WIRED

CAUGHT BY CRYPTO

They thought their crimes were untraceable.

They couldn't have been more wrong.

The shocking case that shredded the myth of Bitcoin's anonymity.

BY ANDY GREENBERG

MAY 2022 ▪ FOLLOW THE MONEY


THAT'S ONE SMALL STEP FOR A MAN, ONE GIANT LEAP FOR MANKIND

SPEEDMASTER MOONWATCH
CO-AXIAL MASTER CHRONOMETER

LOOKS MAGICAL.
WORKS BEAUTIFULLY.

Although not your typical watch interior, our dreamlike world is not too far removed from the real thing. An OMEGA watch calibre is a tiny universe of components. Each working so wonderfully together, our precision timepieces have earned the trust of athletes, deep sea adventurers - and even astronauts.

OMEGA

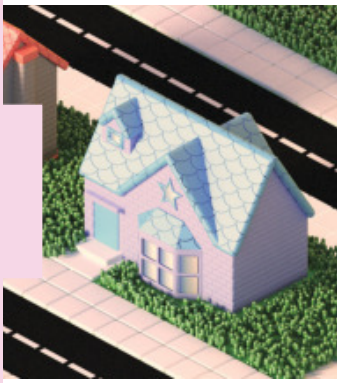
PHOTOGRAPH / NICHOLAS ALBRECHT

ON THE COVER

Illustration by Mike McQuade

Welcome to Video was the biggest global online marketplace for child sex abuse materials ever known, and its administrators and members thought using Bitcoin would shield their crimes from law enforcement. Instead, their crypto transactions led authorities right to them. For the cover, illustrator Mike McQuade went with a universal symbol of forensics. But he drew it using actual blockchain addresses and transaction IDs from the case, provided by writer Andy Greenberg. "Up close it just looks like a bunch of letters and numbers in no discernable pattern," McQuade says. "From afar it takes on the form of a fingerprint."

MIND GRENADES



SIX-WORD SCI-FI

Top to bottom: Elena Lacey, Maria Chimishkyan, Sam Whitney, Violet Reed

Thät's Dazs™

Luxury is where you are.

BY VIRGINIA HEFFERNAN

The Pleasure Principle

The real reason conspiratorial beliefs are so difficult to dislodge.

"THE SEEKING IS A never-ending circle until one is satisfied," Justin reflected, runically, in an email to me. "For me, that satisfaction was never really present until the theories of QAnon started emerging."

Yes, QAnon—the undead cosmology that still haunts the internet. Justin, a Brooklyn entrepreneur who once worked for TED, is best known for having been so jazzed about the QAnon-Trump conceit that he joined the Stop the Steal protest in Washington, DC, on January 6 last year. He now says he wouldn't have gone if he'd known it was going to turn violent.

ILLUSTRATION / SR GARCÍA

I had seen a news story about a penitent QAnon adherent called simply "Justin," and I wanted to hear more; I thought I could find him. (After I did, he asked me to use only his first name.) In our exchanges, he sounded fully deradicalized—candid, earnest, thoughtful about his own choices. "I dissociated so much from my reality," he told me about the years leading up to January 6. He had lost friends. "I acted in a condescending manner to a lot of people, and it was wrong of me to do that."

He was repairing his friendships, helping build a new business, trying to put Stop the Steal behind him. "Anyone who invited or incited violence on Jan 6 I do not support," he wrote. Did he still believe in the vast child-abuse network that defines QAnon's muddled worldview? He said no. Then he added: "It's my hope that such does not exist."

His hope. I left it at that, though, later on, righteousness caught in my throat like a thorn. Why wouldn't Justin *fully* reject QAnon? How could I *prove* to him it's horseshit? I briefly imagined enlightening him with sniper-fired bullet points and rhetorical virtuosity. But the aggression in my fantasy disturbed me. I'm not the policewoman of all rationality, and people's creeds are their own. Maybe this is what missionary zeal feels like. *I must tear out these pagan lies, root and branch.*

In general I believe what Freud did: that it doesn't matter, for purposes of human connection, whether another person's private apprehensions comport with reality or not. If something's true for a person, and she's not harming anyone, a good friend suspends disbelief. This seems self-evident for religious faith ("I believe in one God") or private credos ("we manifest our destinies"). But then there are false empirical claims, like "5G kills" or "a secret cabal of cannibals runs the world." Can people who live in fantasy worlds at such steep odds with reality be good friends and citizens themselves? At the very least, maintaining such worldviews means vigilance about rejecting facts—and the perceptions of other, clearer minds. This estranges others. People who believe lies certainly could, like Justin, act in a condescending manner to a lot of people. If things escalate, they might even invite or incite violence.

Getty Images

John Mack, who was killed by a drunk driver in 2004, was an eminent Harvard psychiatrist who wrestled manfully in the '90s and aughts with the question of what to do about other people's false beliefs.

Starting in 1990, he set out to study people who said they had been abducted by aliens. He first hypothesized that they were mentally ill, but determined to record their worldviews without bias. To the supreme embarrassment of some of his Harvard colleagues, Mack didn't just establish trust with the would-be abductees. By 1994, he had come to share their outlandish beliefs, for which there was no empirical proof.

