

1.These apps are not intrinsically bad. There are a lot of positive, fun reasons for youth to have most of these apps (with the exception of the dating and perhaps vault apps). Just because your children use these apps does not mean they are being groomed by a trafficker.

2.This is not an exhaustive list of the types of apps traffickers may use to groom and recruit youth. Users, both young and old, should use extreme caution while using any online or social networking app, as traffickers could use even the most innocent ones in a predatory manner.

3.For more information on potentially dangerous apps, you can find our "Apps to Watch For" research and resource at sharedhope.org/internetsafety.

1"WebWise – What Are Apps?" *BBC*, BBC, www.bbc.co.uk/webwise/guides/what-are-apps

2Fox-Brewster, Thomas. "This $1 Billion App Can't 'Kik' Its Huge Child Exploitation Problem." *Forbes*, Forbes Magazine, 3 Aug. 2017, www.forbes.com/sites/thomasbrewster/2017/08/03/kik-has-a-massive-child-abuse-problem/#53f0fc31a142