Child Abusers Run Rampant as Tech Companies Look the Other Way

Though platforms bar child sexual abuse imagery on the web, criminals are exploiting gaps. Victims are caught in a living nightmare, confronting images again and again.

By MICHAEL H. KELLER and GABRIEL J.X. DANCE NOV. 9, 2019

The two sisters live in fear of being recognized. One grew out her bangs and took to wearing hoodies. The other dyed her hair black. Both avoid looking the way they did as children.

Ten years ago, their father did the unthinkable: He posted explicit photos and videos on the internet of them, just 7 and 11 at the time. Many captured violent assaults in their Midwestern home, including him and another man drugging and raping the 7-year-old.

The men are now in prison, but in a cruel consequence of the digital era, their crimes are finding new audiences. The two sisters are among the first generation of child sexual abuse victims whose anguish has been preserved on the internet, seemingly forever.

This year alone, photos and videos of the sisters were found in over 130 child sexual abuse investigations involving mobile phones, computers and cloud storage accounts.

The digital trail of abuse — often stored on Google Drive, Dropbox and Microsoft OneDrive — haunts the sisters relentlessly, they say, as does the fear of a predator recognizing them from the images.

“That’s in my head all the time — knowing those pictures are out there,” said E., the older sister, who is being identified only by her first initial to

protect her privacy. “Because of the way the internet works, that’s not something that’s going to go away.”

[Read an interview with the two sisters.]

Horrific experiences like theirs are being recirculated across the internet because search engines, social networks and cloud storage are rife with opportunities for criminals to exploit.

The scope of the problem is only starting to be understood because the tech industry has been more diligent in recent years in identifying online child sexual abuse material, with a record 45 million photos and videos flagged last year.

But the same industry has consistently failed to take aggressive steps to shut it down, an investigation by The New York Times found. Approaches by tech companies are inconsistent, largely unilateral and pursued in secret, often leaving pedophiles and other criminals who traffic in the material with the upper hand.

The companies have the technical tools to stop the recirculation of abuse imagery by matching newly detected images against databases of the material. Yet the industry does not take full advantage of the tools.

Amazon, whose cloud storage services handle millions of uploads and downloads every second, does not even look for the imagery. Apple does not scan its cloud storage, according to federal authorities, and encrypts its messaging app, making detection virtually impossible. Dropbox, Google and Microsoft’s consumer products scan for illegal images, but only when someone shares them, not when they are uploaded.

And other companies, including Snapchat and Yahoo, look for photos but not videos, even though illicit video content has been exploding for years. (When asked about its video scanning, a Dropbox spokeswoman in July said it was not a “top priority.” On Thursday, the company said it had begun scanning some videos last month.)

The largest social network in the world, Facebook, thoroughly scans its platforms, accounting for over 90 percent of the imagery flagged by tech companies last year, but the company is not using all available databases to detect the material. And Facebook has announced that the main source

of the imagery, Facebook Messenger, will eventually be encrypted, vastly limiting detection.

“Each company is coming up with their own balance of privacy versus safety, and they don’t want to do so in public,” said Alex Stamos, who served as chief of information security at both Facebook and Yahoo. “These decisions actually have a humongous impact on children’s safety.”

Tech companies are far more likely to review photos and videos and other files on their platforms for facial recognition, malware detection and copyright enforcement. But some businesses say looking for abuse content is different because it can raise significant privacy concerns.

Tech companies are loath to be seen going through someone’s photos and videos, and imagery flagged in automated scans is almost always reviewed by a person later.

“On the one hand, there is an important imperative to protect personal information,” said Sujit Raman, an associate deputy attorney general in the Justice Department. “On the other hand, there is so much stuff on the internet that is very damaging.”

The main method for detecting the illegal imagery was created in 2009 by Microsoft and Hany Farid, now a professor at the University of California, Berkeley. The software, known as PhotoDNA, can use computers to recognize photos, even altered ones, and compare them against databases of known illegal images. Almost none of the photos and videos detected last year would have been caught without systems like PhotoDNA.

But this technique is limited because no single authoritative list of known illegal material exists, allowing countless images to slip through the cracks. The most commonly used database is kept by a federally designated clearinghouse, which compiles digital fingerprints of images reported by American tech companies. Other organizations around the world maintain their own.

Even if there were a single list, however, it would not solve the problems of newly created imagery flooding the internet, or the surge in live-streaming abuse.

For victims like E. and her sister, the trauma of the constantly recirculating photos and videos can have devastating effects. Their mother said both sisters had been hospitalized for suicidal thoughts.

“Every hope and dream that I worked towards raising my children — completely gone,” she said. “When you’re dealing with that, you’re not worried about what somebody got on a college-entrance exam. You just want to make sure they can survive high school, or survive the day.”