Mack's credentials lent credence to the stories of his research subjects, just as certain credentialed MDs these days throw in with anti-vaxxers and give them unearned authority. In the late '90s I managed to catch Mack on his road show in New Hampshire. He patiently took the audience through the experiences of his research subjects whose accounts of abduction he found credible. The stories, he said, were consistent; the tellers were uninfluenced by a therapist's suggestions, and sane. To Mack, that was proof enough: Aliens were routinely snatching people up into flying saucers, and humanity needed to face facts. (The next speaker at the road show was a man who preached that aliens had made crop circles in the Scottish Highlands.)

In *The Believer*, a 2021 biography of Mack by Ralph Blumenthal, Mack admits he had never witnessed alien abductions or gathered material evidence. Instead, he says, the idea of the abductions eased his grief about losing his mother when he was an infant. Mack once told a therapist: "The abduction story is a welcoming story because it means that—Ooooo, I'm getting goose pimples as I think of this—I'm not alone. There is life in the universe!"

To Mack, the stories were also factual. How could they not be? The aliens in the stories always looked the same: gray, short, with slits for mouths and no noses or ears. They drew blood and other bodily fluids from their hostages.

The abductees, too, fit a type: "unusually sensitive, spiritual individuals who chafe against social constraints and are flexible in accepting diverse or unusual expe-

BUSINESS EXPERTISE THAT SCALES.

As your business grows, your day-to-day concerns get bigger too.

Whether you need financing for new equipment, an asset-based loan for short-term cash-flow, or big-picture business banking advice, let's chat about your future.

Talk to a dedicated Relationship Manager and a team of experts at City National® today.

We make it our business to be personal.

CITY NATIONAL BANK
AN RBC COMPANY

Discover ***The way up***® at cnb.com/business.

riences," as Robert S. Boynton described them in an article about Mack for *Esquire* in 1994. "Abduction runs in families; you are more likely to be taken if your parents or siblings have been."

I was still dwelling on Justin. Like Mack, he got goose bumps from fictions that strike most people as disturbing. This feeling was evidently intensified when he believed the stories were literally true; he couldn't see them as science fiction and get the same high. As Justin told me of his period of most excitement about QAnon, "In 2020 … I felt that the truth was giving me a new lens on the world, and this made me feel very good … The euphoric feeling was a deep spiritual awareness of pure love and joy … I was unabashed, free-spirited, loving, communicative, and wanting to help—whatever that meant."

An unusually sensitive, spiritual individual, Justin in another era might have entertained alien-abduction fantasies. Notably he had also suggested that his supernatural ideas—or his own susceptibility to disinformation—might run in *his* family. "I started as a young boy seeking meaning to life's deeper questions. I would write poetry to try and get my thoughts on paper, but … much of the impetus came from my father and what he bestowed upon me … It's in my blood, so to speak."

All these weird tales—about blood-sucking elites and blood-sucking extraterrestrials—serve psychological purposes, and they're highly stylized along the lines that make pulp fiction pleasing. But none of them have anything to do with evidence. What Mack and Justin, and others who hold outrageously false ideas, mean by "true" may be better understood as "pleasurable." Perhaps this is why such beliefs are so difficult to dislodge. You don't debate with people about the merits of their kinks. Instead, you hope that we all maintain some ironic distance from our cherished stories, especially the pulpy and frightening ones, while recognizing that they don't have to be empirically factual to be emotionally meaningful. When a person forgoes this irony, and grounds their serenity and joy in a false claim about reality, you do little but cause pain if you try to root it out.

When a person grounds their serenity and joy in a false claim about reality, you do little but cause pain if you try to root it out.

Justin, unlike Mack, ultimately saw that the high provided by his strange beliefs wasn't serving him. "The downside of this was I was in such a state of euphoria that I decided to leave my job with no recourse, not pay my rent, etc.," he wrote. "I paid less attention to 'adulting.'" For a person in his twenties to stop adulting for a passion of any kind—art, love, a political movement—seems not atypical; to right one's course comparatively quickly is impressive.

I had a last question for Justin, whose self-possession I had come to admire.

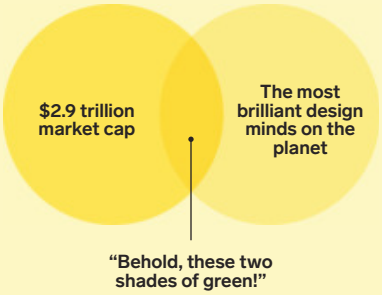
"Do you believe now that the 2020 election was stolen by Joe Biden?" I hit send. A one-word answer came back: "Yes." W

VIRGINIA HEFFERNAN *(@page88) is a regular contributor to* WIRED.

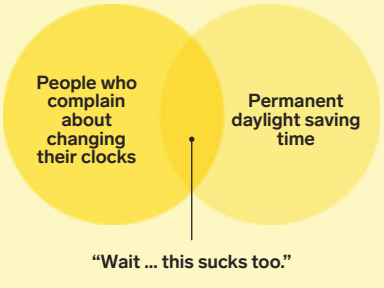
CHARTGEIST

by Jon J. Eilenberg

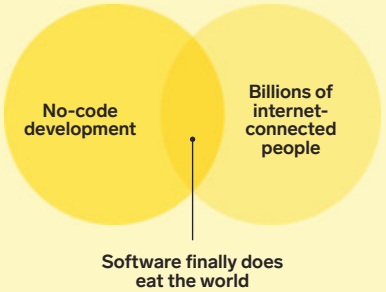
iPhone Innovation



The Human Condition



Programming for All



Everybody's Working for the Good-Binge

Why do we still speak as if our days are ruled by the sundial and the pendulum clock? New times call for new timescales!

