TROUBLE IN TOYLAND 2023

Threats stem from toys with microphones, cameras and trackers, as well as recalled toys, water beads, counterfeits and Meta Quest VR headsets

U.S. PIRG Education Fund

Trouble in Toyland 2023

38th annual toy safety report

Threats stem from toys with
microphones, cameras and trackers,
as well as recalled toys, water beads,
counterfeits and
Meta Quest VR headsets

WRITTEN BY:

TERESA MURRAY
AND
R.J. CROSS

U.S. PIRG EDUCATION FUND

NOVEMBER 2023

PIRG CONSUMER WATCHDOG

ACKNOWLEDGEMENTS

U.S. PIRG Education Fund thanks our donors for supporting our work on consumer protection and public health issues and for making this report possible.

The authors wish to thank the following for editorial contributions:

- Edmund Coby, public policy intern, PIRG.
- Dev Gowda, deputy director, and Nancy Cowles, executive director, Kids In Danger, Chicago.
- Dr. Jerri Rose, associate division chief, pediatric emergency medicine, UH Rainbow Babies & Children's Hospital, Cleveland.
- Joan Lawrence, senior vice president of standards and regulatory affairs, and Kristin Goldman, senior advisor, strategic communications, The Toy Association, New York.
- Ashley Haugen, founder, That Water Bead Lady.
- Lucas Gutterman, Director, Designed to Last Campaign, PIRG.
- Ramsha Ali, research intern, PIRG.
- Emma Van Steertegem, research intern, PIRG.

Thanks also to the following for lending their expertise and insights:

- Rachel Franz of Fairplay.
- Dr. Mark Bertin M.D., PLLC.
- Dr. Brett P. Kennedy of the Digital Media Treatment and Education Center.
- Samuel Levine, director of the Consumer Protection Bureau, Federal Trade Commission.
- Alex Hoehn-Saric, Chair, Consumer Product Safety Commission.
- Peter Feldman, Commissioner, Consumer Product Safety Commission.
- Anna Laitin, Deputy Chief of Staff to CPSC Chair Alex Hoehn-Saric.

The author bears responsibility for any factual errors. Policy recommendations are those of U.S. PIRG Education Fund. The views expressed in this report are those of the author and do not necessarily reflect the views of our funders or those who provided review.

With public debate around important issues, often dominated by special interests pursuing their own narrow agendas, U.S. PIRG Education Fund offers an independent voice that works on behalf of the public interest.

U.S. PIRG Education Fund, a 501(c)3 organization, works to protect consumers and promote good government. We investigate problems, craft for solutions, educate the public and offer meaningful opportunities for civic participation. For more information about U.S. PIRG Education Fund or for additional copies of this report, please visit www.pirg.org/edfund

COVER IMAGE: mindsparx via 123rf.com

CONTENTS

EXECUTIVE SUMMARY 1

THE SMART TOYS CRAZE 4

SMART TOYS HELP FOR PARENTS AND GIFT-GIVERS 7

A LOOK AT THE GOOD AND THE BAD 13

WHAT TO KNOW: Drones, Roblox, smartwatches, smart speakers 17

THE DANGERS OF WATER BEADS 21

RECALLED TOYS FOR SALE 24

WHY ARE TOYS RECALLED ANYWAY? 28

BUTTON BATTERIES 29

CHOKING HAZARDS AND LABELS 30

OTHER RISKS: Counterfeit toys, children of different ages in the home, high-powered magnets 31

TOY-RELATED INJURIES 33

RECOMMENDATIONS AND CONCLUSIONS 35

VIRTUAL REALITY AND META'S QUEST 36

TIPS FOR PARENTS, CAREGIVERS AND GIFT-GIVERS 49

APPENDIX 55

EXECUTIVE SUMMARY

Last month, an 11-year-old girl was kidnapped by a man she encountered while playing a game online. Fortunately, she was found safe a short time later, about 135 miles away from her home. The game, Roblox, is one of the most popular mobile games this year.

This past spring, the Federal Trade Commission accused Amazon of violating the Children's Online Privacy Protection Act Rule (COPPA) through its Alexa service by keeping the voice recordings of children indefinitely and failing to delete childrens' transcripts, even when a parent requested they be deleted. Amazon also gathered geolocation data and used childrens' transcripts for its own purposes.

A few years ago, Fisher Price's Smart Toy Bear was discontinued. It was created for children ages 3 through 8 as "an interactive learning friend that talks, listens, and 'remembers' what your child says and even responds when spoken to," according to WeLiveSecurity. But research found a security flaw in the app would allow hackers to get information about children without permission.

This toy bear is not an isolated case. Multiple toys from major manufacturers have been discontinued in recent years after research from various groups showed that children's voices, images, locations and other information was being improperly collected or hacked. In other cases, vulnerable toys are still for sale.

These days, we're surrounded by smart devices – all of these things with microphones, cameras, connectivity, location trackers and more. These devices connect to the internet and/or to the outside world, and they gather and store data, sometimes very poorly. Our children's holiday gift wish lists may be filled with stuffed animals that listen and talk, devices that learn their habits, games with online accounts, smart speakers and watches, or all kinds of toys that require you to download an app.

The global market for smart toys grew from $14.1 billion in 2022 to $16.7 billion this year, according to a large market research firm. The business of smart toys is expected to more than double by 2027.

These toys, and the threats that come with some of them, may increase with the incredible growth of artificial intelligence. AI is now advertised in toy robots, games and interactive toy animals, some aimed at children as young as 3 years old. AI-enabled toys with a camera or microphone may be able to, for example, assess a child's reactions using facial expressions or voice inflection. This may allow the toy to try and form a relationship with the child and gather and share information with others that could risk the child's safety or privacy.

For Trouble in Toyland 2023, we are focusing first on smart toys and what parents and gift givers need to know to protect the children in their lives.

We also are looking at:

- **Water beads, which are often used as sensory toys, but the tiny, squishy balls can be deadly.**
- **The ongoing risk posed by online retailers that continue to sell recalled toys in violation of the federal law.**
- **Ongoing threats from high-powered magnets, button batteries, choking hazards, counterfeit toys and inadequate warning labels.**

In recent years, traditional toys such as stuffed animals, games, race tracks and building sets have become safer overall. That's largely because of tougher laws adopted in 2008, good oversight by regulators, efforts by many manufacturers, watchdog work by consumer advocates including PIRG and more awareness by parents and caregivers.

Some of the biggest threats in recent years are coming from different sources, such as counterfeit toys, fidget toys that violate safety standards, recalled toys still for sale and toys that invade children's privacy.

Toy-related deaths and injuries treated in emergency rooms among children 14 and younger have declined over the years, but there are still more than 150,000 such injuries a year. This of course doesn't include injuries treated in doctors' offices or that don't require medical attention. Not all injuries are caused by dangerous toys; sometimes an incident is caused by misuse.

PHOTO BY MATHEUS BERTELLI VIA PEXELS

PIRG also tested both Meta's newest virtual reality (VR) headset — the Quest 3 — and Meta's new junior VR accounts aimed at children ages 10 to 12. These wearable console systems create a 360-degree computer-generated world. We found using Meta's new junior accounts greatly increases parental controls over a child's VR experience – but we also found these new additions fail to eliminate some real concerns. Other researchers have found that even for teen Quest headset users, there are plenty of serious risks.

We've identified six main reasons parents should approach VR and Meta Quest headsets with caution:

1) **The technology is in its very early days.** We talked to pediatricians who strongly recommend waiting for Meta to do more thorough testing to ensure VR is safe, and for other

research on the effects on kids' and teens' developing brains before getting one. "It's just not worth the risk right now," developmental pediatrician Dr. Mark Bertin said in an interview with PIRG.

2) **The physical Quest headset is not designed to fit still-developing young bodies.** According to Meta, your child could end up with minor injuries, or possibly problems with visual development.
3) **VR feels really real.** It feels so real it's even being used to do virtual exposure therapy for phobias. But as child clinical psychologist Dr. Brett Kennedy pointed out, "If it feels that real, how you use it really matters." Even mild violence is a lot more intense in 3-D. VR content can also have a bigger impact on users' bodily reactions and mood than 2-D games, especially for younger users, and those effects can last long after you've taken the headset off.
4) **Many of the most popular games and apps available for Meta Quest headsets emphasize social interactions with others online, which can turn negative pretty quickly.** In PIRG's testing, we found interactions with our test 10-year-old's junior account ranged from bizarre to disturbing, including another player shooting himself in the head in front of our young player in an app rated OK for 10-year-old children. Other researchers using teen accounts on popular apps have experienced sexual harassment and even sexual assault attempts, particularly when using teen girl accounts.
5) **Some of the most popular apps available for use with Quest headsets include sexually graphic content**, including lewd audio group chats and people using their virtual avatars to simulate sex. Researchers have found minors have ready access to this content thanks to loopholes, poor moderation controls and content labeling failures.
6) **Quest headsets can gather a lot of data about users**, and playing games often requires agreeing to different third-party companies' data practices wholesale. VR headsets can also gather sensitive motion data, which can be used to infer health or demographic details about you, and there's virtually no regulation controlling how companies or other actors use this data.

The experts we spoke to recommend parents approach VR using the precautionary principle – don't use it at all until these problems have far better solutions, and Meta proves we can trust it with our children and teens.

If you are thinking of going ahead and getting a Meta Quest VR headset for your child or teen, we walk through the things to think about.

THE SMART TOYS CRAZE

The range of smart toys on the market is growing. Toys we never thought needed to be smart suddenly are: Besides toy robots that follow commands and stuffed animals that talk to us, we now have miniature soccer balls that require an app, toy cars with sensors to respond to hand motions, and tablet-interactive doctor's kits that make "playing doctor" a digital affair. Many of the major toy manufacturers have begun to offer more high-tech toys, including Hasbro, Mattel, and Lego.

Smart toys can incorporate various technologies, like cameras, microphones and sensors, as well as artificial intelligence capabilities and connectivity through the internet or Bluetooth.

Connected smart toys are also considered a part of the Internet of Toys (IoToys), featuring a range of Wi-Fi or Bluetooth connections, including remote-controlled drones, smartwatches and app-connected action figures. Some can collect data on your child and transmit it off of the toy to a company's external servers. For example, some interactive dolls with conversation capabilities use microphones and Wi-Fi to transmit a child's words to speech recognition software maintained by the company. The software then compares the child's words to a database of possible responses, which the company then transmits to the doll's microphone over Wi-Fi.

Parents may find that smart toys have their benefits. Companies often say that making a toy "smart" will keep children engaged longer by enabling new play features through software updates.

But smart toys come with unique risks that parents should be aware of.

An uncomfortable reality of smart toys: We don't know with certainty when our child plays with a connected toy that the company isn't recording us or collecting our data. All we have is their promise and the threat of consequences if they break it.

"A company is required by law to abide by claims about its privacy practices stated in its privacy policy and in other representations," said Samuel Levine, director of the Bureau of Consumer Protection at the Federal Trade Commission (FTC.) "If the toy is directed to children under 13 years old, the Children's Online Privacy Protection Act, or COPPA, requires the toy company to ask for your consent before it collects your child's personal information."

But there's a long list of companies the FTC has sanctioned, saying they violated COPPA. In these cases, consumers found out only *after* the fact.

Recent FTC violations include:

Microsoft, 2023. Will pay $20 million to settle allegations that it collected children's information on its Xbox gaming system

including their full name, phone number, email address and date of birth without parental consent. As part of the action, the FTC also made it clear to Microsoft and other companies that a child's personal information includes health information, vital signs and biometric data such as eye tracking, iris and retina scans, voiceprints, fingerprints, and hand and face geometry.

Edmodo, 2023. Ordered to pay $6 million but it was suspended because of the company's inability to pay. This was an educational product aimed at students, not a toy, but the company was accused of using children's data for advertising purposes.

Google and YouTube, 2019. Paid $170 million to settle allegations that Google's YouTube video sharing service illegally collected personal information from children without parental consent.

VTech, 2018. Paid $650,000 to settle allegations that its Kids Connect app, used with various VTech toys, "collected the personal information of hundreds of thousands of children" without notice or consent from parents as required under COPPA. This was the FTC's first children's privacy case involving a toy that connects to the internet.

And the previously mentioned case involving **Amazon, 2023.** The FTC and DOJ charged Amazon with violating children's privacy laws by using its Alexa/Echo service to obtain and keep children's voice recordings and geolocation data for years, and then deceiving parents who requested data be deleted and using the data for its own purposes. The government proposed ordering Amazon to pay $25 million for its COPPA violation.

It's notable that Amazon also offers Alexa-enabled devices and toys, such as a play kitchen and a board game currently. It's removed at least one toy's Alexa functionality by taking down the software that once connected the Fuzzible Friends stuffed animals to Alexa and Echo. We may see a growing number of toys in the future that connect to Alexa.

Internet- and bluetooth-connected toys come with particular risks

Connected toys that access the internet can often collect and store personal data, including audio recordings and user preferences. Collecting this type of data can make your or your child's information more vulnerable to hacking or unauthorized access, as was alleged with Hello Barbie and CloudPets. Data breaches involving various toys and unencrypted data from child users have already been reported.

Additionally, some connected toys can access internet content, which can expose children to inappropriate or harmful material without proper filtering and parental controls. Parents may want to weigh any possible educational benefits of devices with internet access against the risk of children unknowingly accessing inappropriate photos or websites.

While regulators and lawmakers have focused on the safety and privacy of children online for a quarter-century, it's an evolving issue as we see new technology and better technology every year. Levine of the FTC notes the agency has focused on

children's privacy online since supporting COPPA in 1998.

It's good for parents to know that regulators are monitoring the landscape for companies that violate the law and put our children at risk. We likely will see more enforcement and further regulation in the future.

"The FTC is staying on top of trends in the marketplace, like the emergence of artificial intelligence, virtual reality and augmented reality, and their potential implications for children's online privacy," Levine said.

