Microsoft

Combating Child Grooming Online

Key Points

Grooming is the process by which predators manipulate children for purposes such as sexual exploitation or recruitment into extremist or terrorist organizations. Online grooming is when perpetrators use the internet to make contact and develop relationships with children and young people for these purposes.

The Microsoft approach to combating child predation includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and collaborating with government, industry, non-governmental organizations, and others.

Microsoft strongly supports enacting and enforcing laws against the exploitation of children and cooperates with law enforcement to bring internet predators to justice.

Child grooming is a process of emotional manipulation by which predators prepare children and youth for sexual or other exploitation.

The grooming process typically involves an adult befriending a young person and then winning trust by showering the youth with flattery, sympathy, gifts of money or modeling jobs, and other personal attention. The groomer then tries to deepen the relationship, seeking to control the child and continue the abuse, which may include images of child sexual abuse, sex trafficking, recruitment to terrorist causes, or radicalization to violence.

Predators go where children go, and today that includes the internet. Child grooming goes online when predators use the internet for the grooming process. Adults may begin the grooming process by visiting forums where youth interact, such as online games (which may use two-way voice and video technology) or chat rooms, or they may contact children through text messages. Predators use the information that children reveal about themselves online to target vulnerable youngsters with low self-esteem, family or social issues, or lack of resources.

The online exploitation of children for sexual and other purposes is a global problem, and internet companies have a role to play in helping to stop perpetrators. However, it is important to keep the online portion of the problem in perspective. According to the Crimes Against Children Research Center in the United States, the arrest of more than 600 online predators in 2006 constituted about one percent of all arrests for sex crimes committed against children and youth.

Microsoft Approach

The Microsoft approach to combating child grooming online includes developing technology, providing guidance, establishing internal policies, and working with others.

Creating Technology Tools

Microsoft builds safety features into a wide range of its products and services to help parents watch over their children online. For example, the latest versions of Windows offer tools to help parents monitor their children's online activities. Anyone—adult or young person—with a Microsoft account can specify who can view their profiles or contact them. In addition, Xbox Live has Online Safety and Privacy Settings that enable parents to restrict who children can communicate with and who can see their profiles or friends lists.

In 2009, Microsoft Research collaborated with Dartmouth College and NCMEC to develop an advanced technology called PhotoDNA, which helps to refine and automate the search for known child sex abuse images among the billions of photos on the internet. NCMEC used the PhotoDNA license to work with online services such as Facebook to uncover images of child abuse.

Since then, it has become the industry standard for detecting such images.

A few years later, Microsoft launched PhotoDNA Cloud Service for qualified enterprise customers to deploy and detect illegal images on their services.

In 2020, Microsoft teamed up with The Meet Group, Roblox, Kik, and Thorn to develop **a grooming detection technique** that helps identify potential instances of child online grooming for sexual purposes. This technique builds off Microsoft patented technology and is now freely available via **Thorn**—a technology and child protection nonprofit—to qualified online service companies that offer a chat function.

Providing Education and Guidance

The Microsoft Online Safety website and resources page, located at **www.microsoft.com/saferonline,** provide a range of brochures, factsheets, presentation decks and other materials on a variety of online safety topics. A recent addition is a factsheet for parents and teachers about the risks of online grooming for both sexual purposes and terrorism recruiting.

In 2016, Microsoft began research—that continues today—into digital civility: encouraging safer, healthier, and more respectful online interactions among all people. Over the years, Microsoft has polled teens and adults in more than 30 countries about their exposure to 21 online risks, including sextortion and terrorist recruiting. Individual country and global results are available at **www.microsoft.com/digitalcivility**.

Collaborating with Others

Microsoft collaborates with government, industry counterparts, and others around the world. Microsoft is an active member representing the tech industry on the international advisory board of the WePROTECT Global Alliance—a multistakeholder group of nearly 100 countries, 28 technology companies, 30 civil society organizations, and international bodies like INTEROPOL and UNICEF—committed to ending the online distribution of child sexual exploitation and abuse imagery.

Microsoft supports INHOPE, the international association of hotlines and helplines, as well as the victim-services organization, the Marie Collins Foundation (MCF). Microsoft holds a seat on INHOPE's international advisory council and on MCF's strategic advisory board.

Microsoft is a long-standing member of the industry-led Technology Coalition; supports the non-profit Thorn and its Innovation Lab, and is a member of the Child Dignity Alliance's Technical Working Group.

All groups are doing their part to eliminate child sexual exploitation and abuse imagery from the open web.

To help combat online grooming for recruitment to extremist organizations, Microsoft is a founding member of the Global Internet Forum to Counter Terrorism, along with Facebook, Twitter and YouTube. The GIFCT focuses on removing harmful terrorist content from online services and championing counter- and alternative-narratives to extremist propaganda.

Policy Considerations

Policymakers can help address the challenges of combating child exploitation online by supporting the following efforts:

Support Victim Recovery Services

Funding and infrastructure for effective victim recovery services is absolutely essential. Without this, any other interventions have the potential to do more harm than good.

Support Industry-Wide Best Practices and Guidance

Internet companies must continue to work with governments and law enforcement to help address the problem of online predators by establishing industry best practices and guidance. More emphasis must be placed on enabling companies to voluntarily find and report images of child sexual abuse. Policymakers can help change the focus of law enforcement to a model that measures their activities to stop crime and prevent abuse without penalizing the victim.

Enact Laws that Protect Victims of Child Sexual Exploitation

It is vital that governments enact and enforce:

- Child sexual exploitation laws that recognize and protect victims while holding offenders and traffickers accountable.
- Laws against the possession, production, and distribution of child sexual abuse images worldwide. In 2018, the International Centre for Missing and Exploited Children (ICMEC) reported that 118 countries have enacted laws that are "sufficient" to combat child sexual exploitation and abuse imagery. However, 16 countries still have no laws at all.