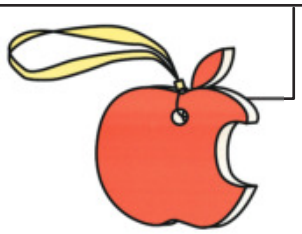
FRIENDS, we need to revamp the calendar. Our years start arbitrarily, based on "the sun," which people rarely see anymore. And months, they're a scam, a way to keep peasants tilling and monks distilling. Those people didn't have social media; they barely had vellum media. Weeks, days, hours, minutes—especially minutes—are just more mechanisms for keeping humans in thrall ultimately based on astronomy, astrology's lesser sibling. In the globalized information environment we currently enjoy, we should and must construct better timescales. I propose some new terminology.

DEMOQUADRENNIAL: An election-focused political season, equivalent to 48 months on the old calendar, stretching from pre-nomination through postelection. Each demoquad is broken into a series of shorter periods known as *surely-thises*. "With the revelations in Washington yesterday, this demoquad enters its record ninth surelythis."

LIGHTMODE/DARKMODE: The new "day" and "night," but no longer tied to the 24-hour solar cycle. A person can opt into them at any time. "I'm off to bed—have a great lightmode!" "It was a long lightmode's journey into darkmode." Transitions between the two are *fades*: "The mode is darkest before the fade."

DEMIC: The duration of a pandemic; split into *waves*, which are further split into *prepanic* and *panic*. (Some have conceptualized a *post-panic* phase, but none has yet occurred.) Examples: "I'll get a new job after the current demic." "We should get dinner while it's still prepanic."

LOOPMAS: A season of good cheer surrounding the randomly scheduled release of new Apple hardware. Replaces "the holidays."



BINGE: Replaces "weekend"; refers to the amount of time necessary to watch a streaming video series in its entirety. The period formerly known as Friday night to Sunday morning is *good-binge*, and the period formerly known as Sunday morning to Monday morning is *sad-binge*. "Babe, the panic is starting soon. Why not come over and spend good-binge with me?" A binge can optionally be experienced at *tubespeed*, a state of heightened awareness in which you partake in culture at 1.25X, 1.5X, or 2.0X. "I went hard tubespeed last sad-binge and finished both seasons."

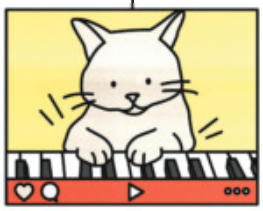
ILLUSTRATION / ELENA LACEY

PUSHINGS: Improvement over "hour"; it increments whenever a new notification or update is pushed to your phone. This allows you to easily characterize the quality of a so-called day: "It was a long lightmode, and I got hungry around sixth pushing and went out for drinks." Or: "Twelve straight pushings and I'm ready for a binge."

FRESHING: Short for "refreshing." The new "minute." "I'll be there in 20 freshings." Or: "I need a few freshings before I come down to dinner." Or: "I have 15 freshings before my plane leaves, and then I'm in the air for about a thousand freshings unless I go darkmode."

WAKEMARE: The period of 20 freshings when one fades out of darkmode and into full consciousness by looking at a steady flow of misery on one's phone. "Hon, try to keep your wakemare to a few freshings, then come down for some toast."

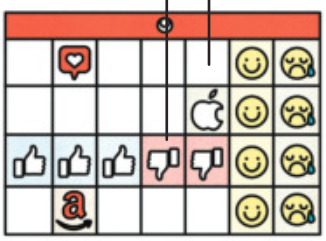
CRYPTOLUDE: A duration of time during which nothing confusing or scammy happens on the internet. Rarely lasts more than two freshings. "I enjoyed a nice cryptolude with my coffee, but now it's time to log on to Discord."



DECKADE: The time spent watching someone make a live presentation on Zoom or Google Meet (a scenario in which tubespeed is unavailable).

BEANDAD: Replaces the antiquated "week." Refers to the time it takes for a main character to rise, fall, and flame out on Twitter. "The Putin mommy poem already feels like 50 beandads ago."

SPRINT: The new "work week." Derived from Agile nomenclature. (Time has historically been extremely Waterfall, which we know is bad for team-based technology work.) The "days" are now referred to as Planspan, Scrumspan, Kanbanspan, Pushspan, and Retrospan, with two days for binge. "Eileen, pace yourself. It's only Scrumspan. We've got three lightmodes to go before good-binge."



BRUSHKNOCKS: A "second" on the old calendar, characterized by the sound of a Slack notification. "I'll be there in two brushknocks."

LITTLEBREAK: A period of partial logoff, often expected to last a full demic but typically ending after several darkmodes. "I'm not going to measure my life in freshings any longer," says the person entering their littlebreak. (They always return.)

LOGOFF: Replaces "death."

PAUL FORD *(@ftrain) is a programmer, essayist, and cofounder of Postlight, a digital product studio.*

iBuying Trouble

Zillow botched its home-flipping program, losing a fortune in the process. Opendoor thinks it can do better. The key? More data.

ZILLOW GAVE UP. For years, the online real estate company—best known for helping owners and prospective buyers estimate the prices of properties—had been purchasing homes from customers who wanted a quick, seamless sale, a practice known as iBuying. The program, called Zillow Offers, involved making a firm, reasonable offer on a home, holding on to the property briefly while making necessary repairs, and then selling it, presumably for a profit. But all too often Zillow found those homes selling for less than it paid for them. Last November, faced with a loss in the hundreds of millions of dollars, the company shuttered Offers and laid off a fourth of its entire workforce.