"Congress is also considering legislation that would strengthen privacy protections for children."

In the meantime, parents and gift-givers can assess a toy they may be considering, or a toy their child already has using our tips in the next section.

PHOTO: ERIK MCLEAN-AYNNNJEOR4 VIA UNSPLASH

SMART TOYS HELP FOR PARENTS & GIFT-GIVERS

We offer insights on smart toys in three ways:

- The types of technology that raise issues and questions you should ask.
- A look at some good and bad toys.
- What to know about specific types of smart toys or children's gifts.

QUESTIONS FOR PARENTS TO CONSIDER ABOUT SMART TOYS

All smart toys may pose a risk to children, depending on the specific toy, the age of the child, the child's technical skills and their capacity to understand what's OK and what's not.

Up front you can ask your friends and family who might be shopping for your child not to buy a smart toy without checking with you first. Likewise, don't buy a smart toy for a child in your life without checking with their parent or guardian.

For any gifts you are considering, you can do a web search for the toy and read reviews people have written. Do any of them cause you concern? Also, look up the toy manufacturer. Does it have a history of troubling violations? What does the toy's privacy policy (which should be available online) say about what the toy does and information it collects?

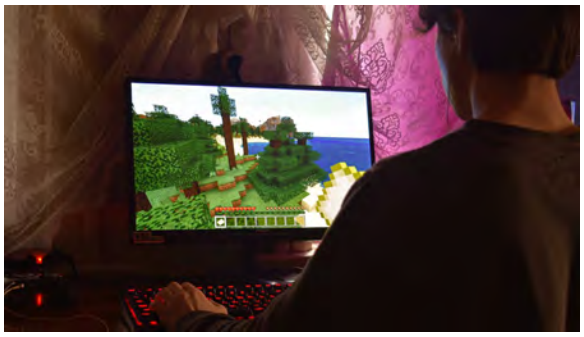


PHOTO BY ALEXANDER KOVALEV VIA PEXELS

"Parents and caregivers should understand the toy's features," said Samuel Levine, director of the Bureau of Consumer Protection at the Federal Trade Commission (FTC.) The big questions parents should pursue, he said:

- Does the toy allow the child to connect to the internet and send emails or connect to social media?
- Does it have a microphone or camera? If so, when will it record, and will you know it's recording?

The specific questions you should ask vary based on the type of toy and its features. In many cases, you should be able to find the information in the toy's privacy policy, which you can find online. (Make sure you're looking at the policy for that toy, not the company in general or just its website.) The answers may help you decide whether the toy is appropriate to buy for your child, what controls you can put in place or whether you should return the toy.

In some cases, you may not discover whether you're comfortable with how the toy operates until you actually use it. If you're not satisfied, you can return it.

QUESTIONS TO ASK:

If it has microphone:

- Is the toy's microphone always on? Does it have a wake word? (This can mean it's always listening.) Or is there a button you have to hold down in order to activate the microphone? The latter option is the safest feature.
- Is there a light or some indication the microphone is listening?
- Does it have a secure Wi-Fi or Bluetooth connection, which would prevent a stranger from talking to or listening to your child through the toy? For example, does it require you to set up your own strong password before play? Or does it allow you to use the toy with a weak default password that could be easily guessed – which could put your kid in danger?
- Do the recordings get collected by someone or some company using a Wi-Fi or Bluetooth connection?
- Where is the collected information stored – just on the toy, or also on the toy company's back-end server, or that of a third party "service provider"? The more companies store your child's data on their servers, the more likely it will be exposed in a breach or a hack.
- How are the recordings used? Some companies say they use recordings to improve their products. Others share them with third parties. In both examples, children and their families could be at higher risk of fraud, unwanted advertising and identity theft.
- Does the privacy policy specifically mention security being a priority for data it collects? Are the recordings stored securely? If not, then you may be better off finding a toy company that takes your child's safety and security more seriously.
- How long are the recordings retained? If the company fails to delete the data beyond what's necessary to fulfill the play function, it can increase the odds your child's data will eventually be exposed in a breach or a hack.
- Who has access to the recordings, or who are they shared with?
- Can you review recordings of your child and tell the company to delete the ones you may be uncomfortable with? This is useful particularly in the case of a child sharing more personal information with a conversational toy than you're comfortable with.

If it has a camera:

- Are the photos your child takes stored on an SD card or sent through Wi-Fi or Bluetooth? Storage on an SD card allows you to review and better control what happens with the photos. Sending photos via W-iFi or Bluetooth is faster but can represent

a risk of photos getting in the wrong hands.

- If they can be sent, are the photos stored on the toy company's back-end server?
- Does the privacy policy specifically mention the security it uses for images or photos it collects?
- Who has access to the images or photos or who are they shared with? Does the company's privacy policy say it shares with third parties?
- Can you access images or photos the company stored or shared?
- What does the company's privacy policy say about your ability to require the company to delete images or photos?

If it connects to Wi-Fi:

- Does it connect automatically to unsecured Wi-Fi networks? A toy for a child should not. You want a button on the toy that must be pressed or some intentional action you take to allow it to search for a network. If there's not a button, is there at least an app that requires a password to connect to Wi-Fi?
- If the toy connects to an unsecured Wi-Fi network, is it able to block any intrusions? You likely have to test this.
- Does it provide a way for your child to send or receive messages, or connect to any social media accounts? The privacy policy might indicate this. Or you might discover it when setting up the toy. It might recommend you to sign in via Instagram or Facebook, for example, or send messages to invite "friends" to connect to your child, and their toy. You don't want to connect a toy to a social media account.
- Does it share any information about your child, including geolocation? If so, it should be clear in the privacy policy, and you want to approach with caution whenever a toy gathers data as sensitive as your child's whereabouts.

PHOTO: DOMINIKSA ROSECLAY VIA PEXELS

If it connects to Bluetooth:

- Is the Bluetooth connection secure with a strong password? Or when you set it up, does it pair automatically with a device that's close, without a password? This could be dangerous if the toy has a range outside your home, or if the child takes the toy to public places.
- Does it contain a GPS that can be tracked, as many smartwatches have? This should be stated in the privacy policy. Location tracking could put your child at risk if the Bluetooth connection isn't secure. Good smartwatches and other secure products will allow you to block unauthorized pairing or require two-factor authentication.

If it collects any personal information from your child or about your child, and that child is under 13 years old:

- Does it transparently and clearly ask for permission to collect data from your child before your child begins play? Companies are required to do this by law. The privacy policy should state its practices. But if your permission isn't required when setting up the toy, you should return the product and report the company to the FTC online or by calling (877) FTC-HELP. If you need one-on-one help, the FTC says you should contact your state attorney general.
- Does the toy state in its privacy policy that it is a product meant for children to use, or does it say, "This product is not intended for use by anyone under 13?" If it's the latter, stay away. It will gather data about your child as if they were an adult, even if they are under 13.
- When you're setting up the toy and receive the notification asking for your consent, does it contain a link to the service's privacy policy, as it must by law? If it doesn't, that's a flag.
- Does it tell you how the information it collects is secured and note that you have the right to get your child's information deleted? These are required by law. If it doesn't provide these disclosures, you should return the product and report the company to the FTC online or by calling (877) FTC-HELP. If you need one-on-one help, the FTC says you should contact your state attorney general.

If it collects data on anyone of any age:

- Can you find its privacy policy? If not, stay away. Reading the privacy policy is where you'll find the answer to some of these questions:
- What types of data does it collect? Photos? Recordings? Your location? You need to decide what you feel comfortable with. You may be OK with a device knowing your location, but not recording conversations. If the privacy policy isn't acceptable, you shouldn't buy the product. If you already have it, you should return it.

- Does the privacy policy say any information collected gets stored on a back-end server? The more information that's stored, the more that can get into the hands of a bad guy if there's a breach or hack.
- Does the privacy policy specifically mention security being a priority for the data it collects? Does it tell you that it stores data securely? If not, you may want to find a product from a company that takes your family's safety and security more seriously.
- How is the information shared and who has access to it? Does it share with or sell data to third parties? This puts you at higher risk of fraud, unwanted advertising and identity theft.
- What are the default data collection settings? Especially pay attention to settings like collecting your geolocation automatically.
- How difficult is it to find settings on the product or app that restricts features you don't want to be active? If it's too cumbersome, you may want to return the product.
- Does it push advertising, particularly based on personal information collected? Its privacy policy should say whether the company or a partner uses data for marketing purposes. If you don't want more marketing calls, texts or emails, you should opt out of having your data, including your contact information, used for marketing.

If there's a privacy policy:

- Does it make it easy for you to find information related to children's data, like pulling the section on children's privacy to the top of the document? If it doesn't make it easy, this is a flag.
- Does it say the product isn't intended for users under 13? That means it's probably gathering a lot of data about your child because if it were for children under 13, the law requires greater data protections.
- Can you find and easily understand the information you need to decide whether you can control what personal data is shared and with who? If not, you shouldn't buy the product. If you already have it, return it.
- Does the company indicate it can "update" its privacy policy? Does it indicate how you will be notified if it does update or change anything? You should have the option to sign up for an email notice, instead of needing to remember to check the company's website periodically to find out.

Here's our complete guide on how to read a privacy policy.

If it has an app:

- What information does it require to create an account? You should not allow a young child to create an account without your oversight or

with an email account you can't access.

- Does the app developer have a privacy policy you can easily locate?
- Does the app's privacy policy state that its services are not intended for children under 13? If this is the case, it's very likely going to collect data on your child regardless of their age.
- What data does the app collect, according to its privacy policy? What is it used for? In your device settings, you should be able to opt out of data sharing you don't want, such as your location or browsing history.
- Does the app include in-app purchases? You may want to look into parental controls on spending so your child doesn't inadvertently wrack up big bills you don't want to pay.
- How secure is the app? Does it have social features, allowing unwelcomed messages or allowing strangers to communicate with your child? You do not want to connect it to or sign in with social media. If you don't and your child is getting unwanted messages, you may want to look at the settings again and delete the app if the problem persists.

If it allows your child to spend money:

Substandard practices can lead to your child spending too much money without your permission or buying things you don't approve of.

- Is there a monthly subscription that costs more than you want to pay?
- Does it store payment information or link to an iTunes, Amazon, PayPal or other account, or save your credit card on file? This could make it easier for your child to spend money without your authorization.
- Does the account or app have parental controls you find useful to limit or monitor spending? This can include requiring your approval for each transaction or for transactions above a certain dollar amount. You may also be able to set alerts to better monitor your child's spending.
- Does it require a balance to be kept in the account? This may allow purchases without your permission.
- What's the process for challenging a transaction?
- What's the highest dollar amount for a single item? Apps can include purchases ranging from 99 cents to $99.99. If high-priced items are easily purchased, it may be more important to you to find and set those parental spending controls.

A LOOK AT THE GOOD AND THE BAD

We bought a few smart toys to see how they work, whether they do what they say and how easy it is to protect information. This isn't a full review or absolute recommendation for or against buying any of them; it's just meant to be a look at how some real toys work and the issues you might encounter.

A TOY WITH UNSECURE BLUETOOTH

Amazmic Kids Karaoke Microphone

This $15 toy karaoke microphone "uses the latest Bluetooth 5.0 technology to provide a more stable connection" – up to 33 feet, according to the online listing. It promised fast pairing and said it's compatible to pair with a phone, tablet, laptop, etc. It also is compatible with a TransFlash card and cable connection.

The instructions say the device requires a password to pair. Good. But the password is 0000. Not good. Further, our microphone paired in about two seconds – with no password at all. We tried this three times on three different iPhones. Same unsecure result with no password required. We were able to pair at about 30 feet. It's troubling there doesn't appear to be an easy way to make it undiscoverable so strangers can't drop in on your child and send undesirable audio messages or play inappropriate music. It does have all kinds of pretty lights. And when you play music through the speaker, it has great sound, to be honest.

PHOTO BY US PIRG EDFUND

A TOY WITH SECURE BLUETOOTH

VTech Kidi Star DJ Mixer

This does require a PIN, which the company encourages users to keep enabled: "VTech strongly recommends keeping the PIN security on for the use of Bluetooth transmission to avoid any connection by an unauthorized device. The disabling of the PIN security should only be used when the connection of an external device with PIN security is impossible. The use of the toy when PIN security has been disabled should be under the supervision of an adult."

In addition, if a device tries to connect via Bluetooth, the toy requires giving it permission. The pairing process requires pressing the Bluetooth connect button to search for a nearby device. Once the device is paired, you have to press the Bluetooth input button to allow this as the audio source. It sells for about $54.

TWO TOYS WITHOUT THE ABILITY TO CONNECT THROUGH WI-FI OR BLUETOOTH

Prysyedawn Toy Smart Phone

This toy smart phone does not connect through Wi-Fi or an app. You can take photos, listen to music and play games. It also has other features such as an alarm clock and calculator. Photos are stored on an SD card. You have to connect it through a USB cord to download photos. This gives the user more control over their child's data. This sold on Amazon for about $33.

Goopow Kids Camera-Video Camera for 3-8 Year Olds

This children's camera takes photos and shoots video. It does not connect through Wi-Fi or an app. It says it can take up to 1440x1080P video and has other functions, including choosing different scenes. Photos and videos can be downloaded through an included card reader. This gives the user control. This is an Amazon "best-seller," available for about $31.

A TOY WITH A BAD PRIVACY POLICY

Cognitoys Dino

This cloud-based, Wi-Fi-enabled smart dinosaur was introduced in 2016, aimed at 5- to 9-year-old children. The dinosaur engaged in conversations, told jokes and stories and answered questions. Connected through Wi-Fi and powered by IBM/Watson, it was intended to be a toy "that learns and grows with children." Dino didn't last long as the tech company behind the toy folded and the app support was discontinued.

