Risk factors for online grooming: Implications for prevention

Associate Professor Michael Salter
michael.salter@westernsydney.edu.au
Online grooming

“Grooming” describes offenders’ actions during the preparatory stages of sexual abuse (McAlindien, 2006), often involving:

- **Gaining the trust of the child**, and sometimes of the child’s caregivers and others around the child,
- **Gaining the compliance of the child** by establishing an emotional connection, manipulation and/or threat and blackmail,
- **Gaining the child’s secrecy**, through victim-blaming, telling the child they won’t be believed or that the offender will get in trouble.

Pre-abuse interactions between sexually abusive adults and children can be quite subtle with shifts in offender motivations and behaviours; ‘grooming’ may be a recurring theme rather than the offender’s sole focus (Kloess et al. 2014).

The prevalence of online grooming of children is unclear but sexual solicitation has been a common feature of minor’s online experiences since the advent of the internet.

Recent Spanish study: 15.6% of girls and 9.3% of boys aged 12 - 15 reported online sexual solicitations from adults (De Santisteban & Gámez-Guadix, 2018).
History of online grooming

Chat rooms in the 1990s were infamous for persistent sexual solicitation of users and minors in particular.

The threat was limited in 1990s and early 2000s due to lack of geographic proximity and limited information exchange between users.

From the mid-2000s, social media platforms encouraged interaction between known users in physical proximity, facilitating online grooming with the intent of contact offending.

With the advent of the smart phone and cheap, high speed internet, online grooming includes coercing minors into images, video and live-stream.

Increased use of social media apps with limited privacy/safety features by pre-teens is lowering the age range of those at risk of online grooming.
Online grooming example - August 2017, USA

Today we went through something that I feel needs to be shared. Our daughter has an app that she has been using with some friends and family members that went from fun, to making me furious. The name of this app is called musical.ly.

First I want to say how proud of our daughter I am and want this to be a warning to your families. Instead of saying the words, let me show you; see below...

Please, tell your kids to let you know if anyone ever asks something like this, let them know it’s okay to tell you. It has helped us in this situation.

If you’re wondering if we called the police, yes and they have the phone to pull all of the information to track this person down.

Please feel free to share if you think it can help others....

I know many will blame us parents for this happening. But we never thought like predators and I guess we were naive in thinking that our daughter was safe on what we thought to be a kid friendly app. We have learned the hard way. I ask that you not judge us (many still will) but let our experience teach us all.

Update: The detective has found the IP address of this person and has submitted a supeona to this app to freeze all records pertaining to this person (s). They are continuing to make progress!

To the people who wonder why a 7 year old has access to this;

Our daughter does not have a phone of her own. This app was on one of our phones for use when we were around. She used this app to connect with her cousins and make goofy duets of songs together. We have accepted friends of theirs and our daughter believed this was another one. I never thought of someone pretending to be 9 to gain access to my child. We live and learn and I continue to do so everyday as a parent.

This post is meant as a warning call to others that let their children use this app. This post wasn't meant for people telling me how to raise my child. My child came and told me and it didn't get any further luckily. She followed what I taught her. I'm sure that others families aren't so lucky. The world we live in needs focus on these types of things, say what you will.
Jessy and you are friends now.

Hi

How are you

I'm fine

Good how are you

How old are you

7 how old are you

Send a chat...

How old are you

Cool

Send me your photos

OK

Make some pics without t-shirt

I like to see your body without t-shirt

I can't

You can

Make some new pics in bathroom

Send a chat...
without clothes

My mom said I can't

don't tell to anyone

it's secret between us only

Lol

make some pics without t-shirt now

madi

Hi

send a chat...

it's secret between us only

Lol

make some pics without t-shirt now

madi

Hi

i am her father and i am a police officer. we have documented your ip address and location. i recommend that you refrain from any other contact.

send a chat...
Factors that increase a child’s risk of online grooming

Youth is a general risk factor for sexual exploitation, with adolescents most at risk.

Girls are at greater risk of online grooming than boys, and same-sex attracted boys are at greater risk than other boys.

**Behavioural risks:** Being online more often, and taking more risks online (e.g. conversing online with strangers about sex, public posting of revealing images).

**Biographical risks:** Online risk taking predicted by prior history of trauma, violence and abuse, and unmet needs (including those related to sex and sexuality). Children with a disability at heightened risk.