At the time, my colleague Chris Stokel-Walker outlined on WIRED.com some of the reasons Zillow failed. The key factor was an inability to predict prices a few months after it made offers, based on the company's famous "Zestimate" of a home's worth. (Any homeowner who obsessively checks their Zestimate knows that, while it provides a useful ballpark, sometimes the appraisal is in the bleachers.) Another complication: After Covid hit, the real estate market first stalled and then caught fire. As chastened CEO Rich Barton admitted to CNBC: "We've been unable to accurately forecast future home prices."

The demise of Offers seemed like a bad moment for iBuying, which is just a tiny slice of the overall market but has ambitions to transform the way people sell houses. By giving sellers a speedy offer (and taking a fee of around 5 percent, about what a broker charges), this approach spares homeowners the stress of staging a sale and going through the high-pressure dramatics of a traditional closing, where at the last moment the prospective buyer might decide to make costly repair requests or demand to keep the chandelier you'd already stipulated you'd be taking to your next pad.

But can other iBuyers avoid Zillow's fate?

That's what I asked Ian Wong, CTO and cofounder of Opendoor, one of the leaders in iBuying. Opendoor, which went public via a special purpose acquisition company last year, reports rising revenues and a gross profit, though it still loses a bundle after costs are accounted for. Basically, I wanted to know why Opendoor feels it can succeed when Zillow fell flat on its face.

Of course, Wong wasn't going to divulge trade secrets, but he told me that Opendoor's confidence comes from its focus on data from the start. Wong was working at Square doing risk analysis when he was introduced to Opendoor cofounder and CEO Eric Wu, who had joined Trulia after that company acquired his real estate startup in 2011. The pair decided to launch Opendoor in 2014 because, Wong says, they saw "an amazing opportunity to bring a data science mindset to this antiquated transaction, which is the single most important one in most people's lives." Buying is just the starting point on Opendoor's road map—the company sees itself as handling every aspect of the real estate process, where those who accept its purchase offers will use its other services, such as title search and mortgage offerings, to find and buy their next home. It even launched a program that fronts buyers the money to make all-cash offers on new homes—a significant advantage in some red-hot real estate markets.

Sounds great, but how does Opendoor avoid losing money? After the Zillow debacle, people noted that those most likely to accept the typically conservative cash offer from an iBuyer are often those whose houses are less likely to impress buyers—and thus are harder for Zillow or Opendoor to get rid of.

Opendoor, Wong told me, isn't overly reliant on what is known as an automated valuation model (AVM), like Zillow's Zestimate, Redfin's Estimate, or a local govern-

"We've gotten so used to tapping on our phones to order groceries, hail a ride, or even buy a car, sell a car. I don't think there's any fundamental difference when it comes to real estate."

ILLUSTRATION / MARIA CHIMISHKYAN

ment's official assessment, which come up with numbers mostly based on the prices of "comparable" properties. Opendoor views pricing as a holistic process that goes beyond a simple AVM to blend hundreds of data points about the marketplace, the region, trends, pricing forecasts, and the house itself. Originally the company dispatched a person to assess each property for necessary repairs, among other things. But early in the pandemic, Wong says, Opendoor switched to virtual tours that turned out to be just as useful and took a fraction of the time. Now a seller performs a live walk-through of the home for an Opendoor representative. Ultimately, he says, these combined data points result in an offer that minimizes risk for Opendoor yet is high enough to have a good chance of closing the deal. "We've spent eight years agonizing over every single component," Wong says.

