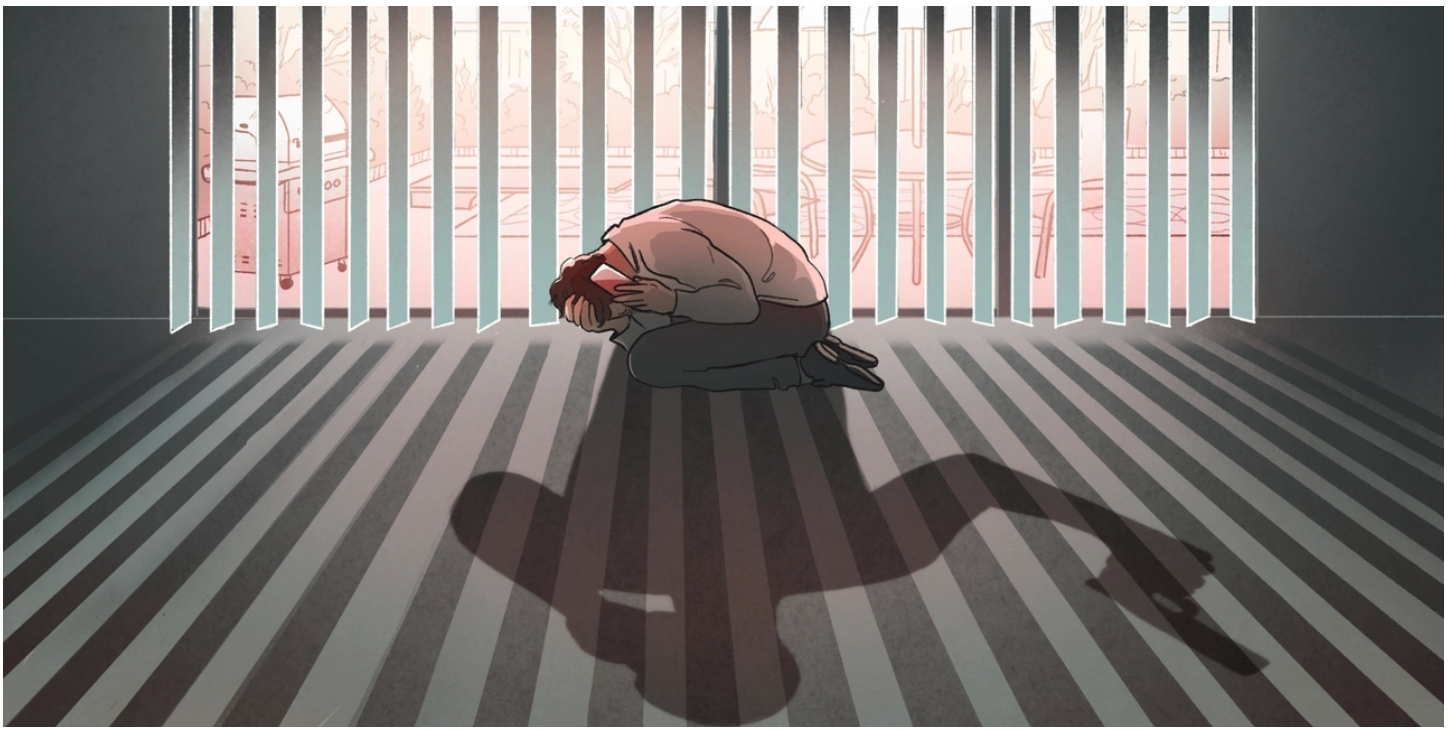
NEWS

'We have your daughter': The terrified father paid the ransom. Then he found his kid where he least expected her.

Criminals are staging a devious new kind of kidnapping — and the FBI is stumped.



Richard Mendelstein is hypercautious about digital security. But all his skepticism flew out the window when he heard his daughter crying for help on the phone. Vicky Leta/Insider

David Kushner

Last year, at about 11 in the morning on July 29, Richard Mendelstein was working in his home office in Princeton, New Jersey, when his phone rang. The caller ID read "unknown."

Mendelstein, a soft-spoken 56-year-old software engineer at Google, is hypercautious about his digital security. He wipes cookies from his web browser, stores his passwords in an encrypted file, and checks incoming emails for phishing ploys. "I question everything," he says. He even answers calls from unknown numbers just so he can report telemarketing scams to the Federal Trade Commission.