**Situational risks:**
- Family neglect, dysfunction, lack of parental involvement or supervision
- Friends engaged in online risk
- Peer alienation and victimisation
- Lack of sexual education.

**Psychological risks:** Low self-esteem, low self-confidence, mental illness (esp depression).

Key messages about victim risk factors

We can’t assume that minors are at risk because they don’t know about online risks; it is older and more experienced teenagers who engage in the most online risk taking.

Minors who are ‘at risk’ offline are also ‘at risk’ online.

Previous ‘offline’ abuse is a risk factor for ‘online’ abuse.

Traumatised or abused children are riskier and ‘needier’ online, and more likely to:
• seek out social contact and emotional reassurance online,
• meet ‘online’ friends in real life.

Children with needs that may be manipulated by offenders include those who are:
• same-sex attracted
• living with a disability
• living with a mental illness.

Risk factors ‘cluster’ and online grooming is likely to be part of a larger picture of abuse and disadvantage in a young person’s life. Media representations of appalled protective parents contacting police about online child grooming reflect a reporting bias.
Victim perspectives of being groomed online

Technological factors that enable online grooming

Design

- Posting is public by default
- Platforms facilitate direct public or private contact from strangers
- Visible ‘metrics’ of interest/engagement (likes, hearts, friends) that reward personal or sexualized exposure (personal information, revealing photos)
- No attempt to verify user identity (e.g. phone number) and provision of untraceable services
- Cultures of explicit sexual talk/innuendo and imagery, including poor security enabling ‘porn’ spam/bots
- Facilitation of CEM exchange

Administration

- Platforms that privilege user privacy above child safety
- Lack of investment in proactive content moderation
- Insufficient enforcement of age provisions and no mechanism to do so
- Platforms that devolve child safety to parents and parental supervision
- Terms of service that do not explicitly state that using the app for the purposes of child sexual exploitation is a breach of service and will result in the provision of data to law enforcement
Key messages about technological risk factors

The Web 2.0 business model is based on incentivizing interaction between as many users as possible through the self-generation and circulation of attention-grabbing content.

Core child safety measures are contrary to the business model:
• restricting user access and age, limiting circulation of content and robust content moderation is expensive
• while maximising user exposure maximises profit.

Profit maximisation and cost minimisation are the common themes that run through the design and administrative factors that place children at risk.

The commercial reasons why platforms do not prioritise child safety are often obscured by appeals to ‘parental responsibility’ or to the ‘open web’, which are frequently championed in the media and by industry lobbyists.
Kik chat app 'involved in 1,100 child abuse cases'

By Angus Crawford
BBC News

21 September 2018

'A brick wall'

Constable Jason Cullum from Northamptonshire Police's paedophile online investigation team told the BBC delays due to the "bureaucratic nightmare" of obtaining information from the company put children at further risk.

He is investigating a complex grooming case involving more than 90 profiles - some suspected offenders, others child victims - but he needs information from Kik to identify and trace them.

Police officers contacting Kik are given an automated response and directed via a complex legal process - under the Mutual Legal Assistance Treaty (MLAT) - to gain a court order.

"It's incredibly frustrating. We're banging our heads against a brick wall," said PC Cullum.

"There's a child that's going to be abused for probably another 12 months before we know who that is."

Canada and the US have strict rules on releasing personal information to law enforcement agencies to protect individuals' privacy.

Kik says it will release some information if there is an "imminent threat of death or serious physical injury to any person".

In these cases, the app will release "limited basic subscriber data".
Implications for prevention

Educating children about online risks is necessary but not sufficiently protective. Young people with the most information and experience are taking the most risks.

Parental supervision is important but not a ‘magic bullet’:
• it can become overbearing and a breach of trust
• the most ‘at risk’ children do not have protective parents.

To prevent online grooming, we should be attentive to young people’s:
• individual vulnerabilities (prior trauma, mental illness, disability)
• situational risks (family dysfunction, peer harassment)
• unmet needs (lonely, low self-esteem, sexual development).

‘Safety by design’ principles are crucial to providing safe online environments for children, particularly as apps are marketed to an increasingly young audience.

The limited gains of industry self-regulation suggests that platforms should be subject to legislative requirements in terms of safety and cooperation with law enforcement.
References


Thank you!

michael.salter@westernsydney.edu.au