PHOTO BY US PIRG EDFUND

The privacy policy was disturbing. Here's a small sample:

"Information We Collect

"Personal Information. We collect information that possibly personally identifies you and your child, such as your full name, address, mobile phone number, wi-fi SSID, IP address, device MAC addresses, e-mail, payment information (including zip code), child's name, child's date of birth, child's gender, and other personally identifiable information, that you choose to provide us with or that you choose to include in your account ("Personal Information"). For example, you may provide us with certain Personal Information when you use the Parent Panel.

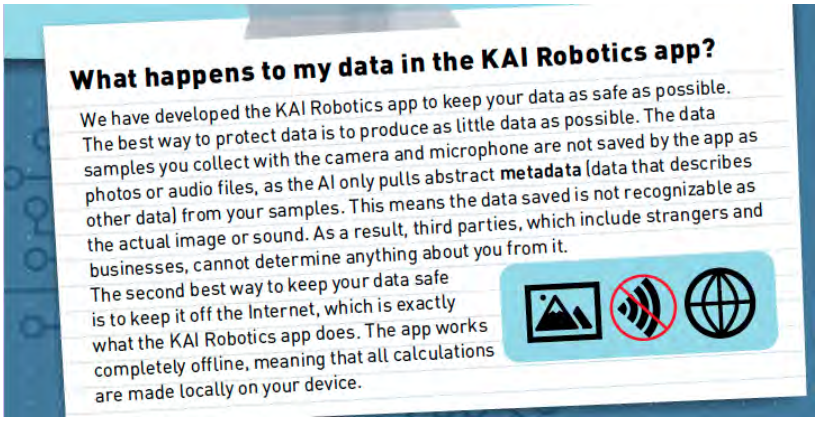
"Play Data. When a child interacts with his or her Dino, we automatically collect certain play-related information from your child and from such interactions ("Play Data"). For example, when your child plays with the Dino, we may automatically collect information about your child's likes and dislikes, interests, and other educational metrics."

A TOY WITH A GOOD PRIVACY POLICY

KAI: The Artificial Intelligence Robot

The Kosmos Artificial Intelligence robot allows users to "explore the concept of machine learning" by building and programming an intelligent, six-legged, app-enabled robot that is supposed to respond to sounds and gestures.

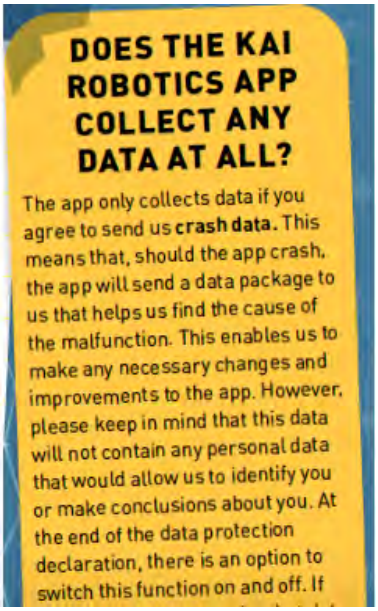
This toy's privacy policy is an example of a good, easy-to-read explainer. It spans two pages of the toy's 68-page instruction manual. A couple of excerpts:



What happens to my data in the KAI Robotics app?

We have developed the KAI Robotics app to keep your data as safe as possible. The best way to protect data is to produce as little data as possible. The data samples you collect with the camera and microphone are not saved by the app as photos or audio files, as the AI only pulls abstract **metadata** (data that describes other data) from your samples. This means the data saved is not recognizable as the actual image or sound. As a result, third parties, which include strangers and businesses, cannot determine anything about you from it.

The second best way to keep your data safe is to keep it off the Internet, which is exactly what the KAI Robotics app does. The app works completely offline, meaning that all calculations are made locally on your device.



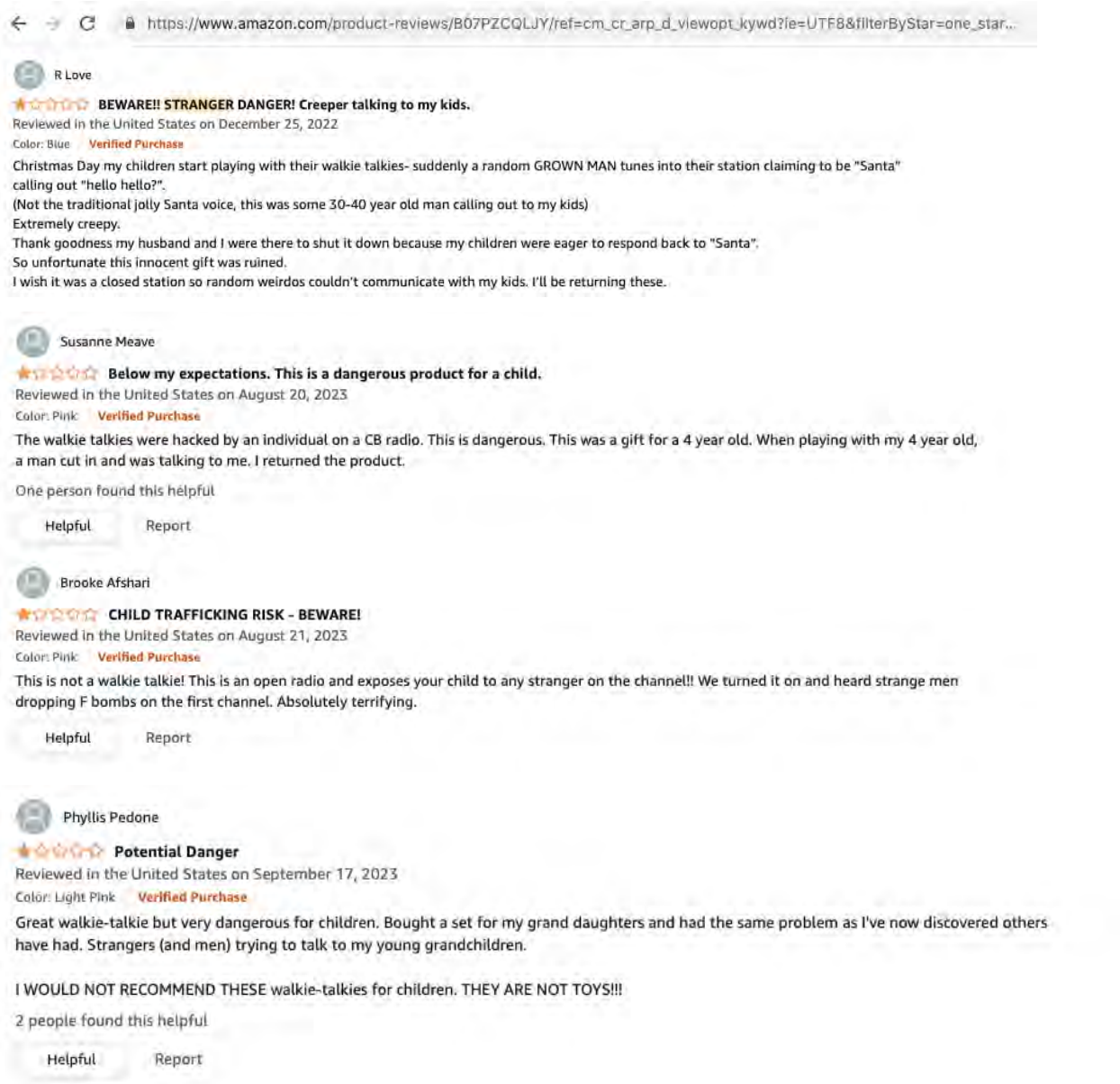
DOES THE KAI ROBOTICS APP COLLECT ANY DATA AT ALL?

The app only collects data if you agree to send us **crash data.** This means that, should the app crash, the app will send a data package to us that helps us find the cause of the malfunction. This enables us to make any necessary changes and improvements to the app. However, please keep in mind that this data will not contain any personal data that would allow us to identify you or make conclusions about you. At the end of the data protection declaration, there is an option to switch this function on and off. If

Selieve Toys-Walkie Talkies for Kids

These walkie-talkies with 22 channels and a three-mile range are a "bestseller" on Amazon with more than 32,000 ratings. It sells for about $19.99. This is not a toy we would recommend for younger children unsupervised. It's not what we think of as a smart toy because it's older technology. But the quality has improved over the years. This claims a three-mile range. There are multiple reviews on Amazon that report

strangers or even ”creepy people” talking to young children or using foul language; the available channels are easy to find when you’re in range.



A TOY WITH INSECURE STORAGE
CloudPets

After privacy advocates raised serious security issues, major retailers stopped selling CloudPets a few years ago and the company closed. The stuffed animals used Bluetooth to connect to a parent’s phone to allow a loved one (maybe a grandparent in another state) to send audio messages back and forth. But the database where the recordings were stored was not secure. A hacker obtained personal information for 800,000 CloudPet owners: children’s names, relatives authorized to send messages, email addresses, passwords, as well as 2.2 million audio files hosted on Amazon Web Services.

WHAT TO KNOW ABOUT SPECIFIC TYPES OF SMART TOYS

DRONES

The last few years have seen a surge in consumer drones thanks to better technology, lower prices, increasingly user-friendly controls and opportunities for aerial photography and recreational use. As the technology continues to advance, the consumer drone industry is expected to continue to grow. An expanding market for retailers is marketing drones to children.

Drones for children can vary greatly in price, capabilities and intended use, from indoor toys for preschoolers, to camera drones, racing drones and stunt drones. They can cost as little as $30 or can top $10,000.

Drones come with a unique set of concerns:

1. **Safety first:** Drones with fast-spinning propellers can be dangerous. Collisions with people, animals or property can lead to injuries or property damage. A toddler in the UK lost an eye after being hit by a drone flown by a family friend.

2. **Legal responsibilities:** Drones come with unique legal responsibilities. The Federal Aviation Administration (FAA) oversees drone rules but states and localities may place additional restrictions. The FAA requires all drones that weigh greater than 0.55 lbs (250 grams) to be registered.

PHOTO BY LUIS QUINTERO VIA PEXELS

3. **Respecting privacy:** Drones equipped with cameras can intrude on others' privacy, leading to unintentional privacy violations, which children might not fully grasp.

ROBLOX

Roblox is one of the most popular mobile games among kids this year, cracking the top 10 in downloads for both Android and Apple. Roblox offers a creative and engaging platform for kids to design games, interact with friends and unleash their creativity, but it's not without its potential dangers.

1. **Inappropriate content:** Roblox allows users to create and share content, leading to potentially age-inappropriate games and avatars. Instances of explicit or violent themes have been reported in Roblox

PHOTO BY MATHEUS BERTELLI VIA PEXELS

games. User-made avatars can introduce children to inappropriate content.

2. **Online predators:** An 11-year-old girl from Delaware was kidnapped from her home by an adult who communicated to her through Roblox. She was later found safe.

3. **In-app purchases and microtransactions:** Roblox makes its money through in-app purchases and its artificial currency Robux. Kids may not grasp the consequences of real money spent on virtual items and spend more than parents would prefer.

4. **Addictive nature:** In 2020, 36 million people — two-thirds of them under 16 — spent more than 30 billion hours on Roblox. Its engaging gameplay can lead to excessive screen time, raising concerns with some experts about the game fostering Internet Gaming Disorder among young users.

PHOTO BY CAIO VIA PEXELS

SMART SPEAKERS

Smart speakers are among the most popular Internet of Things (IoT) devices in American households. These voice-activated virtual assistants, such as Amazon Echo, Google Home and Apple HomePod, have found their way into millions of homes, offering various capabilities such as streaming music, sending messages, controlling other smart devices and conducting web searches.

With more than 71 million Alexa-enabled devices in use as of 2023, these smart speakers have quickly become ubiquitous. However, the rise of conversational commercial products also raise significant privacy and safety concerns for both adults and children:

1. **Data collection:** One of the primary issues with smart speakers is their persistent data collection. Equipped with internal microphones, these devices wait for a specific "wake word," often the name of the virtual assistant persona created by the respective company, such as Amazon's Alexa, Apple's Siri, or Microsoft's Cortana, to activate. While this system is designed to be convenient to consumers, it's not

without flaws. A 2020 study by Northwestern University researchers found that Apple, Microsoft, Google and Amazon smart speakers were prone to accidental activations, recording users' conversations without a "wake word" prompt up to 19 times a day. In 2023, Amazon paid $25 million to settle FTC and DOJ allegations it had violated COPPA for failing to delete young users' voice and geolocation data collected by its smart speakers.

2. **Inappropriate content:** Smart speakers can access content from the internet, which means children may encounter or request inappropriate content, such as explicit music, jokes or harmful advice. While these devices aim to filter profanity, third-party apps can contain content that parents may not want their children to access. In one case, academic researchers were successfully able to smuggle 234 policy-violating skills onto the Alexa Skills Store, the marketplace for third-party apps on the Echo smart speaker.

3. **Voice-enabled online shopping:** Smart speakers offer voice-activated online shopping, and children left unsupervised may make unauthorized purchases. This can result in high charges on a parent's credit card, as was the case with Brooke Neitzel, a 6-year-old who unwittingly spent $160 of her mother's money on a KidKraft Sparkle Mansion dollhouse and dozens of sugar cookies. Neitzel made the purchases by simply asking her Amazon Echo device "Can you play dollhouse with me and get me a dollhouse?"

PHOTO BY INGO JOSEPH VIA PEXELS

SMARTWATCHES

Smartwatches can be a fun and functional wearable technology. They may provide entertainment for kids and peace of mind for parents hoping to have a way to communicate with their child before making the jump to buying a smartphone.

There are hundreds of kids' smart watches on the market with varying degrees of technical capabilities and at various price points. Some are very basic with low-fidelity LCD displays that allow kids to see the time and play some mobile games. They typically sell for less than $40. On the other end of the spectrum, there are watches such as Verizon's Gizmo Watch 3, a 4G-enabled kids' smart watch that acts as a communication device through its app with connected-GPS tracking and video calling capacities. The 8GB Gizmo Watch 3 sells for about $150.