And because online offenders are known to seek out abused children, even into adulthood, the sisters do not speak publicly about the crimes against them. Their emotional conversations with The Times were the first time they’ve spoken publicly about the abuse.

“You get your voice taken away,” E. said. “Because of those images, I don’t get to talk as myself. It’s just like, Jane Doe.”

Searching for Abuse

Joshua Gonzalez, a computer technician in Texas, was arrested this year with over 400 images of child sexual abuse on his computer, including some of E. and her sister.

Mr. Gonzalez told the authorities that he had used Microsoft’s search engine, Bing, to find some of the illegal photos and videos, according to court documents.

Microsoft had long been at the forefront of combating abuse imagery, even creating the PhotoDNA detection tool a decade ago. But many criminals have turned to Bing as a reliable tool of their own.

A report in January commissioned by TechCrunch found explicit images of children on Bing using search terms like “porn kids.” In response to the report, Microsoft said it would ban results using that term and similar ones.

The Times created a computer program that scoured Bing and other search engines. The automated script repeatedly found images — dozens in all — that Microsoft’s own PhotoDNA service flagged as known illicit

content. Bing even recommended other search terms when a known child abuse website was entered into the search box.

While The Times did not view the images, they were reported to the National Center for Missing and Exploited Children and the Canadian Center for Child Protection, which work to combat online child sexual abuse.

One of the images, the Canadian center said, showed a naked girl on her back spreading her legs “in an extreme manner.” The girl, about 13, was recognized by the center’s analysts, who regularly review thousands of explicit images to help identify and rescue exploited children and scrub footage from the internet. The analysts said the authorities had already removed the girl from danger.

Similar searches by The Times on DuckDuckGo and Yahoo, which use Bing results, also returned known abuse imagery. In all, The Times found 75 images of abuse material across the three search engines before stopping the computer program.

Both DuckDuckGo and Yahoo said they relied on Microsoft to filter out illegal content.

After reviewing The Times’s findings, Microsoft said it uncovered a flaw in its scanning practices and was re-examining its search results. But subsequent runs of the program found even more.

A spokesman for Microsoft described the problem as a “moving target.”

“Since the NYT brought this matter to our attention, we have found and fixed some issues in our algorithms to detect unlawful images,” the spokesman said.

Hemanshu Nigam, who served as a director overseeing child safety at Microsoft from 2000 to 2006, called the findings a “major failing,” and added that “it looks like they’re not using their own tools.” Mr. Nigam said it showed the company was seemingly unaware of how its platforms could be manipulated by criminals.

Child abusers are well aware of Bing’s vulnerabilities, according to court records and interviews with law enforcement officials. Going back years,

pedophiles have used Bing to find illegal imagery and have also deployed the site's "reverse image search" feature, which retrieves pictures based on a sample photo.

The same computer program, when run by The Times on Google's search engine, did not return abuse content. But separate documentation provided by the Canadian center showed that images of child sexual abuse had also been found on Google and that the company had sometimes resisted removing them.

One image captured the midsections of two children, believed to be under 12, forced into explicit acts with each other. It is part of a known series of photos showing the children being sexually exploited.

The Canadian center asked Google to take down the image in August last year, but Google said it did not meet its threshold for removal, the documents show. The analysts pressed for nine months until Google relented.

Another image, found in September 2018, depicts a woman touching the genitals of a naked 2-year-old girl. Google declined to take down the photo, stating in an email to the Canadian analysts that while it amounted to pedophilia, "it's not illegal in the United States."

When The Times later asked Google about the image and others identified by the Canadians, a spokesman acknowledged that they should have been removed, and they subsequently were. The spokesman also said that the company did not believe any form of pedophilia was legal, and that it had been a mistake to suggest otherwise.

A week after the images were removed, the Canadian center reported two additional images to Google. One was of a young girl, approximately 7, with semen covering her face. The other was of a girl, between 8 and 11, with her legs spread, exposing her genitals. Google told the Canadian center that neither image met "the reporting threshold," but later agreed to remove them.

"It baffles us," said Lianna McDonald, the center's executive director.

Criminals Everywhere

The problem is not confined to search engines.

Pedophiles often leverage multiple technologies and platforms, meeting on chat apps and sharing images on cloud storage, according to a review of hundreds of criminal prosecutions.

[Read a report on the emerging psychology of pedophiles.]

"The first thing people need to understand is that any system that allows you to share photos and videos is absolutely infested with child sexual abuse," said Mr. Stamos, the former security chief at Facebook and Yahoo, who is now a professor at Stanford.

Criminals often discuss in online forums and chat groups how to exploit vulnerabilities in platforms, the criminal cases show. They carefully follow the prosecutions of people who have been found with explicit imagery and learn from them. There are even online manuals that explain in graphic detail how to produce the images and avoid getting caught.