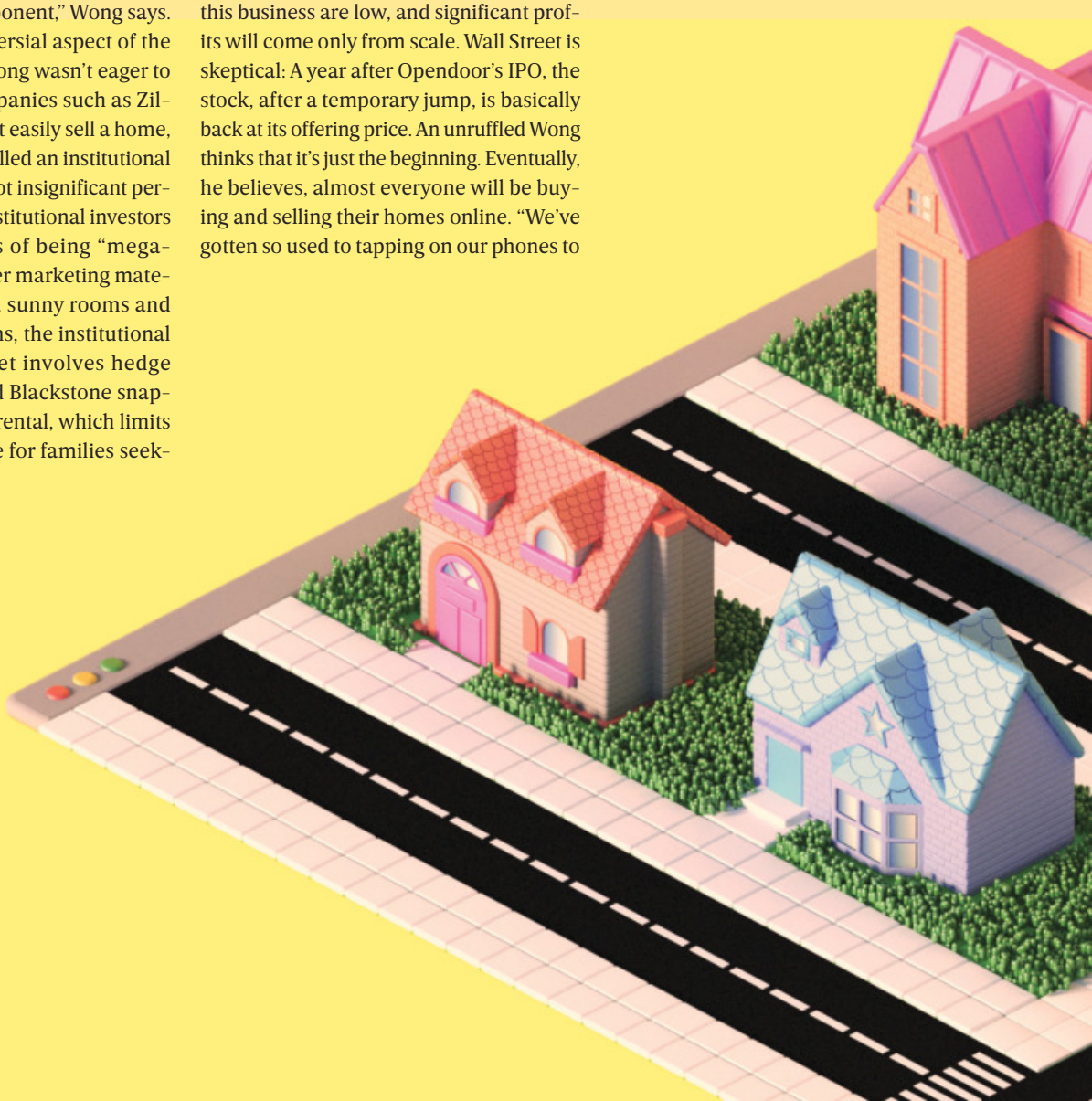
There's one controversial aspect of the business model that Wong wasn't eager to talk about. When companies such as Zillow and Opendoor can't easily sell a home, the fallback is what's called an institutional sale. All iBuyers sell a not insignificant percentage of houses to institutional investors who have aspirations of being "mega-landlords." While iBuyer marketing materials emphasize clean, sunny rooms and frictionless transactions, the institutional segment of the market involves hedge funds such as KKR and Blackstone snapping up properties for rental, which limits the inventory available for families seeking to buy homes. Even the Biden administration recently weighed in on the evils of this trend: "Large investor purchases of single-family homes and conversion into rental properties speeds the transition of neighborhoods from homeownership to rental and drives up home prices for lower-cost homes, making it harder for aspiring first-time and first-generation home buyers, among others, to buy a home."

Opendoor's Wong acknowledges that a minority of the homes it buys are flipped to institutional firms, but he won't put a figure on how many. A recent Bloomberg study found that 20 percent of homes bought by iBuyers go to those companies—and twice as many in some markets.

In Opendoor's latest reported earnings, it said it sold 15,181 homes, which brought in $2.3 billion in revenue. The margins in this business are low, and significant profits will come only from scale. Wall Street is skeptical: A year after Opendoor's IPO, the stock, after a temporary jump, is basically back at its offering price. An unruffled Wong thinks that it's just the beginning. Eventually, he believes, almost everyone will be buying and selling their homes online. "We've gotten so used to tapping on our phones to order groceries, hail a ride, or even buy a car, sell a car," he says. "I don't think there's any fundamental difference when it comes to real estate."

If that happens, it might save people a lot of time and eliminate a lot of stress. On the other hand, anyone who has undergone a lengthy home search knows that, as excruciating as the process can be, you exit the ordeal knowing not only the market but your own priorities. Finding the place where you will eat, sleep, raise your family, and probably even work is a test of not just the spreadsheet and the bank account, but the heart.

Editor at large STEVEN LEVY *(@StevenLevy) has contributed to* WIRED *since its inception. For more of his Plaintext columns, visit* WIRED*.com/tag/plaintext.*