Smartwatches come with some security and privacy considerations for parents and guardians.

1. **Location tracking risks:** While location tracking is a key safety feature, it can inadvertently expose a child's whereabouts and pose risks if data falls into the wrong hands. The Norwegian Consumer Council found multiple critical security flaws in various smartwatch brands that could expose real-time location data, and could be made by hackers to display an incorrect location — alarming if a child's location was needed in an emergency.
2. **Data privacy vulnerabilities:** Some smartwatch companies share technical backend infrastructure, meaning vulnerabilities in one smartwatch can affect others. A study of children's smartwatches in 2020 found that several lacked encryption and authentication, potentially exposing childrens' sensitive data.

   Smartwatch companies have come under fire by European regulators, with kids' smartwatches that can eavesdrop without being detected being banned within Germany. The German telecoms regulator, the Federal Network Agency (BNetzA), went as far as recommending that parents destroy these "eavesdropping" devices.

THE DANGERS OF WATER BEADS

Water beads are a colorful, squishy sensory toy. Some are small as pinheads or ice cream sprinkles. Some are the size of marbles. The problem is, as the name suggests, something happens when combined with water. What they do is grow, from the size of a pea, for example, to two inches in diameter.

So if a child swallows one of these beads that are colorful and look candy, it can expand in the child's body. It can block the airway or damage the digestive tract.

"If ingested, inhaled, or inserted in ear canals, water beads absorb bodily fluids and can lead to potentially life-threatening injuries," said Dev Gowda, deputy director of Kids In Danger in Chicago. Those can include intestinal or bowel blockage, lung or ear damage and other life-altering injuries.

About 7,800 children were treated in emergency rooms from 2016 through 2022 for injuries or illnesses caused by water beads, according to data from the Consumer Product Safety Commission.

There has also been at least one death blamed on water beads: a 10-month-old in Wisconsin who died in July 2023.

The CPSC in September issued a strong warning to families to keep water beads out of any place where babies and young children might be.

"Regulation of water beads is the logical next step and I anticipate the CPSC starting the process in the coming year," CPSC Chair Alex Hoehn-Saric told U.S. PIRG Education Fund.

Just this week, Congressman Frank Pallone Jr., (D-N.J.) announced plans to introduce legislation banning water beads marketed to children.

A look at how water beads grow

U.S. PIRG EdFund put beads in a bowl and added water. After 32 hours, they grew to nearly 2 inches in diameter. You can see the size compared with a quarter.

Ashley Haugen wishes they never existed. It's been six years since her 10-month old daughter Kipley swallowed some small colorful water beads that belonged to her older sister. That was the beginning of the Texas family's nightmare during the hours it took for the beads to be discovered and surgically removed, and the weeks after that as Ashley and her husband realized Kipley suffered from brain damage.

It also began Haugen's mission to warn other parents and regulators about the dangers of water beads through her non-profit organization, That Water Bead Lady.

Haugen has spent the years learning about the science and the marketing and the lack of understanding and resources.

Unfortunately, other children have since been injured and at least one died this year after ingesting the squishy beads, which – when wet – can grow from the size of an ice cream sprinkle to an inch in diameter or larger – even 100 times their original size – and cause an intestinal blockage.

Haugen and other parents whose children were seriously hurt after swallowing a water bead met last spring with Hoehn-Saric, along with Commissioners Mary Boyle, Peter Feldman and Richard Trumka, to plead for water beads to be better regulated or even banned.

Water beads are often sold in packages of 30,000 to 50,000. They're tiny. They roll. They stick in hidden places. "Dry water beads can be the size of a pinhead, making them nearly undetectable if dropped on the floor or spilled in a playroom," the CPSC says in an advisory on its website.

In September, the first recall of water beads since 2013 was announced after a 10-month-old Wisconsin baby died and a 9-month-old baby in Maine was seriously injured after swallowing one of the water beads. About 52,000 Chuckle & Roar Ultimate Water Beads Activity Kits were recalled. The water beads were sold by Target for about $15 from March 2022 through November 2022.

More importantly, the CPSC signaled more regulation and restrictions of water beads are coming. The risk is not limited to a single product, Hoehn-Saric said.

"I am deeply concerned about the hazard posed to small children from water beads," Hoehn-Saric said. "This year we issued a recall of one water bead product following the death of a small child. We also made clear in our public messaging that water beads should never be in homes or other spaces where babies and small children may spend time."

Haugen takes some comfort knowing her message is getting out. "I am hearing an overwhelming uproar from families across the country, signaling the increasing surge in awareness about the dangers of water beads," she told U.S. PIRG Education Fund.

"As a parent it is deeply unsettling to discover water beads in unexpected places, like ticking time bombs around your home,

or utilized as sensory toys in your child's school or therapy clinic without your knowledge or consent."

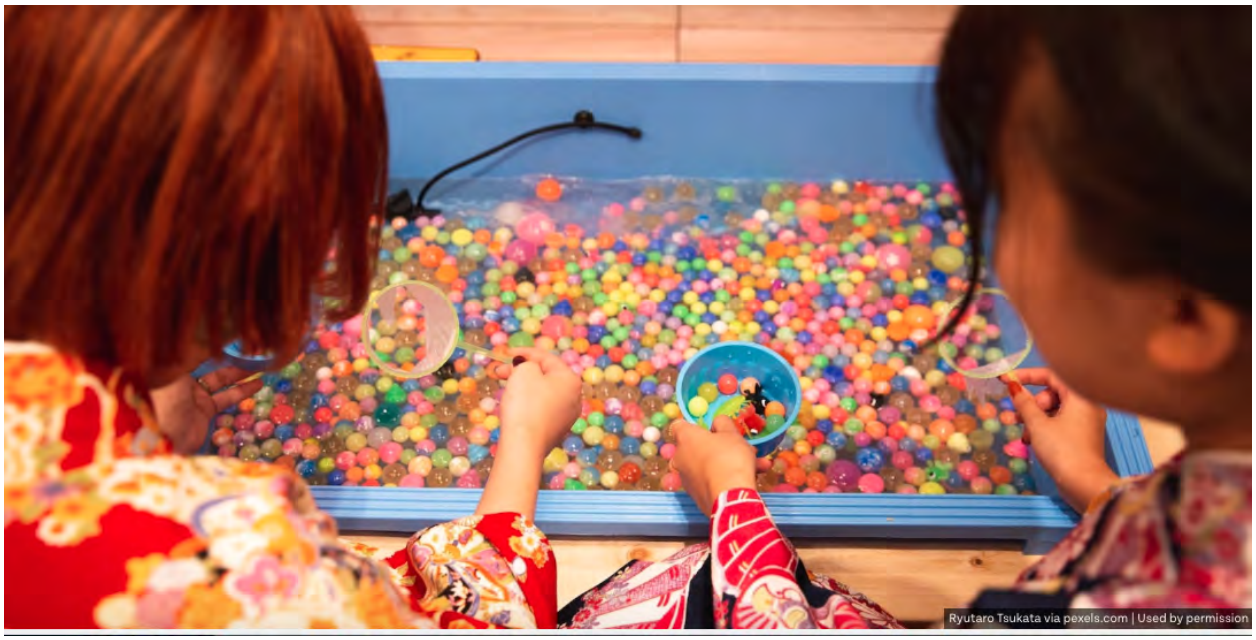
Based on all of the conversations Haugen has had with families across the country, she said it's important to realize that an injury from a water bead "can happen to any family. … Implying that better supervision or cleaner homes is the solution to preventing these incidents is misleading."

Haugen's goal is to get water beads banned and to warn families who may already have them in their homes.

Gowda of Kids In Danger said water beads are not worth the risk.

"No amount of supervision can keep children safe from water beads. Even if you're buying them for older kids, the tiny beads can spread in the home and a younger child may get hold of them," Gowda said.

"Get rid of any you have in your home now and then stay vigilant because families have reported that they continue to find water beads even years later."



RECALLED TOYS FOR SALE

One of the most frustrating and senseless dangers in Toyland is the sale of toys that have already been recalled because they're dangerous. Sometimes the toys have small pieces that can break off easily and choke or cut a child. Other times the toys contain excessive levels of lead.

In any case, once a toy or any other product has been recalled, it's illegal for anyone to sell it. This problem has existed for years. In last year's Trouble in Toyland report, we documented how easy it is to buy recalled toys. U.S. PIRG Education Fund bought, paid for and received more than 30 recalled toys from a variety of online retailers.

We conducted a similar experiment this year, on a smaller scale, by buying five toys of the 17 toys that had been recalled this year. Once again, it was too easy.

We bought toys from three online retailers. They are:

- Silver Lining Cloud Activity Gym by Skip Hop, recalled Feb. 9, 2023. Purchased Oct. 6, 2023, through Facebook Marketplace.
- Calico Critters Animal Figures by Epoch Everlasting Play, recalled March 9, 2023. Purchased Oct. 14, 2023, through eBay.
- Basket with Balls by Monti Kids, recalled April 6, 2023. Purchased Oct. 2, 2023, through eBay.
- Baby Shark Sing & Swim Bath Toys by Zuru, recalled June 22, 2023. Purchased July 28, 2023, through eBay.
- Rainbow Road board book by Make Believe Ideas, recalled Sept. 21, 2023. Purchased Oct. 1, 2023, through Little Giant Kid.

TRACKING DOWN RECALLED TOYS

To check whether toys you're considering buying or toys already in your home have been recalled, go to cpsc.gov/recalls

TO CHECK ON A TOY BEFORE YOU BUY

Do a keyword search on saferproducts.gov

PHOTO: US PIRG EDFUND

It is illegal to sell recalled toys. Here are the five recalled toys U.S. PIRG Education Fund purchased online in recent months: Silver Lining Cloud Activity Gym; Rainbow Road board book; Basket with Balls by Monti Kids; Baby Shark Sing & Swim Bath Toys; and Calico Critters.

The CPSC and members of Congress have also stepped up attention on products for sale after they've been recalled.

In August, a bi-partisan group of representatives in Congress wrote letters to 17 companies, including Meta (Facebook,) Amazon, Walmart, Target, Ebay and Poshmark. The letters noted that online marketplaces are expected to prevent the sale of recalled products through their sites.

The letters said the companies have "been falling short on this mission."

The letters were sent by House Energy and Commerce Committee Chair Cathy McMorris Rodgers (R-WA); Full Committee Ranking Member Frank Pallone, Jr. (D-NJ); Innovation, Data; Commerce Subcommittee Chair Gus Bilirakis (R-FL); and Subcommittee Ranking Member Jan Schakowsky (D-IL).

A few months earlier, in April, CPSC Chair Alex Hoehn-Saric sent his second letter in as many years to Facebook/Meta CEO Mark Zuckerberg. The message was about the same as in the 2022 letter.

Much of the ire has stemmed from sales of recalled Rock 'n Play rockers, which have been connected to about 100 infant deaths in recent years. But the principle – that it's illegal to sell recalled products – applies to all products, including toys.

"Facebook is uniquely positioned to identify recalled and violative products … and stop their sale before they are listed," Hoehn-Saric wrote. "Moreover, at best, CPSC is catching these unlawful products after they have been listed for sale and made available to the public; we do not know how many illegal sales occurred that we did not identify. … If CPSC staff can identify these illegal listings using your site, Meta indisputably can prevent them from appearing in the first place."

To carry that further, if U.S. PIRG Education Fund can so easily find and buy recalled toys, why can't these companies update their sites once a week to reflect the CPSC's newly recalled products? Of course they can. For the products we bought, the listings weren't even misspelled. Some had been recalled months before. For last year's investigation, some of the products had been recalled a year or two before.

And some of these sites allow you to save searches and get email alerts when a new product matching those keywords is listed.

So they can do that but not flag those listings Of course they can. This is obvious they often send we messed up emails after the recalled product is received. See Appendix.

The other question is why some companies, such as T.J. Maxx, Home Depot, Best Buy and Meijer have faced multi-million dollar civil penalties for selling recalled products, but companies such as Facebook Marketplace and eBay haven't?

"Under CPSC's statute, different safety obligations apply when a company is a manufacturer, distributor, private labeler, or retailer of goods," Hoehn-Saric told U.S. PIRG Education Fund. "Online marketplaces that host third-party sellers don't fit neatly into one of those categories for most of their operations."

It may come down to Section 230 of the 1996 Communications Decency Act, which some say insulates online platforms from being responsible for products sold illegally on their websites. It says: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Now, many would say that publishing opinions is one thing and allowing the illegal sale of goods is something else. Still, if Congress would amend the law, or the question would be resolved in a court case, the CPSC would have more clarity to pursue enforcement against platforms such as Facebook Marketplace and eBay, just like the regulator does with big box retailers.

CPSC Commissioner Peter Feldman told U.S. PIRG Education Fund that something needs to change with these online companies. "The status quo can't stand," he said. "It's clear there's more they can do and should be doing to keep their users safe. These firms absolutely have the resources necessary to prevent these transactions."

If these online retailers continue to allow the sale of recalled products, the CPSC may try a different tactic than just sending letters, Feldman said. "All options are on the table."

Aside from the interpretation of the law that may protect online retailers for now, there's certainly no reason the companies couldn't voluntarily block the sale of recalled products, as they do with other products they're not allowed to or don't want to sell, such as guns, animals or drugs.

"Yes, I share your concern about recalled, non-compliant, and dangerous products online," said Hoehn-Saric, the CPSC chair, told U.S. PIRG Education Fund.

That's why he met with six of the largest online marketplaces in the last year, including eBay and Facebook Marketplace, to urge them to work with the CPSC.