The digital trail that has followed one young abuse victim, a girl who was raped by her father over four years starting at age 4, is sadly representative of the pattern.

The girl, now a teenager living on the West Coast, does not know that footage of her abuse is on the internet. Her mother and stepfather wish it would stay that way.

"We're just afraid of all the negative impacts that it might have — because I've spoken with other moms whose daughters know their images are online and they're train wrecks," her mother said. "She doesn't need to be worrying about most likely the worst part of her life available on the internet."

Her stepfather also worries. "To her, the internet is looking up puppies."

Sex offenders frequently share photos and videos of the girl's abuse on sites that appear on Bing and elsewhere. When the images are detected, the F.B.I. notifies the girl's family or their lawyer. Over the past four years, her family says, they have received over 350 notifications about

cases across the country, including in Florida, Kansas, Kentucky, Michigan, Minnesota and Texas.

Images of the girl surfaced in a case reported to the authorities by a woman who had been conversing with a Michigan man on Facebook Messenger.

The man had proposed that the woman and her children live as nudists, while also suggesting to her that incest was normal. He offered to move in with her along with his 13-year-old daughter, whom, he said, he had orally raped the night before.

The man, Snehal Yogeshkumar Shah, had also been communicating on Messenger with other abusers, who recommended he download the Kik messaging app and create a Dropbox account to store his illicit material. The police found more than 400 illegal photos and videos in his Dropbox account and on his iPhone, including some of the West Coast girl. They also found chats on Kik between him and two young teenagers containing explicit imagery. He is now in prison.

Images of the girl also emerged in an investigation into Anthony Quesinberry, an Army specialist in San Antonio who shared abuse content on Yik Yak, a now-shuttered social networking app. He told investigators that he'd been addicted to the imagery for years and had obtained it using search engines, Tumblr, Dropbox, Kik and the live-streaming video platform Omegle. He was sentenced to more than 16 years.

The girl's mother said she could see the effects of the trauma years later. Sometimes, her daughter becomes inexplicably angry. More often, she can seem detached, as if nothing bothers her. There "are things, developmentally, that she is just having to learn now," said her mother, who agreed to be interviewed with her lawyer and only if her name and location were withheld.

When the girl turns 18, she will become the legal recipient of reports about the material. At that point, her mother and stepfather hope, she will be better able to handle the news. They also hold out hope that the tech companies will have managed to remove the images from the internet by then.

“I would love to be able to tell her they were online,” her mother said, “but they are not anymore.”

‘Pictures Are Forever’

Other parents are resigned to the possibility that the images may remain online forever.

In a foster family with multiple victims, one teenage daughter recently went on antidepressants to cope with feelings that her abuse was her fault. Another daughter found the courage to begin dating eight years after her abuse. But when her worried brother recently went online to test whether the imagery was still available, agents from the F.B.I. visited their home. It is illegal to view child sexual abuse material, regardless of intentions.

“I don’t fool myself into thinking I’m doing great anymore,” said the foster mother, who requested anonymity to protect the privacy of her children. “I’m just surviving day by day.”

Two of her foster daughters were filmed being raped by their father, while others were abused but not photographed or filmed. The difference, she said, can be profound over time.

“They’re angry that those pictures are forever,” she said.

To discourage them from posting on social media and risk being recognized, she has told her children their abusive images live on the internet. “I don’t think they’ll ever be totally wiped out,” she said.

So far, the tech industry has proved her right.

It has been 10 years since PhotoDNA was developed at Microsoft, yet the industry’s efforts to detect and remove known illegal photos remains uneven and cloaked in secrecy.

The industry’s response to video content has been even more wanting, according to interviews, internal company emails and reviews of thousands of court records. There is no common standard for identifying illegal video content, and many major platforms — including AOL,

Snapchat and Yahoo — do not even scan for it. AOL and Yahoo did not respond to requests for comment about their video policies. A Snap spokesman said the company was working with industry partners to develop a solution.

A spokesman for Kik, before it was sold last month, said the company was also working on the issue; on Friday, the new owners said it now scanned for video.

“Over all, the tech companies are doing the minimal amount necessary to maintain public respect for their organizations,” said Chad M.S. Steel, who teaches computer forensics at George Mason University and has assisted federal investigators in abuse-related cases. “But they’re not doing nearly as much as they could based on the technologies available.”

Tech companies have known for years that videos of children being sexually abused are shared on their platforms, according to former employees at Microsoft, Twitter, Tumblr and other companies. One former Twitter employee described gigabytes of illegal videos appearing more quickly than they could be taken down on Vine, the video service since shuttered by Twitter.

That was in 2013, when fewer than 50,000 videos were reported. Last year, tech companies referred more than 22 million to the National Center for Missing and Exploited Children, the nonprofit clearinghouse mandated by the federal government to act as a repository for the imagery.