But this wasn't a robo-caller looking to sell him discount car insurance or consolidate his loans. On the other end of the line, Mendelstein heard a girl sobbing in fear. His stomach dropped. His daughter, Stella, was a junior at Northeastern University. He could barely make out her words through her tears. He asked her to repeat herself.

"They kidnapped me!" she screamed. "Dad, please help!"

Then he heard someone grab the phone. A man with a deep, clear voice spoke.

"Listen very carefully," the kidnapper told Mendelstein. "We have your daughter. If you do exactly as I say, nothing will happen. I just want money."

Mendelstein's heart pounded as the kidnapper told him to follow his instructions to the letter. "Don't hang up," the

man said. "Don't talk with anyone. Don't take any calls. Don't text."

Just then, Mendelstein's wife, Rachel, walked in. She'd heard him on the phone sounding distressed, and came to check on him. "Are you OK?" she asked. But Mendelstein was afraid to respond, given the kidnapper's instructions. The caller told him to go outside, get in his car, and drive to a bank. *This was real. This was happening*. If he ever wanted to see his daughter alive again, it was time to get the ransom money.

The kidnapper kept him on the phone as he sped through the streets, ordering him to name the roads as he passed them. As Mendelstein reported on his progress — *Nassau, Witherspoon, Hulfish* — he declined the barrage of frantic calls and texts from his wife, afraid of making the slightest misstep. He was all adrenaline now.

Arriving at the bank, he filled out a withdrawal slip for $4,000, the ransom amount the kidnapper specified. Mendelstein didn't know why the number was so low, or what would happen next, but the kidnapper told him to not ask questions. Just withdraw the cash, and he would be directed where to take it.

Mendelstein, in a flash, decided to take a gamble. With a shaky hand, he scribbled a quick note. "My daughter has been kidnapped," he wrote, along with the number of the kidnapper, and the name and number of his wife.

Then, before he could hand the note to the teller, the call

abruptly cut off.

Terrified, Mendelstein ran outside and sped to the nearest police station. On the way he called his wife. "Stella's been kidnapped," he told her.

"What?" Rachel screamed. "How do you know?"

"Because I spoke to her," he said.

Just then, as he pulled into the parking lot of the Montgomery Township Police Department, the kidnapper called back. Mendelstein hung up on his wife to take the call.

Cut off from Richard and frenzied with fear, Rachel tried calling Stella. To her shock, her daughter picked up. She was safe and sound at school, she said.

Reeling from confusion, Rachel didn't know what to believe. Fearing that the kidnapper had a gun to Stella's head, Rachel demanded to FaceTime her, to make sure she was OK. Even when she saw her daughter on the screen, seemingly happy and relaxed, she still wasn't certain. She told Stella to get a friend to come to the phone as well.

"Dad said you've been kidnapped," Rachel gasped.

"What?" Stella said. "I'm fine!"

Rachel sobbed with relief. Stella *was* fine. Then her thoughts turned to Richard. In a panic, she phoned the

police, desperate to reach her husband and give him the news. When she finally reached an officer, he listened calmly to her story. He didn't seem surprised. "This is most likely a scam," he told her.

But that wasn't the most pressing issue. "Where is your husband?" the officer asked.

"I don't know," Rachel replied. She and Stella feared the worst. Who was on the phone with Richard? Where was he being sent with $4,000 in cash? And what were the criminals going to do with him after they got the money?

The kidnapper told him not to talk to anyone, but Mendelstein took a gamble and tried to tip off the bank teller.
Vicky Leta/Insider

About 10 years ago, when Erik Arbuthnot first started hearing about phony-kidnapping hustles, his fellow agents at the FBI scoffed at the cases. "Don't worry about those," they told Arbuthnot. "Those are fake. We handle the real ones."

Now the cases have become so widespread that the bureau has a name for them: virtual kidnappings. "It's a telephone extortion scheme," says Arbuthnot, who heads up virtual-kidnapping investigations for the FBI out of Los Angeles. Because many of the crimes go unreported, the bureau doesn't have a precise number on how widespread the scam is. But over the past few years, thousands of families like the Mendelsteins have experienced the same bizarre nightmare: a phone call, a screaming child, a demand for ransom money, and a kidnapping that — after painful minutes, hours, or even days — is revealed to be fake. There's the pastor in Memphis who, like Mendelstein, was told his daughter had been kidnapped. The man in Miami who thought his wife and baby daughter were being held for ransom. The guy in Missouri who got conned into thinking his elderly mother had been taken. Overall, the FBI reports, internet scams nearly doubled in 2020 — and extortion cases like virtual kidnapping have rung up the third-most victims, right behind phishing schemes and phony sales calls.