"Online marketplaces can and should adopt common sense practices to protect consumers," Hoehn-Saric said. "This includes prioritizing product safety within the companies and vetting sellers and products that platforms allow to be sold on their sites. Some companies are taking steps in the right direction, but clearly not enough is being done."

For now, the CPSC is playing whack-a-mole. When listings for recalled products are found or reported to the CPSC, the regulator issues "take-down requests."

The CPSC issued more than 57,000 take-down requests to e-commerce platforms in FY23, with the vast majority of those going to Facebook Marketplace.

"This reliance on industry's good will," Hoehn-Saric said, "is not a long-term solution to the problem."

TO FILE A COMPLAINT

If you have a serious incident with a toy, you can alert the CPSC by filing a report on saferproducts.gov

WHY ARE TOYS RECALLED ANYWAY?

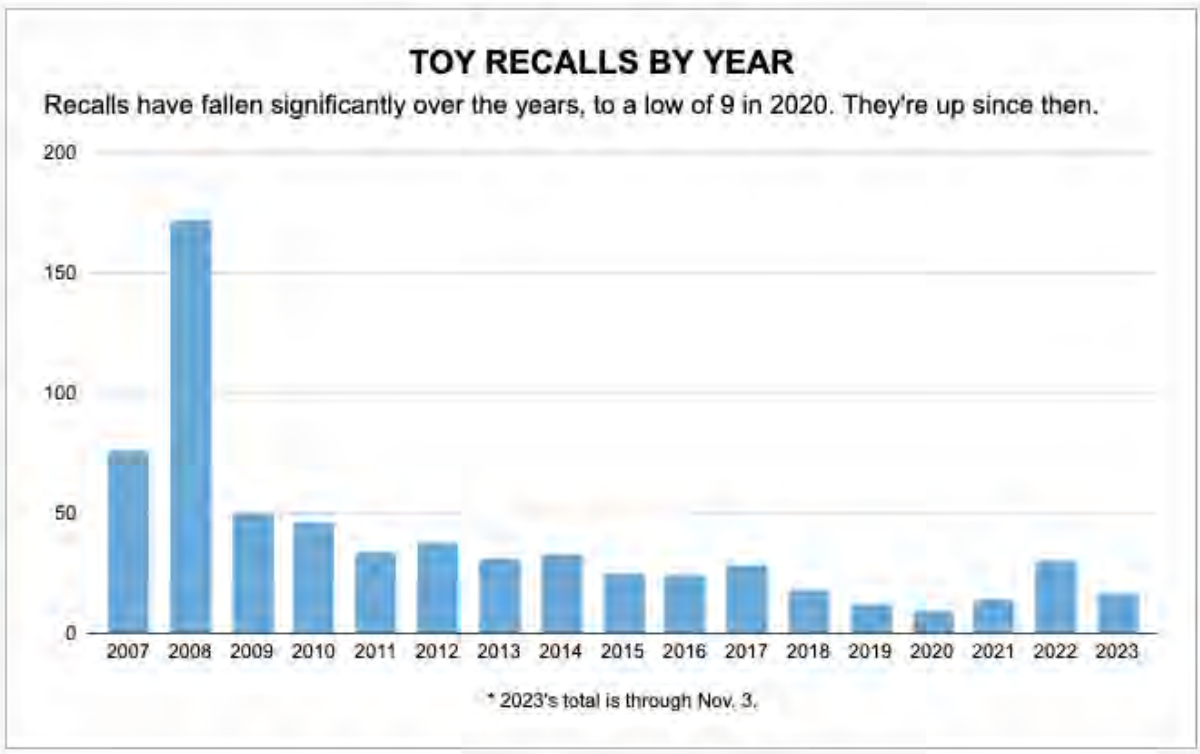
Toys are recalled either after defects or injuries have been reported to the company or the CPSC, or if the CPSC finds a problem through random testing. Recalls are almost always voluntary, in cooperation with the CPSC, because mandatory recalls generally have to go through a court.

Toy recalls have declined significantly in the last 15 years. In 2007, there were 76 recalls. That jumped to 172 recalls in 2008. Recalls declined gradually after that, to a recent low of only nine recalls in 2020. Last year, there were 30. So far this year, through Nov. 3, there have been 17.

The expectations for toys are high. "All children's toys manufactured or imported on or after February 28, 2018, must be tested and certified to ASTM F963-17 (ASTM International was formerly known as American Society for Testing and Materials," the CPSC says.

Further, "all toys intended for use by children 12 years of age and under must be third-party tested and be certified in a Children's Product Certificate as compliant to the federal toy safety standard enacted by Congress," the CPSC says. The laboratory must be one accepted by the CPSC.

The standards vary depending on the type of toy and the age group it's marketed to.



BUTTON BATTERIES

Four years after 18-month-old Reese Hamsmith died because she ingested a button battery from a remote control, a law named after her will take full effect. Reese's Law will require stronger safety procedures for products that use button or coin batteries, such as key fobs, bathroom scales, game controllers, tealight candles and greeting cards, effective March 19, 2024. The law also requires packages containing replacement batteries to comply with child-resistant packaging.

The CPSC in September 2023 approved final standards aimed at reducing the threat to children 6 years old and younger by requiring compartments holding button batteries to be more difficult to open. Opening these compartments must require something like a screwdriver or coin, or two separate, simultaneous movements by hand.

The new battery standards don't apply to toys for children less than 14 years old if the toys adhere to the Toy Standard.

If swallowed, button batteries "can burn through a child's throat or esophagus in as little as two hours," the CPSC says.

About 54,300 people went to emergency rooms from 2011 through 2021 after button or coin batteries were ingested or inserted in their body, such as through their nose or ear, according to CPSC estimates based on data from the National Electronic Injury Surveillance System. Victims are usually children 4 years old and younger.

PHOTO VIA PIXABAY

At least 32 deaths are blamed on button batteries from Jan. 1, 2011 through March 31, 2023, including three last year and two in the first three months of this year.

CPSC Commissioner Richard Trumka noted in a statement the CPSC gave product manufacturers six months to comply after its September 2023 vote. "But make no mistake: manufacturers shouldn't wait six months — I expect them to comply with the rule ASAP. Compliance with CPSC's rule on button and coin cell batteries will save lives."

The new rules for battery compartments and packages of replacement batteries will better protect children. It's still important for parents and caregivers to make sure compartments are secure and that young children can't access discarded or replacement batteries.

CHOKING HAZARDS AND LABELS

From 1980 to 1995, nearly 200 children died after choking on balloons, small balls or marbles. All of those products now must adhere to the revised labeling requirements.

In 1994, about 5,000 children were treated in emergency rooms after swallowing or aspirating toys or pieces of toys. That's a stunning number. And of the 18 toy-related deaths in 1994, 13 were blamed on choking.

The CPSC launched a massive labeling campaign. By Jan. 1, 1995, all newly manufactured toys intended for children 3 to 6 years old had to be labeled as a choking hazard to children younger than 3. The change was aimed at saving lives.

In 2021, one child died from choking on a toy, according to the CPSC. The 17-month-old boy swallowed a plastic toy,

which was part of a playset. Still, though, more than 9,000 children age 4 or younger were treated in emergency rooms in 2021 for ingesting a toy or a piece of a toy.

To determine whether a toy or part could be a choking hazard, check whether it can fit through a cardboard toilet paper roll. If it does, it could be swallowed by a child.

Toys that contain small parts and pose a choking risk must be labeled that they're not safe for children less than 3 years old, as the ones below are labeled prominently.

PHOTO BY USPIRG EDFUND

OTHER RISKS

COUNTERFEIT TOYS

Counterfeit toys continue to infiltrate retailers' shelves and online platforms, with many coming in from overseas. Counterfeit toys can't be assumed to meet stringent, mandatory U.S. safety standards, which require that all toys designed for children 12 and younger "must be third-party tested, be certified in a Children's Product Certificate and comply with the federal toy safety standard enacted by Congress," the CPSC says.

There are more than 100 safety standards and tests required for toys.

It is reasonable to assume that counterfeiters don't worry about those important safety standards and testing. In fiscal year 2022, CBP seized 381 shipments of toys worth $7 million for copyright infringement, meaning they're counterfeits.

One shipment seized on a given day could contain hundreds or even thousands of the same item.

Last year's seizures are up from 284 shipments the year before, an increase of 34%.

"Legitimate toy companies spend significant resources to bring their products to market – including steps to certify their products are safe," said Joan Lawrence, senior vice president of standards and regulatory affairs for The Toy Association, the industry's trade association.

"However, under current law, sellers on third-party online marketplaces are unfortunately able to operate anonymously and take advantage of consumer faith by selling products that may be counterfeit, stolen, or recalled and may not comply with safety laws – putting our children at risk."

The Toy Association has been urging Congress to pass stronger laws, aimed in particular at online marketplaces that sell all kinds of products, whether they're counterfeit, stolen or recalled.

This shipment of toys looks like real Toy Story-branded toys. They're counterfeit and likely don't meet U.S. safety standards. They were seized by U.S. Customs and Border Protection.

Congress did pass the INFORM Act aimed at counterfeit and stolen goods, but it only cracks down on higher-volume sellers.

Counterfeit products can pose other risks, Lawrence said. They may not be appropriately age-labeled, especially if they have small parts, and they're often made of materials of poor quality that can put children at risk.

Counterfeit smart toys are a growing problem as smart toys become more mainstream, she said. "It may be tempting to purchase one online at a low price from an unknown seller," she said. But these toys may violate FTC guidelines and federal children's privacy laws, she said.

CHILDREN OF DIFFERENT AGES IN THE HOME

It can be challenging to make sure children of different ages don't have access to toys they shouldn't, Lawrence said. A child less than 3 shouldn't be around dolls with tiny accessories, for example, or small parts of a building set. Children who are 5 or 6 should not be able to access a chemistry set.

"Remember, the age-grading isn't about how smart your child is," she said. "It's safety guidance that's based on the developmental skills and abilities of children at a given age, and the specific features of the toy.

Dr. Jerri Rose, associate division chief of pediatric emergency medicine at U-H-Rainbow Babies & Children's Hospital in Cleveland, said it's important to educate older children about safe storage of toys, and make sure younger children are closely supervised.

HIGH-POWERED MAGNETS

In May 2023, a 2-year-old boy required surgery to repair a bowel obstruction caused by two tiny, colorful magnets that he had swallowed.

Two months earlier, in March, a 9-year-old girl had to have tiny, 5 mm magnets removed from her nose at a hospital after she and her friends were simulating nose piercings when magnets went up her nose.

Cases such as these are the reason the CPSC in 2022 adopted new rules for magnets.

The tiny, colorful magnets are often marketed as fidget toys. But they caused 26,600 children to be rushed to hospital emergency rooms from 2010 through 2021, according to the CPSC. At least seven children have died after ingesting high-powered magnets. The problem: if two or more magnets are swallowed, they can connect and pinch internal tissue together and cause serious issues such as intestinal blockage or blood poisoning.

Effective last year, federal standards now require magnets that are loose or able to come out of products to be either too large to swallow or weak enough to reduce the risk they'll connect inside the body if two or more were swallowed. If magnets fail the CPSC's small parts cylinder test – any object fits completely into a test cylinder 2.25 inches long by 1.25 inches wide, then they must have a flux index (a measurement of strength) of less than 50 kG2 mm2.

Despite the new standards, these dangerous magnets are still in many, many homes.

TOY-RELATED INJURIES

The CPSC tracks overall toy-related injuries and deaths involving people of all ages, and provides breakdowns for 14 years and younger, 12 years and younger and 4 years and younger. The statistics reflect people treated in U.S. hospital emergency rooms.

The overall number of injuries increased for 2022, according to a CPSC report released Nov. 14. About 209,500 toy-related injuries were treated in U.S. emergency rooms in 2022.

Of those:

- 76% – about 159,500 – were sustained by children 14 years old or younger;
- 69% were sustained by children 12 years old or younger;
- 38% were sustained by children 4 years old or younger.
- Males accounted for 54% of injuries.

The incidence of injury was greatest among children 4 years old and younger: 432 out of every 100,000. That compares to 267 out of every 100,000 children 14 and younger and 63 out of every 100,000 people of all ages.

About 94% of toy-related injury patients were treated and released.

As for the types of injuries:

- 41% were classified as lacerations or contusions/abrasions.
- 46% were to the head and face area.
- Non-motorized scooters were connected with the largest number of toy-related injuries for all ages among products classified as toys.

There were 11 toy-related deaths among children 14 and younger in 2022: Five were related to balls, including choking on bouncy balls and blunt force trauma to the head. Others involved balloons, stuffed animals or other toys.

There is good news: The numbers of toy-related injuries for children 14 and younger decreased significantly — by more than 10% since 2015, the CPSC said.

Injuries and incidents occur when:

- Toys don't meet standards, such as if they have parts that can easily be removed or break off and be ingested.
- Children get access to a toy not meant for a child their age, such as a small bouncy ball or building blocks.
- Children use a toy in a way that wasn't intended.
- Counterfeit toys are purchased.
- Toys violate our children's privacy.

Toys that don't meet standards or wear over time is the reason parents and caregivers should inspect new toys and consider whether a particular toy is appropriate for their child right now, said Dr. Jerri Rose, associate division chief of pediatric

emergency medicine, at UH-Rainbow Babies & Children's Hospital in Cleveland.

Issues to consider:

- Are there small parts that can break off that the child could put in their mouth? A small part is defined by the CPSC as any object that fits completely into a test cylinder 1.25 wide by 2.25 inches long. The diameter of a toilet paper tube works for a home test. This is about the size of the fully expanded throat of a child less than 3 years old.

- Could a piece of the toy break off easily and produce something sharp that could cut the child or poke an eye?