Efforts to tackle the urgent problem of video content have run into roadblocks of the companies’ own making. Google, for example, developed video-detection technology that it makes available to other companies, and Facebook also has a system. But the two cannot share information because the fingerprints generated by each technology are not compatible.

In 2017, the tech industry approved a process for sharing video fingerprints to make it easier for all companies to detect illicit material, according to confidential emails and other documents that were part of a project run by the Technology Coalition, a group focused on child safety issues that includes most major companies.

One document notes the project's justification: "Video has become as easy to create as images and no standard solution/process has been adopted by industry."

But the plan has gone nowhere.

The lack of action across the industry has allowed untold videos to remain on the internet. Of the center's 1.6 million fingerprints, less than three percent are for videos.

Photos and videos are each being handled in ways that give criminals great leeway. None of the largest cloud storage platforms — including Amazon Web Services, Dropbox, Google Drive and Microsoft's OneDrive and Azure — scan for abuse material when files are uploaded, according to law enforcement officials, former employees and public statements by the companies.

While the files may be scanned later, when users share them, for example, some criminals have avoided detection by sharing their account logins rather than the files themselves.

A Florida man, Gregory Householder, told investigators that he had used online platforms for eight years and had regularly shared logins to Dropbox accounts with other offenders. Mr. Householder said he knew he was committing a crime, but did not believe he would get caught.

A spokesman for Amazon, which does not scan for abuse imagery whatsoever, said that the "privacy of customer data is critical to earning our customers' trust," and noted that the company had a policy that prohibited illegal content. Microsoft Azure also said it did not scan for the material, citing similar reasons.

Privacy concerns were raised by other companies, including Dropbox and Google. A Dropbox spokeswoman said scanning raised a specter that privacy advocates could take issue with.

Some companies, like Dropbox and Google, invoked security concerns when asked about their detection and removal practices. A spokesman for Apple declined to specify how it scanned its platforms, saying the information could help criminals.

Several digital forensic experts and law enforcement officials said the companies were being disingenuous in invoking security. Mr. Stamos, the former Facebook and Yahoo security chief, said the companies just “don’t want to advertise that they are open for business” to criminals.

“If they’re saying, ‘It’s a security problem,’ they’re saying that they don’t do it,” Mr. Stamos said.

An Uncertain Future

A heinous case in Pennsylvania warns of a tsunami of new, hard-to-detect abuse content through live-streaming platforms.

More than a dozen men from around the world were logged in to the business conference software Zoom. They were chatting while watching a live stream that had nothing to do with work: A man was sexually assaulting a 6-year-old boy.

One of the viewers, according to court documents, asked the assailant to spread the boy’s buttocks. Another to “spit in his face.” A third to “rape him.”

The boy was orally raped and violently penetrated while some of the men, appearing on cameras of their own, cheered and masturbated for the others to see.

The men also broadcast prerecorded clips of young children — including infants — being raped, beaten and urinated on.

During the trial, an investigator said that offenders often knew that live streams are harder to detect and leave no record.

“That’s why they go to Zoom,” said the federal prosecutor in the case, Austin Berry, during his closing remarks. “It’s the Netflix of child pornography.” Prosecutions in other cases have involved live streaming on Apple’s FaceTime, Facebook, Omegle, Skype, YouNow and others.

None of the major tech companies is able to detect, much less stop, the live streaming through automated imagery analysis, although a technology

executive at Zoom said the company had made significant improvements since the Pennsylvania case using other methods.

And while Facebook, Google and Microsoft have said they are developing technologies that will find new photos and videos on their platforms, it could take years to reach the precision of fingerprint-based detection of known imagery, according to interviews.

Men in the Pennsylvania case were caught in 2015 only because Janelle Blackadar, a detective constable with the Toronto police, discovered the broadcast while conducting an undercover investigation. The detective recorded the stream using screen-capturing technology, and within hours alerted Special Agent Austin Berrier of Homeland Security Investigations.

The 6-year-old boy was rescued the next day, and 14 men from multiple states have since been sentenced to prison.

In January, the assailant, William Byers Augusta, 20, received a sentence of up to 90 years.

The Pennsylvania state prosecutor in the case, describing the offenders as monsters, said in court that Mr. Augusta had "encouraged people all over the world to tune in."

Produced by Rich Harris, Virginia Lozano, Adriana Ramić and Rumsey Taylor.

Related Coverage

- 'If Those Were Pictures of You, You Would Understand' NOV. 9, 2019
- The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? SEPT. 28, 2019
- Preying on Children: The Emerging Psychology of Pedophiles SEPT. 29, 2019

An Explosion in Online Child Sex Abuse: What You Need to Know SEPT. 29, 2019