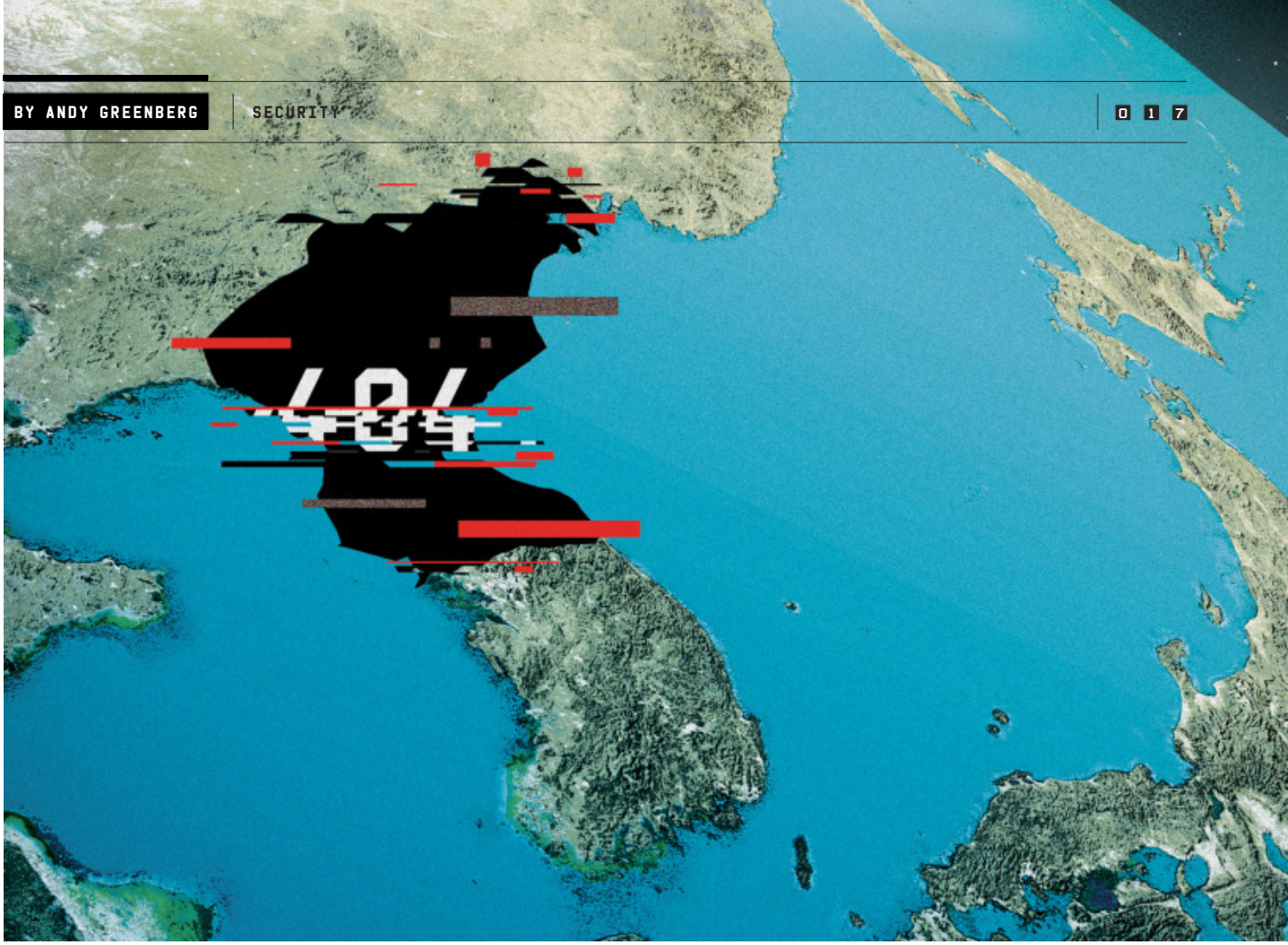
Get More A.I.
Get More Robots
Get More Ideas
Get More Rockets
Get More Crispr
Get More Blockchain
Get More Informed
Get More at WIRED.com

Subscribers get unlimited access to all WIRED stories online.

To authenticate your subscription, go to WIRED.com/register. Not a subscriber but want to get the best daily news and analysis of the biggest stories in tech? Subscribe at WIRED.com/subscribe.

WIRED

Christie Hemm Klok



Error: North Korea Not Found

Appalled by the Hermit Kingdom's cyberattacks on security researchers—and the lack of a US government response—one hacker took matters into his own hands.

IN JANUARY, observers of North Korea's strange and tightly restricted corner of the internet noticed something strange: The country seemed to be dealing with serious connectivity problems. On several different days, nearly all of its websites—the notoriously isolated nation has only a few dozen—intermittently dropped offline, from the booking site for its Air Koryo airline to Naenara, a page that serves as the official portal for dictator Kim Jong-un's government. At least one of the central routers that allow access to the country's networks appeared at one point to be paralyzed, crippling the Hermit Kingdom's digital connections to the outside world.

Some North Korea watchers pointed out that the country had just carried out a series of missile tests, implying that a foreign government might have launched a cyberattack against the rogue state to warn it off saber-rattling. But responsibility for the outages didn't lie with US Cyber Command or a state-sponsored hacking agency. It was the work of one American man in a T-shirt, pajama pants, and slippers, lounging in his living room night after night, watching *Alien* movies, eating spicy corn snacks, and periodically walking over to his home office to check on the programs he was running to disrupt the internet of an entire country.

In one sense, it was a simple act of revenge. In late January 2021, the

ILLUSTRATIONS / ELENA LACEY

independent hacker, who goes by the handle P4x, was himself hacked by North Korean spies. P4x had spotted a Google security team blog post warning that North Korean hackers were targeting cybersecurity researchers around the world. He recalled that just 24 hours earlier he'd opened a file sent to him by a fellow hacker, who had described it as an intrusion tool P4x might be interested in. The name of the hacker matched one that the blog post had warned was used by the North Koreans. Sure enough, upon closer inspection, P4x saw that the attachment he'd opened contained a backdoor designed to provide remote access to his computer. He was shocked and appalled that North Korea had personally tried to hack him.

P4x says he was contacted by the FBI but was never offered any real help to assess the damage from the hack or to protect himself against future attempts. (Fortunately, he had opened the file in a "virtual machine," digitally quarantined from his system, so the attackers had no opportunity to swipe anything of value.) Nor did he ever hear of any consequences for the hackers who targeted him; he wasn't aware of any investigation or formal recognition from any US agency that North Korea was responsible. It began to feel, he says, like "there's nobody on our side."