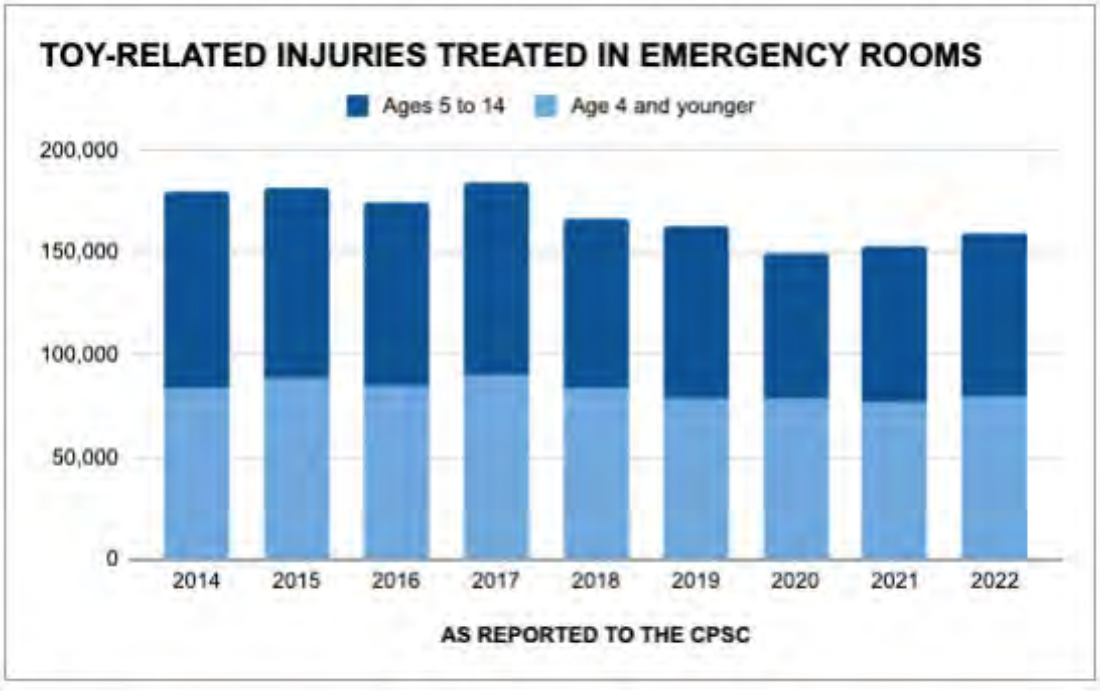
- Does the label say non-toxic?

- What does the label on the box or package say? When a toy is approved and meets standards, it should say what age it's approved for, Rose said.

- If the toy involves electricity, does it say it's UL-approved?

- If there are batteries, especially button batteries, are the compartments secure so they can't be opened by a young child. Screws can come loose during shipping.

- Is your child old enough to play with the toy responsibly? Just because a child is older than 3 doesn't mean he can automatically be trusted to not put small parts in his mouth. Parents know their children best.



RECOMMENDATIONS

- We support the bipartisan COPPA 2.0, introduced this year, which updates the 1998 Children's Online Privacy Protection Act to better protect kids' and teens' privacy online, particularly regarding data collection, advertising and a parent's ability to delete their child's information on file.

- We support the bipartisan TOTS Act, which would require companies that sell high-tech smart toys to clearly label on the box if it contains a Wi-Fi connection and the ability to gather data on children. It was introduced in January 2023.

- We support the Sunshine in Product Safety Act, which would allow the CPSC to warn consumers more quickly about all kinds of dangerous products, including toys, in advance of a recall. It was reintroduced in March 2023.

- We celebrate enactment of the federal INFORM Act, which took effect in June 2023. It's aimed at cracking down on U.S. sellers that allow counterfeiters and thieves. Now we're watching for compliance and enforcement.

- The CPSC should step up enforcement and impose meaningful penalties against merchants that sell counterfeit or recalled toys, or fail to promptly report complaints about product-related injuries.

- The CPSC should get clarity on whether federal law allows online retailers such as Facebook Marketplace and eBay to sell recalled toys without the same multi-million-dollar consequences that regulators impose on brick-and-mortar retailers.

- Toy manufacturers should make a commitment to do a better job of adhering to existing toy safety standards and improving testing.

- Merchants should do more to prevent recalled toys and counterfeit toys from being sold.

- The CPSC should continue to research the risks of phthalates and other toxics often found in toys made of plastic. Phthalates make plastic softer and more flexible.

- Lawmakers should pass stronger data privacy laws, explicitly prohibiting companies from gathering more data from consumers than is necessary to deliver the service a consumer is expecting to get, and use it for any secondary purposes, especially for data that could be generated while using a VR headset.

VIRTUAL REALITY AND META'S QUEST HEADSET

Virtual reality (VR) headsets are growing in popularity, and might be at the top of your child's holiday wish list this year. It makes sense they can be pretty neat. And Meta, the company currently selling the most VR headsets, recently lowered the recommended age in a push to expand to younger users.

PIRG tested both Meta's newest VR headset, the Quest 3, and its new junior accounts for kids ages 10 - 12. We found using these accounts increases parental controls over a child's VR experience – but we also found these new additions fail to eliminate some real concerns.

If your child is asking for one, the child health experts we spoke to recommend exercising extreme caution.

What is virtual reality?

Virtual reality, or VR, refers to a wearable console system that creates a 360-degree computer-generated world. Put on a headset and you're completely surrounded by whatever virtual content you load up, complete with surround sound.

To look at a virtual sky, you look up. To see if there's a virtual someone standing behind you, you turn around. If someone opens a virtual door in the distance, it sounds distant. If someone shoots a gun three feet to your right, it sounds like it went off right next to you. The whole point of VR is that it feels a lot more real than on 2-D screens. Everything is more immersive and more intense.

Meta (formerly Facebook) is a major player in VR, and last month it released its latest model of VR headset, the Quest 3 (currently selling at $499.99). Meta has two other models of Quest headset available for purchase: the Quest 2 (released in 2020, currently $299.99), and the professional grade Quest Pro Mixed-Reality headset (currently $999.99).

Downloading games in Meta's Quest app store lets you use the headset to play 3-D golf or ping pong, fight a sword or light saber battle, get in a bar fight, ride along on the Apollo 11 mission, power wash a house or shoot a sniper rifle as a World War II soldier. You can play by yourself or with others, and use your microphone to have conversations with other players online.

There's no doubt VR can be entertaining, and early studies have shown it can even have therapeutic benefits, such as helping people with phobias do exposure therapy virtually. But there are a lot of unknowns about the technology, and child health experts have raised concerns that parents may want to hear.

Meta is targeting its VR systems to kids

In 2023, Meta has taken steps to increase the youth market of VR users, despite the number of possible risks to children and teens raised by child health experts and lawmakers.

In April, Meta announced it was lowering the age for Horizon Worlds Meta's primary VR social app from 17 down to 13. In June, Meta then announced a change to its user policies lowering the recommended age for using its headsets from 13 down to 10 just two weeks after announcing it would later this year release the new Quest 3 headset in time for the holiday shopping season.

Meta's Quest headsets have struggled to gain widespread traction, and its moves to get more children onto its VR platform come at a time when the impacts of digital content and social media on young users are rightfully getting more scrutiny.

Despite receiving a letter from Senators Ed Markey and Richard Blumenthal, and a petition from more than 70 advocacy groups and child health experts requesting Meta not lower the age for its Horizon Worlds app, as of this writing, Meta has kept Horizon Worlds accessible to anyone 13 and older.

But as Dr. Brett P. Kennedy, a children's clinical psychologist and co-director of Digital Media Treatment & Education Center in Colorado, also stressed in an interview with PIRG that "the lower Meta makes that age, the easier it is for predators to access those kids."

Growing Pains: The health and wellbeing risks of VR technology for children

Virtual reality, like all technology, is a tool. And this tool is very, very new.

"At the risk of sounding cliche, it really is like the wild west," Dr. Kennedy said. Meta itself provides warnings about its Quest 3 headset in the fine print: "Not All Children are Ready For Meta Quest."

All research on VR is in its early stages, since the technology itself is new. There are a lot of unknowns about how VR affects young users' attention spans and developing brains. What we do know is that there are a host of possible harms significant enough that parents might want to proceed with real caution.

We know VR affects the brain—we just don't fully understand how

The little research out there about VR shows there's a need for a lot more studies when it comes to VR and the brain.

For example, in a 2019 interview, UCLA researcher Dr. Mayank Mehta recounted a study he did scanning the brains of rats as they used VR. The rats' brains behaved in really unexpected ways: 60% of the neurons in the hippocampus "simply shut down in virtual reality" and the other 40% fired randomly. Though far from conclusive, this result could mean using VR triggers abnormal brain function, which could possibly cause the brain to rewire itself in unpredictable or even undesirable ways.

Professor Mehta emphasized his study did not conclude anything definitively, either

good or bad. But he added that "the long-term consequences are really hard to measure in the human brain because humans age very slowly."

"We can't wait for 40 years, for teenagers who are today using virtual reality to see what happens to them when they're 60."

Overall, the health professionals we talked to advised parents to stay away for now.

"We know there are potentially big impacts on kids and teens," said Dr. Mark Bertin, developmental pediatrician and Assistant Professor of Pediatrics at New York Medical College, in an interview with PIRG. "The amount of technology in our children's lives is already impacting their mental health. Introducing yet another piece of technology - especially one as novel and engaging as virtual reality - could have real ramifications for the development of long-term social-emotional well being, cognitive skills like focus, and for regulating behavior in general.

Until we know more, it just isn't worth the risk right now."

Physical injury from VR & Meta Quest use

Using a VR headset can cause a number of physical harms, particularly for children.

The headset isn't designed for kids

Quest headsets are not designed to fit a child's body, and it's possible you won't be able to fit it safely on your child.

At just over 1 pound, the Quest 3 is heavy enough it can result in bodily strain to children's developing muscles – particularly their eyes, neck and back.

According to Meta, kids may experience soreness, blurry vision, or other discomforts, and may be reluctant to tell you if it might mean their headset getting taken away. They may also experience headaches or nausea during or after use.

The Quest headset also includes surround 3-D sound and using it at high volume for long periods of time can result in permanent hearing damage a particular concern for young ears. The Quest headset is also getting louder; the Meta Quest 3 has a 40% louder audio range than its predecessor, the Quest 2, making it easier for kids to make things too loud on accident.

Impacts on visual development

Using a VR system may impact your child's vision. Meta's own health and safety standards state that "younger children's visual systems are still developing and may be negatively impacted by using virtual content."

The Quest 3 headset includes adjustable features to get a better fit however only so much can be adjusted to make the system suitable for children. The distance between a child's eyes (known as interpupillary distance, or IPD) may be too small for the headset's lens adjustment range, which in turn increases the risk of blurry vision, eye strain, nausea or headaches.

These risks don't go away in older children. For all users, Meta notes that using the Quest headset may result in eye strain, blurred or double vision and eye or muscle twitching. A PIRG researcher testing the Quest 3 consistently experienced difficulty focusing her eyes for about an hour after each 20-minute session of headset use.

VR feels real - which can have negative effects on young players

One of the biggest draws of VR is just how real and intense the experience can be, especially as compared to 2-D. That is also one of the biggest reasons for parents to proceed with caution.

The early research on VR suggests that the intensity of 3-D virtual content can impact both a player's physiological and emotional state in previously unseen ways. As Meta puts it, users may react to VR experiences "as if it were happening in the physical world."

This has potentially positive benefits for people, such as allowing it to be used to help treat stress-related disorders, like phobias, through virtual exposure therapy.

But one of the pediatricians we talked to emphasized that the power of VR's realness is exactly why its use for commercialized entertainment especially for minors merits real caution.

"If it feels that real, how you use it really matters," Dr. Kennedy said. "While the experience in VR can feel amazing, the negative physical and emotional consequences can be significant and shouldn't be overlooked."

Research about negative impacts is starting to trickle in. A 2021 study found those playing a game in VR reported stronger negative emotions than participants who played the exact same game on a laptop's two-dimensional screen. The VR users' negative emotions lingered throughout the day, well after use.

Meta emphasizes that younger children may have more "intense reactions to virtual content and may have a more difficult time distinguishing virtual content from the physical world, even after they stop use."

Meta's own warning about VR content in its Health & Safety guide.

Violent content feels more real, and can be easily and even accidentally accessed by young players

Because the immersiveness of VR makes everything more intense, parents may be concerned where violence is involved. 3-D games make it feel like you're fighting with real-sized people standing in front of you.

In an interview with CNN, one parent recounted that the violence in a fantasy game played by his 11-year-old son on his Quest headset felt uncomfortably real. And the father knew, the story said, that when his son "looked down in VR he was seeing a weapon held in virtual hands, not just a plastic game controller.

"It bothered me in a way it doesn't on flat screens even, because they're doing it with their hands in physical presence," the parent told CNN.

PIRG's testing also found that kids -- even at age 10 -- can access games with violence relatively easily.

For example, while playing Rec Room – a game rated E for Everyone ages 10 and up in Meta's app store – a PIRG researcher playing as a 10-year-old boy on a junior account was encouraged by the app to explore horror games and first-person shooters.

Though these games took place in relatively cartoonish settings, playing in 3-D makes the experience feel more intense, especially for young players.

More notably, even cartoonish violent play can become disturbing when other people are involved. One Rec Room game recommended to our 10-year-old junior account was the multiplayer game Breaking Point. Shortly after opening the game, our researcher was ushered in to sit around a table in a darkened room with other real players to play Russian Roulette with players pointing guns at one another and choosing which player at the table to shoot.

Within moments, the player seated across from our junior account shot himself in the head, effectively killing his avatar and removing himself from the rest of the round. Our researcher chose Breaking Point to test because, of the games Rec Room was offering our test 10 year old account, it was one that was *not* obviously a horror or first-person shooter game, like other options including Recoil Arena, Survive Mr. Beast and Vietnam Warzone

Parents will have different levels of comfort in the amount of violence their children have access to. Parental involvement in selecting content is extremely important if parents do bring a VR system home. Bottom line: 3-D content is a whole new ballgame and may merit parents revisit what is appropriate for their child with new eyes.