What Arbuthnot calls the "explosion" of kidnapping hoaxes started in the summer of 2015. A detective in Southern California contacted the FBI about a string of fake kidnappings targeting residents of his upscale precinct in Beverly Hills. One woman received a call

telling her that her 20-year-old daughter was being held for ransom. "I hear what sounds like my daughter hysterically crying, screaming, out of breath, like she's in duress," the woman, who asked not to be identified, later recalled. "I barely can understand the words, but I made a semblance of the fact that she was saying she was in a van and she was kidnapped, and I'm hysterical." While withdrawing the ransom money from the bank, the woman had the same idea as Mendelstein: She slipped a note to a bank employee, who contacted the police. The cops quickly determined it was all a con.

Valerie Sobel, a Beverly Hills resident who runs a charitable foundation, also received a call from a man who told her he had kidnapped her daughter. "We have your daughter's finger," he said. "Do you want the rest of her in a body bag?" As proof, the kidnapper said, he was putting her daughter on the phone. "Mom! Mom!" she heard her daughter cry. "Please help — I'm in big trouble!" Like Mendelstein, Sobel was told not to take any other calls. After getting the ransom money from her bank, she was directed to a MoneyGram facility, where she wired the cash to the kidnappers — only to discover that her daughter had never been abducted.

The cases weren't just terrifying the victims; they were also rattling police officers, who found themselves scrambling to stop kidnappings that weren't real. "They're jumping fences, they're breaking down doors to rescue people," Arbuthnot tells me. The calls were so convincing that they even duped some in law enforcement. Shortly after Arbuthnot started investigating the calls, a Los

Angeles police sergeant named O.C. Smith was driving down the freeway when his phone rang. "Daddy, Daddy, help me!" he heard his daughter cry. "I'm in a van being taken somewhere!" The kidnappers demanded $1 million or they'd "put a bullet in the back of her head." While Smith was negotiating with the kidnappers, he had the presence of mind to ask a fellow officer to check with his daughter. She turned out to be safe at school.

But whoever was behind the schemes, and how they were pulling them off, remained a mystery. The feds were stumped. "I had no idea who was making the calls," Arbuthnot says.

In Princeton, Richard Mendelstein's family didn't know where he was or what had happened to him. They assumed he was delivering the ransom money to the kidnappers, whom they feared would be waiting for him at the drop location. "Everyone was nervous," Rachel recalls. "None of us knew who was behind it." They dispatched their friends to various locations across town, hoping they'd be able to spot Richard's car and stop him before it was too late. The police, meanwhile, were working with Verizon to track Richard's cellphone.

As the drama unfolded, word spread through town. I know the Mendelsteins, whose names I've changed at their request to protect their privacy. When I heard their story, it hit especially close. When I was 4, my 11-year-old brother,

Jonathan, was kidnapped and murdered by two strangers. It took me decades to unravel the trauma, as I chronicled in my memoir, "Alligator Candy." I know firsthand what it feels like for a family to go through something so terrifying, and I reached out to the Mendelsteins as soon as I heard the news.

In Princeton, friends and family members rallied to help locate Richard. Rachel discovered, to her surprise, that other people she knew had also been victimized by virtual kidnappers. Her sister had a friend who was told her daughter had been kidnapped while studying in Australia, and her brother-in-law said his father had been tricked into believing his grandson had been abducted. To the Mendelsteins, it felt like telling their friends their emails had been hacked: Suddenly, everyone had a similar story to tell.

As news of the fake kidnapping circulated around Princeton, so did the rumors. An hour or so after the ordeal began, Stella got a call from a cousin who said she'd heard the kidnappers had gotten into Richard's bank account. She feared they might be with Richard, forcing him to follow their orders at gunpoint.

"That was when I broke down," Stella recalls. "Because I thought they were together."

"Dad!" the girl cries in tears. "Dad! Dad! Dad!"

I'm listening to a recording of a virtual kidnapping that Arbuthnot is playing for me, to demonstrate just how harrowing the calls can be. "It begins with the crying," he says. "That's what most people hear first: *Help me, help me, help me, Mommy, Mommy, Daddy*."