After a year of letting his resentment simmer, P4x took matters into his own hands. "If they don't see we have teeth, it's just going to keep coming," he says. (P4x spoke to WIRED and shared screen recordings to verify his responsibility for the attacks but declined to use his real name for fear of prosecution or retaliation.) "I want them to understand that if you come at us, it means some of your infrastructure is going down for a while."

P4x says he's found numerous unpatched vulnerabilities in North Korean systems that have allowed him to single-handedly launch denial-of-service attacks on the servers and routers that the country's few internet-connected networks depend on. He declined to reveal those vulnerabilities, which he argues would help the North Korean government defend against his attacks. But he named, as an example, a known bug in the web server software NginX that mishandles certain forms of data, allowing machines that run the software to be overwhelmed and knocked offline. He also alluded to finding "ancient" versions of Apache web server software, and he says he has started to examine North Korea's national operating system, known as Red Star OS, which he described as an old and likely vulnerable version of Linux.

P4x has largely automated his attacks, periodically running scripts that identify which systems remain online and then launching exploits to take them down. "For me, this is like the size of a small-to-medium pentest," he says, using the abbreviation for a "penetration test," the sort of whitehat hacking he carries out to reveal vulnerabilities in a client's network. "It's interesting how easy it was to have some effect in there." The result of these relatively simple hacks has been immediate. Records from the uptime-measuring service Pingdom show that at several points during P4x's campaign, almost every North Korean website was down.

Junade Ali, a cybersecurity researcher who monitors the North Korean internet, says he began to observe these mysterious, mass-scale cyberattacks and closely tracked them without having any idea who was carrying them out. Ali says he saw key North Korean routers go down, taking with them not only access to the country's websites but also to its email and other internet-based services. "As their routers failed, it would literally be impossible for data to be routed into North Korea," Ali says, describing the result as "effectively a total internet outage." P4x notes that while his attacks disrupted all websites and services hosted in the country, they didn't cut off North Koreans' outbound access to the rest of the internet.

As rare as it may be for a single pseudonymous hacker to cause an internet blackout on that scale, it's unclear what impact the attacks have had on the North Korean government. Only a tiny fraction of the country's citizens have access to internet-connected systems to begin with, says Martyn Williams, a researcher for the 38 North Project, from the Stimson Center's North Korea–focused think tank. The vast majority of residents are confined to the country's walled-garden intranet. Williams says the sites P4x has repeatedly taken down are largely used for propaganda and other functions aimed at an international audience.

While knocking out those sites no doubt presents a nuisance to some regime officials, Williams points out that the hackers who targeted P4x last year—like almost all North Korean hackers—are almost certainly based in other countries, usually China. "If he's going after those people, he's prob-

"He's probably directing his attention to the wrong place. But if he just wants to annoy North Korea, then he is probably being annoying."

ably directing his attention to the wrong place," Williams says. "But if he just wants to annoy North Korea, then he is probably being annoying."

P4x says he would count annoying the regime as a success and that targeting ordinary citizens—most of whom lack internet access—was never his goal. "I definitely wanted to affect the people as little as possible and the government as much as possible," he says.

These attacks amounted to no more than, as P4x puts it, "tearing down government banners or defacing buildings." He now intends to try hacking into North Korean systems to steal information and share it with experts. He's hoping to recruit more hacktivists to his cause with a dark website he launched called the FUNK Project—i.e., "FU North Korea"—in the hope of generating more collective firepower. "This is a project to keep North Korea honest," the site reads. "You can make a difference as one person."

This hacktivism is meant to send a message not only to the North Korean government, P4x says, but also his own. His cyberattacks on North Korean networks are an attempt to draw attention to what he sees as a lack of US government response to the country's targeting of Americans. "If no one's going to help me, I'm going to help myself," he says. (When WIRED asked the FBI about its response to the incident, it replied with a statement: "The FBI is committed to pursuing the malicious actors and countries behind cyberattacks, and will not tolerate intellectual property theft or intimidation.")

Other hackers targeted by North Korea don't agree that P4x's hacking spree is the right way to make a statement. Dave Aitel, a former NSA hacker and founder of the security firm Immunity, was targeted in the same espionage campaign. But he questions whether P4x's approach to getting even is productive, given that he may be getting in the way of stealth intelligence efforts going after the same North Korean computers. "I would not want to disrupt real Western intelligence efforts that are already in place on those machines, assuming there is anything of value there," Aitel says.

He agrees, though, that the US government response to North Korea's campaign has been lacking. Aitel says he reached out to the FBI and never heard back, but he lays the blame for the government's silence at the feet of the Cybersecurity and Infrastructure Security Agency. "This is one of the biggest balls CISA has dropped," he says. "The United States is good at protecting the government, OK at protecting corporations, but does *not* protect individuals." (A CISA spokesperson responded in a statement that the agency "is committed to supporting the cybersecurity community in detecting and protecting against malicious cyber actors," adding that "as part of this work, we encourage any researcher that is being targeted by cyber threats to contact the US government so we can provide all possible assistance.")

Aitel points out that many of the targeted researchers likely had significant access to software vulnerabilities, enterprise networks, and code for widely used security tools. That could result, he warns, in another security debacle of the kind discovered in late 2020, in which Russian state hackers hid their own code in the IT management software of the company SolarWinds to penetrate as many as 18,000 networks worldwide.