A screenshot of Breaking Point, a game inside the app Rec Room that was recommended to PIRG's test account for a 10-year-old.

Minors can have access to graphic sexual content

Apps available for use on Meta's Quest headsets can be inappropriate for minors and yet easily accessed by young users, including violent or sexually graphic material. "Content that's not developmentally appropriate can be very harmful," said Dr. Bertin, the developmental pediatrician. "You can't unsee things."

A BBC News researcher using VRChat – a prominent app on Meta's app store with a minimum age rating of 13 – posed as a 13-year-old girl and was able to access virtual strip clubs and explicit rooms where players simulated sex. The non-profit group Center for Countering Digital Hate found a similar problem with Horizon Worlds – Meta's own social VR app - with minors present in sexually explicit places like virtual strip clubs, private rooms designed for simulating sexual acts, and bars offering sex toys for players to interact with.

Some of this is due to loopholes. Research and anecdotal evidence shows that there are lots of younger players using parents' accounts or ones for those 18 and older, which makes it easy for players to access mature content. Some of it is a failing of the current content labeling system.

Importantly, the graphic sexual content in VRChat and Horizon Worlds involved interacting with other players, making it potentially dangerous.

Apps hosting player-made content make it more difficult for parents to vet for appropriateness

Some of the most popular apps available for the Meta Quest headsets are multiplayer worlds where anonymous users can create their own games and experiences. Some of these apps are more designed with young

users in mind, such as Roblox. Others, however, are more likely to have age-inappropriate content, including Rec Room, or likely to have graphic content, like Horizon Worlds and VRChat.

After parents allow a child or teen to access one of these apps, helping moderate their experience becomes a much more involved process. For example, Rec Room's Quest app store page boasts "MILLIONS of player-created rooms."

On Rec Room, parents can restrict access to rooms with "mature" content by having their child use the app's junior account. However, other users create each piece of content, and *they* are responsible for setting age restrictions for users under 13 and putting content warnings (such as "gore/violence" or "mature themes") on what they create. As our testing showed, there is no guarantee that user-moderators will set permissions or content warnings that all parents would agree are adequate.

Quest has lots of opportunities to interact with others online

Meta's Quest keeps up the company's emphasis on social media, promising: "Virtual hangouts. Real connection." Indeed, of the most popular games listed in Meta Quest's app store as of this writing, all of the free ones are all also multiplayer.

Similar to conventional social media, people can "friend" your Quest account, and inside of the apps themselves, you can "follow" or add someone as a "friend," enabling you to invite them to join you inside a particular app or talk using microphones or chat features. The Quest sign-up process includes a nudge to link your Facebook or Instagram account to your VR, making it easier for other users to access more information about you and connect in the real world.

Social interaction online can be a positive thing. However, when it comes to kids, VR social interactions come with risks that parents should be aware of particularly that the 3-D and immersive element of VR means that bad interactions with other users can feel more real for your kid or teen.

Profanity and hateful speech

It likely won't surprise parents of kids and teens who play online multiplayer video games with chat and voice features that profanity is a common feature in VR games too.

In PIRG's testing of the popular app Rec Room, for example, our researcher's 10-year-old user with a junior account managed to stumble on bad language, despite the fact Rec Room automatically disables audio for junior accounts. Our fake 10-year-old walked by a whiteboard where a player was repeatedly drawing genitalia and the phrase "s*** my d***".

Unfortunately, hateful speech continues to be an issue in VR multiplayer games as well. The same user at the whiteboard proceeded to write other racially motivated profanity, and someone had already drawn a swastika.

Bullying

In one of the Rec Room games our PIRG 10-year-old junior account tried, we experienced a bit of disorienting bullying. Inside the game Snipers vs. Runners in the Rec Room app, our junior account shook hands with another player, thus becoming friends and able to locate each other inside Rec Room instantly at any point that we were both logged on.

After shaking hands, the other player began to slap the PIRG junior account player repeatedly, following when we tried to move away. The game began another round, separating us from the other player. The moment the round ended, however, all players were dumped back in the waiting room together, and the same player ran up and began slapping our junior account player again. This went on for three rounds before we'd had enough.

Even young users may be able to interact with others inside of apps

As of this writing, Meta's accounts for ages 10 to 12 don't allow your child to use some of Meta Quest's social features like accepting follow requests from other users.

(It's worth mentioning that Meta emphasizes this is the case "at this time" and "for now" so this may very well change in the future.)

However, once a child is inside a particular app, parents may have to set app-specific parental controls restricting social interaction on each app.

PIRG's 10-year-old test account being handed a gift by a stranger inside the app Rec Room.

Meta explains that even if your child is using an account for a 10- to 12-year-old, third-party "[a]pps may have social features such as messaging, voice, photo sharing, video, and the ability to meet and interact with others in the same virtual space, that could allow your child to interact with people they may not know."

In our test of the app Rec Room, for example, our fake 10-year-old user with both a junior Meta and a junior Rec Room account could make friends with other players without approval from a parent, and received in-game gifts from strangers – something which could make some parents uneasy. (It is nice, however, that Rec Room automatically stops its junior accounts from using voice or chat features.)

Sexual harassment and assault

PIRG's 10-year-old junior account player in his hour on Rec Room did not experience any sexual harassment or assault, thankfully. However, other researchers have documented this happening to teen accounts.

The Center for Countering Digital Hate's testing of Meta's own social VR app Horizon Worlds documented minors receiving solicitations to send suggestive photos from adults.

Researcher Rachel Franz at the children's advocacy group Fairplay shared with PIRG her experience testing the app VRChat with a 14 year old girl's account.

"In one word: horrible," she said. Playing on the young teen account, Franz was chased by another player who attempted to sexually assault her avatar.

Franz emphasized the physical realness of VR made the assault attempt a lot scarier. "Being pursued feels real," Franz said. "And the psychological and psychological impact is real. Even after I took the headset off, my heart was racing. That moment has stayed with me."

Franz also said VRChat's function for blocking another user from interacting with you was difficult to use when being chased. "You have to click on a moving target while being chased and having profanities screamed at you," she said. "In that moment, it was practically unusable- and I am an adult with a fully developed sense of coordination."

Fairplay has forthcoming research next year on marketing practices in VR apps available for use with Meta's Quest headsets.

The data privacy risks of VR headsets

VR headsets collect a lot of data, ranging from information we're used to technology gathering – such as our email addresses – to new kinds of sensitive data that previous technologies have not been capable of gathering, such as our eye or body movements. Equipped with sensors, microphones and cameras, VR headsets can gather extensive amounts of data in little time; just 20 minutes using a wearable VR headset generates about 2 million unique recordings of a user's body language.

The World Economic Forum offers a hypothetical of how this VR data could be abused:

Say the developer of a free VR maze game collects data on how players move their body and how efficiently they solve the maze. An insurance company buys this data from the app developer and analyzes the data of a player that just applied for a life insurance policy. Its analysis finds that the player's movements match patterns of people with very early stages of dementia, and denies the player's insurance application. The player had no idea that data was being collected when he played the maze game, let alone that it would be sold to

an insurance company and used to make a decision about his policy.

"This is a hypothetical situation," the World Economic Forum writes. "But the science of using movements tracked in VR to predict dementia, and the technology to do so, are very real. Currently, there are no standards or regulations as to how this data is collected, used or shared."

Meta's Quest headsets can collect a lot of data about you

All editions of the Meta Quest headsets include microphones and cameras. These features help bring VR to life, but they also enable a lot of data collection.

Audio and visual data
Data collected by the Quest headsets can include voice recordings or background sounds in your home. The privacy notice says: "Depending on where you use Voice Commands, the microphone may pick up other sounds in the immediate area beyond your voice including ambient noise or nearby background conversations."

The Quest 3 in particular can gather detailed visual data. This newest version is designed for better mixed reality use. That means overlaying a virtual element onto your physical space, like showing an alien sitting on your couch. To do this, the headset needs to gather data like the dimensions of your room and the placement of your furniture. If misused, that information can communicate a lot about your family such as where you shop and how much money your family has.

Sensitive movement data
Quest headsets also use cameras and sensors to gather movement data about you, like your headset's position and orientation and how you move the hand controllers. This allows it to simulate your movements virtually. It translates your actual body movements to allow your avatar to move the same way. But movement data can be very revealing.

For example, researchers in a 2023 UC Berkeley study were able to identify a single person out of a database of more than 50,000 people, with 94% accuracy, using only 100 seconds of an individual's head and hand motion data collected using Meta's VR game Beat Saber.

The study concludes that using VR motion data could identify people as accurately as fingerprints do.

PHOTO: PIRG EdFund
The Quest 3 headset has six cameras, four of which you can see here.

A different 2023 UC Berkeley study found that using just a few minutes of a player's movement data collected through a VR escape room game, researchers could infer a player's geolocation, their age and physical fitness level and physical or mental disabilities. As the researchers point out, malicious actors could easily set up an innocent looking VR game and harvest lots of data from players. Because of the immersiveness of VR games, it would also be easy for a game to be designed to encourage players to take certain actions in order to gather better data about, say, their reaction time or size of the player's room. With little to no regulation around how VR companies can use movement data, parents may want to be aware of the sensitivity of VR-generated data before bringing a system home.

Third-party apps may gather excessive data about you

Whenever apps gather excessive information from us and sell or share it with other companies, it increases the odds our data will be exposed in a breach or a hack.

Apps on your phone or tablet are notorious for collecting lots of unnecessary data, including data about children. Apps available in Meta's VR app store can collect a lot, too.

For example, the free and popular VR app Rec Room, which we tested, states in its privacy policy it may collect "your first, middle and last name, email address, username, mailing address, Social Security number or employer identification number, telephone number, IP address, or display name" among other things.

In order to know what a VR app is gathering on you or your child, you need to review its privacy policy – and each app will have its own fine print. Each app will likely also have its own privacy settings that may by default gather more information than you're comfortable with, so you may want to check the settings on every app your child uses too.

Parents should be particularly cautious about free apps. The saying about other online products is probably also true for VR apps: If the product is free, then you – and your data – are probably the product.

Other users can collect data about you and your child through apps on Quest

Some apps allow users to take screenshots and recordings of virtual spaces and save them to their account for private viewing or later sharing. This means your avatar and voice may appear in other people's screenshots or recordings.

This is true even if you have the highest privacy settings, and is true even for the youngest children's accounts, for ages 10 to 12.

TIPS FOR A QUEST VR HEADSET

Overall, the experts we spoke to recommend you avoid allowing your child to have a Quest VR headset this holiday season.

The technology is in its very early days and there's a lot of research to be done by both Meta and independent researchers to evaluate whether VR is safe for developing brains. "We know there are potentially big impacts on kids and teens," said Dr. Bertin. "Until we know more, it just isn't worth the risk right now."

Before you bring it home:

Try it out yourself. Use Meta's search tool for stores such as Best Buy that have Quest headsets available for testing. Getting a sense of what immersive 3-D content feels like will help you decide whether your child can handle it. Try a game with a level of violence you'd be OK with your child playing on a 2-D screen, and see how it feels to you. Also consider taking your kid along to make sure the headset will actually fit well enough on your child they'll be able to use it.

During set up:

- Let it sit out of the box for a bit before you use it right away. The plastic smell can be intense.

- **If you have a 10- to 12-year-old, create their own junior account for them.** These accounts have more restrictive settings and parental controls that will help keep your kid safer. Meta will require you to set up an adult account first, and then use a second email address to set up a junior account. It may seem like an annoying extra step, but it's worth it for the safety features.

- **If you've bought the headset for your teen**, help them set up a Meta account that's separate from your child's existing Facebook or Instagram account. This will help limit strangers' abilities to learn more about your teen or contact them outside of VR.

- **Take advantage of the parental control features immediately.** In the Family Center, you'll be able to set time limits, windows where the headset is off limits and restrictions on in-app purchases, and block your child or teen from downloading certain apps all together. For kids under 13 we suggest blocking Rec Room, and for all minors blocking Horizon Worlds and VRChat.

During play:

- **Start small and take it slow.** The experts we spoke to recommend to start with short periods of use, introduce one app at a time and test it together first.

- **Do your research every time you add a new app.** Look at the app's listing in the Meta apps store and check the age rating, whether it includes in-app purchases and whether it has multiplayer interactions. You might want to be particularly careful about apps where your kid can interact with others. Look and see what parental controls the app offers. Can you shut off the microphone or chat features? You can also look at the reviews other players have left. Some may raise useful flags.

  Finally, look at the app's privacy policy. Is there anything there that gives you pause? Use our guide on how to ready a privacy policy to help you find flags.

- **Restrict headset use to shared spaces in your home.** You might not be able to look over their shoulder as easily if they are playing on a desktop, but you can still get a sense of the experiences they're having if you can see and hear them.

- **Take advantage of the casting feature.** Especially for younger users, make play something that happens together by casting what your kid is seeing in their headset to your TV or phone.

- **Make sure your child is playing only when logged into their account – not yours.** Both research and anecdotal evidence show that there are plenty of minors using an adult's account with the Quest headset. It's a lot easier to find or stumble on sexually graphic content this way, and to have voice and chat interactions with other players online in graphic spaces.

- **Monitor your child's mood after VR sessions.** Do they seem more irritable or on edge? Amped up and having a hard time winding down? More withdrawn from their surroundings? Noticing changes in your child is important for making sure the experiences they're having are appropriate, and will make conversations with them about their experiences more helpful.

TIPS FOR EVERYONE WITH ALL TOYS

- Carefully check toys, both when they're new and every so often, to see whether there's wear and tear. Look for loose parts that could easily break off and be swallowed or cut your child.