Virtual kidnapping calls, like any other telemarketing pitch, are essentially a numbers game. "It's literally cold-calling," Arbuthnot tells me. "We'll see 100 phone calls that are total failures, and then we'll see a completely successful call. And all you need is one, right?"

The criminals start with a selected area code and then methodically work their way through the possible nine-digit combinations of local phone numbers. Not surprisingly, the first area where the police noticed a rash of calls was 310 — Beverly Hills. But it's not enough to just get a potential mark to pick up. Virtual kidnapping is a form of hypnosis: The kidnappers need you to fall under their spell. In hacker parlance, they're "social engineers," dispassionately rewiring your reactions by psychologically manipulating you. That's why they start with an emotional gut punch that's almost impossible to ignore: a recording of a child crying for help.

The recordings are generic productions, designed to ensnare as many victims as possible. "They're not that sophisticated," Arbuthnot tells me. It's a relatively simple process: The criminals get a young woman they know to pretend they've been kidnapped, and record their

hysterical pleas. From there, the scheme follows one of two paths. Either you don't have a kid, or suspect something is amiss, and hang up. Or, like many parents, you immediately panic at the sound of a terrified child. Before you can form a rational thought, you blurt out your kid's name, if only to make sense of what you're hearing. *Lisa?* you say. *Is that you? What's wrong?*

At that point, you've sealed your fate. Never mind that the screams you're hearing aren't those of your own kid. In a split second, you've not only bought into the con, but you've also given the kidnappers the one thing they need to make it stick. "We've kidnapped Lisa," they tell you — and with that, your fear takes over. Adrenaline floods your bloodstream, your heart rate soars, your breath quickens, and your blood sugar spikes. No matter how skeptical or street-savvy you consider yourself, they've got you. "They're absolutely expert social engineers from the beginning," Arbuthnot says.

Once you're under their command, your panic may drive you to offer up additional details the kidnappers can make use of, like your last name or home address. Now, thanks to Google, they know you're Lisa's mom, Angela White. You live in Sherman Oaks, you work at Home Depot, you belong to the Mayberry Church, the name of your son is Max, and we're coming for him next.

It's literally cold-calling. We'll see 100 phone calls

that are total failures, and then we'll see a completely successful call. And all you need is one, right?

- Erik Arbuthnot, FBI agent

The other elements of virtual kidnappings are taken straight from the playbook for classic cons. Don't give the mark time to think. Don't let them talk to anyone else. Get them to withdraw an amount of cash they can get their hands on right away, and wire it somewhere untraceable. Convince them a single deviation from your instructions will cost them dearly.

In some cases, the kidnappers have even used a cold call to make the victim think that someone who is with them in the room has been abducted. Arbuthnot recalls the convoluted case of a California auto mechanic and his wife who went on vacation in Tijuana. They had just checked into their hotel when the phone in their room rang. The caller told them that he was from the Sinaloa cartel and that the couple was suspected of working with a rival gang. "You're in our territory now," the caller warned.

The mechanic protested that he wasn't a drug dealer — he was just an American on vacation with his wife. The caller told him to prove it. "Put her on the phone," he ordered. Then, having thrown the couple off balance and secured their cooperation in a seemingly minor request, the caller raised the stakes. "If you're not a member of the rival cartel," he told the wife, "then do what I say and you won't get hurt. But if you aren't willing to cooperate, we're going to come get you."

The next step was to separate the couple. While the wife stayed on the phone with the caller, the husband was ordered to go downstairs, get in a green taxi he would find parked in front of the hotel, and tell the driver to take him to a nearby convenience store. Never mind that there are green taxis outside every hotel in Tijuana — the effect led the mechanic to believe he was being watched. Once he arrived at the convenience store, the caller told him to buy a prepaid cellphone and throw away his own phone. The burner phone was now his lone link to the outside world — and no one but the kidnappers had the number. "Now they've isolated him," Arbuthnot says. "The only person who can talk to him are the bad guys." They ordered him to withdraw money from an ATM and wire them the cash.

His wife, meanwhile, was ordered to go to another hotel, check in to a new room, and ditch her cellphone. The husband, who had been instructed to return to their original hotel room, had no idea where his wife had been taken and had no way to contact her. Cut off from each other, both of them believed their spouse had been abducted by the cartel. With a single phone call, the con artist had initiated not one but two virtual kidnappings.

The level of psychological manipulation grew perverse. The kidnapper called the wife in her new hotel room, then ordered her to turn on a porn channel and take off her clothes. He said he had a video camera in the room and was watching her. If she didn't follow his instructions, he said, her husband would be killed. "Now touch yourself," the caller ordered. She complied.

The caller told the mechanic and his wife to call people back home for more ransom money. "He's calling her family saying she's been kidnapped," Arbuthnot recalls. "And she's calling his family telling them he's been kidnapped." Several family members fell for the ploy, wiring thousands of dollars to the kidnappers. The ordeal continued until one relative finally contacted the authorities. Nearly eight hours after the nightmare began, the wife heard someone pounding on her hotel door. She opened it to find two FBI agents, who had been dispatched by the US Consulate. "You're OK," they assured her. "You're not kidnapped."

Some elements of virtual kidnappings are taken straight from the playbook for classic cons. Don't give the mark time to think. Convince them a single deviation will cost them dearly. Vicky Leta/Insider

While Richard Mendelstein barreled up a highway in New Jersey with the ransom money, ignoring his family's desperate attempts to reach him, it seemed as if he were trapped in a movie thriller. The caller was sending him 20 minutes north of Princeton, to the town of New Brunswick. *Left here, right here.* The kidnapper knew the streets, knew exactly where he was sending Richard, which only ratcheted up Mendelstein's terror. *Would the kidnapper be there when he arrived? And would he get there fast enough to save his daughter?*

The caller directed him to a money-wiring center in a sketchy part of town and gave him the details on where to send the cash: to a money-wiring center in Mexico City. Mendelstein did as he was told. Then, once the transfer was complete, he decided to check his texts. One of the first to pop us was from his friend Steve. Stella was fine, Steve told him. She hadn't been kidnapped. The whole thing was a scam.

A scam? Mendelstein read the word over and over again, struggling to comprehend what was happening. A quick phone call to Rachel confirmed the truth: The whole thing had been a hoax. When I ask Richard how he felt, he blinks numbly, still frozen from the shock of it all. "I don't remember," he says, quietly. "It was a relief that it wasn't real."

But the police didn't want him to leave the money-wiring center. Even though Stella was safe, the criminals could still have been trailing Mendelstein at that very moment.

"They thought somebody might be watching me," he recalls, "and that maybe there was a local person involved."

There was reason to be cautious. In 2017, the FBI had received a call from a sheriff in Texas. "We're having these weird things happen," the sheriff said, "these extortions." Virtual kidnappers were targeting phone numbers in The Woodlands, a community outside Houston that was rich in oil money. The criminals had persuaded one family to pay a ransom for their daughter, who was away at college. Crying and hysterical, the mother had sped past the town's mansions and estates, following the directions to a neighborhood school. Once there, she was told to get out of the car, take the paper bag she had stuffed with $25,000 in cash, and drop it in a trash can on the playground.

That's where one of the criminals made a pivotal mistake. When a woman came to the school in person to retrieve the money, a surveillance camera caught the license plate of her black pickup truck. Before long, a SWAT team stormed the woman's house and arrested her.

Her name was Yanette Rodriguez Acosta, and she turned out to be the girlfriend of Ismael Brito Ramirez, a 38-year-old who was serving time in Mexico City on murder and kidnapping charges. While in prison, Ramirez had decided to move into virtual kidnapping. Fake abductions had been going on in Mexico for years, a lucrative racket for street gangs and drug cartels. Those kidnapping calls, however, all involved Spanish-speaking criminals and Spanish-speaking victims. Ramirez, who spoke English in

a clear American accent, wanted to export the scam to America.

Ramirez smuggled some burner phones into the prison and set up a system for collecting ransom payments. His victims were ordered to wire cash to Mexico City, where mules would be waiting to pick up the money and deliver it to Ramirez. In Texas and two other states where Acosta had recruited accomplices, the victims were ordered to drop off the cash at locations where it could be retrieved in person. All told, prosecutors say, the network set up by Ramirez scammed nearly 40 people.

But the most innovative aspect of the scheme was the kidnapping calls: They were made from *inside* the prison in Mexico City, where Ramirez was serving time. "Who has time seven days a week, 12 hours a day, to make phone calls to the US, over and over and over, with a terrible success rate?" Arbuthnot says. "Prisoners. That was a really big moment for us. When we realized what was happening, it all made sense."