- When your child gets a new toy, and periodically after that, check whether the toy has been recalled. Go to cpsc.gov/recalls. Check for incidents as well as recalls at saferproducts.gov

- Evaluate whether particular toys are appropriate for *your* children, starting with the minimum age warning label. Even if your child is "old enough," they may not be able to be trusted to play with the toy as intended.
  "Remember, the age-grading isn't about how smart your child is—it's safety guidance that's based on the developmental skills and abilities of children at a given age, and the specific features of the toy," said Joan Lawrence of The Toy Association. Also consider whether your child is also responsible enough to keep the toy out of reach of any younger children.

- Be leery of toys from unfamiliar sellers or international sellers. They may be more likely to sell counterfeit toys or toys that don't meet U.S. safety standards.

- When researching a toy, check whether the manufacturer has its own, official website. "We always tell toy shoppers that if they are not familiar with an online seller, simply do a bit of research," Lawrence said. "If there are a lot of typos and grammatical errors or poorly photoshopped images, it's likely that the product is a counterfeit or imitation toy.

- Look for labeling on toys that says it's non-toxic.

- Make sure that anything that's electric says it's UL-approved.

- Vintage toys are great for the memories, but be wary of toys made before 2008, when the Consumer Product Safety Improvement Act took effect. Toys that comply with that law are safer in many ways. The law set new limits on lead, phthalates and heavy metals, and requires third-party testing to make sure toys meet ASTM F963-17, which is the Standard Consumer Safety Specification for Toy Safety that covers a range of potential hazards in toys.

- For scooters, hoverboards and other riding toys, require your child to wear safety gear – particularly helmets that fit properly, said Dr. Jerri Rose, associate division chief of pediatric emergency medicine, UH-Rainbow Babies & Children's Hospital in Cleveland.

- Make sure they know how to ride on streets shared by vehicles that can injure or kill them. Just because a child is a certain age doesn't necessarily mean they can be trusted, Rose said.

- Report incidents involving toys to the CPSC at saferproducts.gov

TIPS FOR YOUNGER CHILDREN

- For any toys with plastic film coverings on toys to protect them during shipping, be sure to remove the film. It's often found on mirrors or parts that can be scratched before use. It can pose a choking hazard to children.

- Keep small balls, blocks and other toys with small parts out of reach from children younger than 3.

- High-powered tiny magnets are now prohibited from being manufactured. But the new federal rule doesn't affect magnets that may be in people's homes. If you have children or teens in your home, you shouldn't have tiny magnets, the American Academy of Pediatrics says. Also explain to your kids how dangerous these magnets are, in case they come across them at a friend's house.

- Certain types of water beads haven't yet been banned, but they're dangerous for young children.

- Keep deflated balloons away from children younger than 8 and keep your ears open for an inflated balloon that pops. Children can choke on balloons that haven't been blown up and ones that have broken.

- For children younger than 18 months, keep them away from toys with any strings, straps or cords longer than 12 inches.

- If there are batteries, especially button batteries, make sure the compartments are secure and can't be opened by a young child. In addition, make sure to never leave new or used batteries where children can reach them.

- Watch out for painted jewelry, cheap metal or other toys with paint that seems to chip off easily. We know young children often put things in their mouths. The objects could contain lead, which is particularly harmful to children's developing brains and nervous systems.

TIPS FOR PARENTS ON DRONES

Drones have become increasingly popular in recent years. However they come with their unique set of concerns. They come with special legal restrictions, like possible registration requirements with the Federal Aviation Administration.

To protect children when using drones, parents can consider these issues:

- **Drone size:** Choose the right size drone for your child. Larger heavier drones will have faster and heavier propellers and may be more difficult to control and a problem for younger children.

- **Pets and wildlife:** Teach your child to keep their drone a safe distance from all animals (domestic and wild). The noise and movement may make an animal anxious or agitated, risking harm to all involved.

- **Registration:** Depending on the drone you buy and if it is over a certain weight, it must be registered, and the user must adhere to specific guidelines. The Federal Aviation Administration (FAA) oversees drone rules but states and localities may place additional restrictions. The FAA requires all drones that weigh greater than 0.55 lbs (250 grams) to be registered.

- **Age restrictions:** Research whether there is a minimum age for drone pilots in your area. Ensure your child meets the legal age requirements or that they are supervised by an adult if necessary.

- **Privacy:** Parents should supervise and educate their kids on privacy considerations. Privacy breaches can lead to legal consequences, so it's essential to fly drones responsibly and ethically.

- **Boundaries:** Make sure your kid understands where is and isn’t appropriate for flight. Avoid areas with heavy traffic, airports or private properties without permission.

TIPS FOR PARENTS ON ROBLOX

Roblox offers a creative and engaging online platform for kids to design games, interact with friends and unleash their creativity, but it's not without its potential dangers.

Roblox hosts user-made content, which can sometimes be explicit or violent. It also allows other players to interact with one another; earlier this year an 11-year-old girl from Delaware was kidnapped from her home by an adult who communicated to her through Roblox. It also contains in-app purchases, and some experts have raised the alarm that it might be addictive for some kids.

To protect children, parents can:

- **Use customized parental controls:**
  Use features that restrict chat capabilities, set spending limits and enforce account restrictions. Make sure only approved friends can join your child's games.

- **Teach your child about in-app purchases:**
  Children should learn about in-app purchases and the real costs associated with virtual items. Explain the importance of getting permission before making any purchases. Set spending limits inside the app.

- **Educate children about privacy:**
  If your child is going to play on Roblox with others, they should be told to limit interactions and not share details such as their real name, location or age. Parents may want to take an interest in their child's gaming experience, particularly if their child is reporting any new friends or regular acquaintances in the game.

TIPS FOR PARENTS ON SMARTWATCHES

Smartwatches may provide entertainment for kids and peace of mind for parents hoping to have a way to communicate with their child before making the jump to buying a smartphone. There are some security and privacy considerations for parents and guardians. For example, testing of some brands has shown security vulnerabilities that could expose real-time location data. Others can include features like calorie counters that some have questioned as encouraging unhealthy behavior in children.

To protect children, parents can:

- **Research up front:** Look for flags that a smartwatch manufacturer has had trouble with safety and security previously. For example, Mozilla Foundation's Privacy Not Included website reviews products including smartwatches that can be helpful. They've flagged the Huawei Watch Kids 4 Pro and the Verizon GizmoWatch as having less than ideal data practices.
- **Evaluate features:** Determine which features are essential for your child. Consider factors like GPS tracking, communication, games and apps, and decide how comfortable you are with each. Some smartwatches have features like calorie counters, which some have raised could shift kids' focus from healthy play to obsessive tracking behaviors.
- **Privacy controls:** Prioritize smartwatches with robust privacy controls. Make sure the watch has settings to restrict location sharing and limit access to sensitive data.
- **Parental monitoring:** Choose a smartwatch that gives you the parental controls you're hoping for, such as tools for checking your child's location or time limits on games. Many smartwatches offer companion apps for parents to stay connected and informed.
- **Data protection**: Verify how a smartwatch handles and stores data by using Ctrl + F on Windows or Cmnd + F on IOS when reading a watch's privacy policy. Search for the terms "data" or "security" to find how that company uses data. For further guidance on deciphering privacy policies, see PIRG's guide.

TIPS FOR PARENTS ON SMART SPEAKERS

Smart speakers such as Amazon Echo, Google Nest and Apple HomePod have become common in American households, offering convenience and entertainment. However, they also raise some real concerns.

Smart speakers are known for their data collection capabilities, and different companies have different policies. In 2023, Amazon paid $25 million to settle FTC and DOJ allegations it had violated COPPA for failing to delete young users' voice and geolocation data collected by its smart speakers.

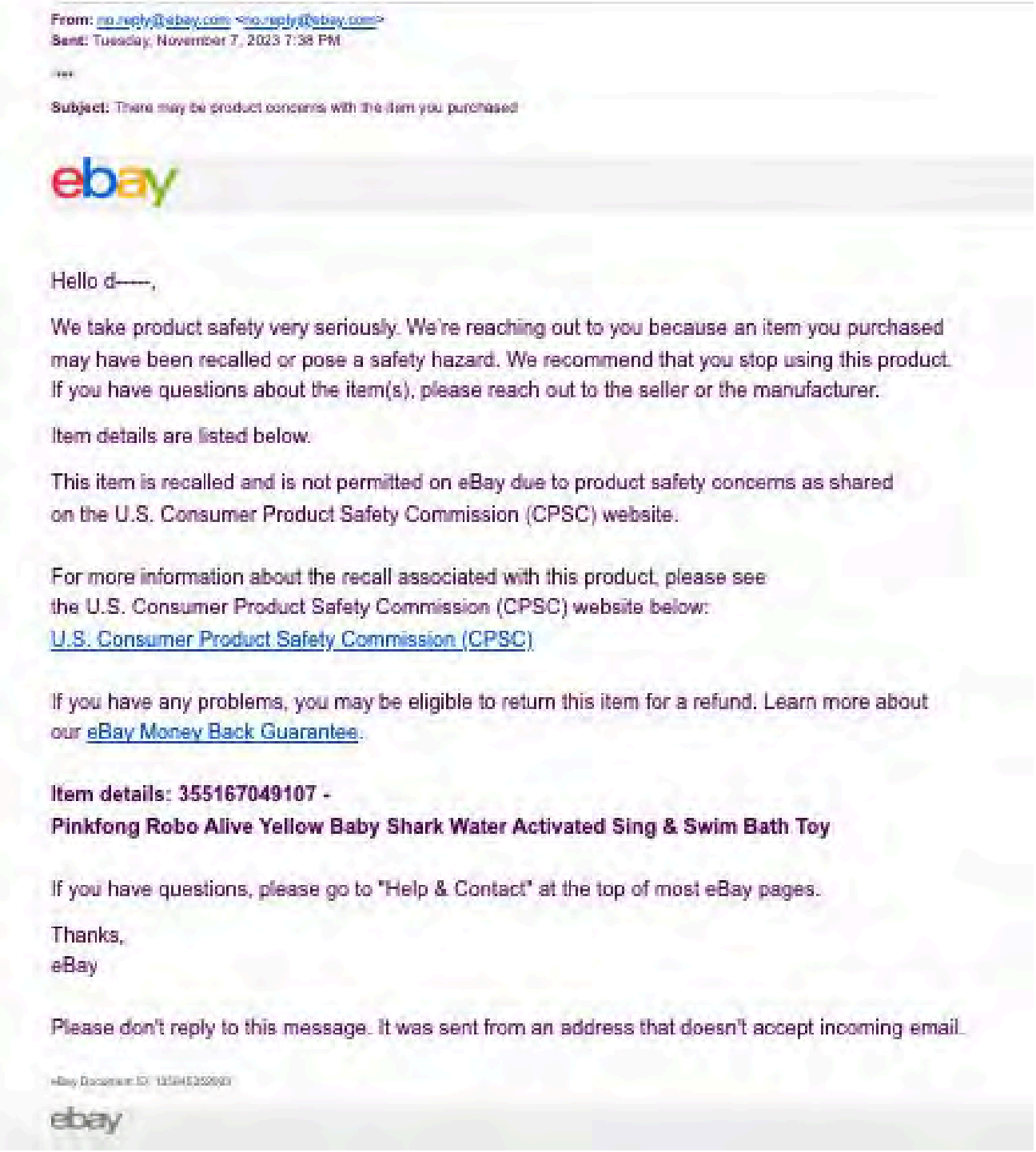
Because smart speakers can access the internet, kids may request or encounter inappropriate content. In one case, academic researchers were able to smuggle 234 policy-violating skills onto the Alexa Skills Store, the marketplace for third-party apps on the Echo smart speaker. Kids have also accidentally spent a lot of money while talking to a smart speaker. One 6-year-old spent $160 by simply asking her Amazon Echo device: "Can you play dollhouse with me and get me a dollhouse?"

To protect children when using smart speakers, parents can:

- **Enable parental controls:** Most smart speaker platforms offer parental control features that allow parents to restrict access to explicit content and certain features.
- **Review voice history:** Periodically review voice command history and any recorded conversations to ensure your child's privacy is protected and submit deletion requests.
- **Put the smart speaker in a communal place:** This makes it easier to monitor how your child interacts with the speaker.
- **Disable voice purchasing:** To avoid disable voice purchasing or require a PIN or password for purchases. This extra layer of security can prevent unexpected charges.
- **Regularly update firmware:** Keep the smart speaker's firmware up to date. Manufacturers often release updates that can enhance security and privacy features to prevent the risk of cyber attack stealing your or your kids' data.

APPENDIX

Ebay is one of the online sellers that list all types of products that have been recalled. You can buy them and receive them. *Then* Ebay sends you an email and says, oops. Clearly they can identify these listings. Why don't they do this before they're sold, not after?



From: no.reply@ebay.com <no.reply@ebay.com>
Sent: Tuesday, November 7, 2023 7:38 PM

To:

Subject: There may be product concerns with this item you purchased

ebay

Hello d-----,

We take product safety very seriously. We're reaching out to you because an item you purchased may have been recalled or pose a safety hazard. We recommend that you stop using this product. If you have questions about the item(s), please reach out to the seller or the manufacturer.

Item details are listed below.

This item is recalled and is not permitted on eBay due to product safety concerns as shared on the U.S. Consumer Product Safety Commission (CPSC) website.

For more information about the recall associated with this product, please see the U.S. Consumer Product Safety Commission (CPSC) website below:
U.S. Consumer Product Safety Commission (CPSC)

If you have any problems, you may be eligible to return this item for a refund. Learn more about our eBay Money Back Guarantee.

Item details: 355167049107 -
Pinkfong Robo Alive Yellow Baby Shark Water Activated Sing & Swim Bath Toy

If you have questions, please go to "Help & Contact" at the top of most eBay pages.

Thanks,
eBay

Please don't reply to this message. It was sent from an address that doesn't accept incoming email.

eBay Document ID: 135945355993

ebay