Without leaving his prison cell, Ismael Brito Ramirez had figured out how to scale virtual kidnappings. All he needed was bored prisoners and burner phones. Vicky Leta/Insider

With Ramirez as the mastermind, fake kidnapping calls had become the hottest hustle behind bars. Using prisoners to make the cold calls explained how the criminals were able to dial so many places at once, as well as why the callers were so good at intimidating victims. It also clarified why the ransom demands were usually small. Because the feds were looking for millions in laundered drug money, the crooks figured they wouldn't notice an occasional few grand wired from the US. Like a Silicon Valley entrepreneur, Ramirez had found a way to use the technology at his disposal to scale virtual kidnapping, without ever leaving his prison cell. And unlike email scammers, Ramirez wasn't preying on greed or ignorance or financial desperation. He was monetizing love. He was selling the one thing parents value most: the

lives of their children.

In 2018, Acosta was sentenced to more than seven years in federal prison, convicted on one count of conspiracy to commit wire fraud and one count of conspiracy to commit money laundering. "This is a disgusting crime that preyed on a parent's love for a child," US Attorney Ryan Patrick told the court. "Even though there was no actual kidnapping, the crime was designed to be very real to the victims."

Ramirez was charged with conspiracy to commit extortion, wire fraud, and money laundering. Similar charges were brought against Julio Manuel Reyes Zuniga, an American citizen who is accused of working with Ramirez to orchestrate more than 30 virtual kidnappings in his home state of California while he was serving time for murder in Mexico. The charges against both men carry a maximum sentence of 20 years, but there's an obvious problem: Ramirez and Zuniga are already incarcerated, as the feds suspect is the case with almost every other virtual kidnapper who is still cold-calling potential victims. Which raises the question: How do you stop a crime that's being committed by criminals you've already caught?

"What are we going to do?" Arbuthnot says. "We're going to put these people in jail? They're already in jail."

Indeed, despite the charges against Ramirez and Zuniga, virtual kidnappings have spread to prisons in Puerto Rico and the Dominican Republic, as well as to other cities in Mexico. In Tamaulipas, prison officials tried installing

equipment to prevent inmates from making calls on their cellphones, but the technology was so powerful that it knocked out service throughout the city. "Obviously, that didn't work," Arbuthnot says with a sigh. "It's an uphill battle."

Two months after their ordeal, I visit the Mendelsteins at their home in Princeton. They haven't recovered their cash, and don't expect to. There are no leads in the case, and the FBI hasn't been able to link the crime to any of the suspected kingpins they've identified.

But while the kidnapping of their daughter may have been fake, the pain it caused the Mendelsteins is all too real. Even though it wasn't an actual kidnapping, like the one my family went through, they experienced all of the same emotions and trauma that come when a child is missing: the fear, the panic, the helplessness. Stella was never abducted. But for a few hours, the entire family was held hostage.

"For me, the trauma is about my vulnerability," Richard tells me in his living room, sitting next to Stella and Rachel. "I fell for it. I never questioned it. That's the thing that gets me, because I question everything. But there was something effective about the way it was executed." He pauses, shaking his head. "Now I have this hanging over me," he says. Stella is safe, for which he's grateful. But he

can't let go of the shame he feels at being duped.

There is little likelihood that the explosion in virtual kidnappings will abate anytime soon. The FBI lacks the capacity to track so many random phone calls and small wire transfers coming from so many directions at once. It's not like old-fashioned kidnappings in the movies. There are no federal agents tailing the terrified parent to the drop-off location, ready to pounce on the criminals and free the kidnapped child. In virtual kidnappings, the parents are alone. The drop-offs take place electronically. The criminals are already behind bars. And there are no children to free. There's only a voice on the phone, and the pain and humiliation it leaves behind.

For now, the FBI is left trying to educate the public about how to spot the scams. "Our message is short," Arbuthnot says. "Just hang up." But if that's the only solution the feds can come up with, then virtual kidnappers have little to fear. The "Nigerian prince" email scam, one of the longest-running and best-known frauds in internet history, continues to rake in nearly $1 million a year. Public awareness might cut into the profits of virtual kidnappers, but it won't put them out of business.

If anything, hanging up on kidnapping scams could soon get even harder. It won't be long, Arbuthnot suspects, before the kidnappers learn how to make deepfakes, taking audio of real kids from online postings and manipulating it to sound like a plea for help. Instead of relying on generic recordings, kidnappers will be able to make use of the real thing, digitally tailored to each

victim. "They certainly could do that," Arbuthnot says. "It just hasn't happened yet." All it takes is some free software, a Google search, and time. And if there's one thing virtual kidnappers have, courtesy of the courts, it's plenty of time.