US government criticisms aside, P4x is clear that the message behind his hacking is aimed primarily at the Kim regime, which he describes as carrying out "insane human rights abuses and complete control over their population." While he acknowledges that his attacks likely violate US computer fraud and hacking laws, he argues he hasn't done anything ethically wrong: "My conscience is clear."

And what's his endgame? "Regime change. No, I'm just kidding," P4x says with a laugh. "I just want to prove a point before I stop."

Senior writer ANDY GREENBERG *(@a_greenberg) covers security, privacy, and information freedom. He's the author of the forthcoming book* Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency *(see page 60)*.

READOUT

The world, quantified.

14M

→

Passenger cars it would take to equal the emissions of all military activity in the EU in 2019—three years before the start of the war in Ukraine.

90%

→

Estimated percentage of imported neon that the US sourced from Russia and Ukraine. The gas is essential for semiconductor manufacturing.

$50M

→

Amount an activist collective raised to pay Julian Assange's legal bills by selling an NFT called "Clock," which displays how many days he has been behind bars.

24

→

Estimated number of trees felled per second in Brazil in 2020—mostly by ranchers and farmers clearing land for cattle and crops.

Sources (from top): Conflict and Environment Observatory, TechCet, AssangeDAO, MapBiomas

Fight the Algorithmic Power

To push back against unfair labor practices, China's food delivery workers are using social media, unofficial unions, and even the software that drives the gig economy.

HUANG HUI CAN sum up his six-month stint as a gig worker in Shanghai in one word: "exhausting." A PhD candidate at King's College in London, he embedded with a group of people who delivered food on their electric motorbikes, many for 12 hours a day. Huang soon realized that he could not keep up with his colleagues. Plus, the work is risky. He says he saw six accidents involving couriers during his stint, one of which was fatal. "It was really shocking," he says.

Huang is among a cohort of researchers studying how algorithms control gig workers' lives. In the past decade, China's platform economy has engulfed almost a quarter of the country's labor force, with an estimated 200 million people working in "flexible" employment. Between 2011 and 2020, the food delivery industry ballooned from $3.4 billion to $105 billion. Couriers kept joining, driving down delivery fees; the platforms kept lowering delivery times, attracting more customers. The result? Huang's experiences were spot-on. Couriers got in more and more accidents as they raced to meet the shorter delivery times and to make up for the lower fees per order. A report from Shanghai's traffic police showed that in the first half of 2017, a delivery rider was involved in a deadly traffic accident every 2.5 days.

There has been criticism of the industry's labor practices, especially the data-driven pressures imposed by the two largest food delivery platforms, Meituan and Alibaba-owned Ele.me. But as companies use algorithms to push couriers to work faster, squeezing them with tighter delivery times, gig workers have started to rebel. Some are gaming the system to gain higher wages; others are banding together to turn the algorithms against their bosses. Many more are using social media to organize. (Of course China doesn't allow workers to unionize or strike, so all these efforts are unofficial.)

Couriers have set up WeChat groups to share information on places where it's difficult to deliver, such as gated communities or large buildings with multiple elevators. These are treated as "no-fly zones," where couriers refuse to go, according to researchers Tiziano Bonini from the University of Siena and Zizheng Yu and Emiliano Treré from Cardiff University. The couriers "know it is impossible to deliver in the time expected," Bonini says. "So they organize collective rejections until that order comes back with a higher price." If they're going to get dinged for taking too long, at least they'll be paid more.

In busy cities such as Shanghai, some delivery work is organized around "stations." These are hubs that coordinate orders from different restaurants, guaranteeing couriers a steady stream of deliveries and taking a fee from the platforms they work for. "There are two types of delivery drivers," says a courier for Meituan, who asked to remain anonymous over concerns for job security. "Some are part of stations, and they will get more orders. Then there are drivers who go it alone, and they are freer but get fewer orders." This gives station workers bargaining power: If they refuse to work for lower wages, causing a station to lose orders, the station's rating plummets, and it receives less business. Meanwhile, the couriers can continue working independently. "Even minor disruption in the form of these very small-scale collective actions can bring the station-level managers to the bargaining table," says Eli Friedman, an assistant professor of international and comparative labor at Cornell University.

The most famous informal union is the Knights League, which was set up in 2018. Prominent gig activist Chen Guojiang reportedly managed 16 WeChat groups for the League, reaching over 14,000 delivery drivers. He would tell gig workers "how to support each other, because everyone is weak," Yu says, "but if they can form a link, some kind of solidarity, then maybe they can ask more from the platforms." He was arrested in March 2021 on charges of "provoking trouble," after he tried to mobilize strikes among fellow couriers in Beijing.

The platforms have gotten creative about finding ways to get more out of their contractors. Some tweak their algorithms to turn delivery work into a game: Couriers on Meituan and Ele.me are ranked by performance in ways that impact their income. Companies often stage competitions to encourage couriers to take more orders, inspiring some to game the algorithms right back, by faking orders to improve their standing.

Which brings us back to the biggest problem: worker safety. A recent investigation by the nonprofit Beijing Zhicheng Migrant Workers Legal Aid and Research Center found cases in which couriers' data vanished after an accident. Gig workers need order data to prove they were injured at work, but if they can't access the app, they can't provide evidence to back up their claims.

A slew of incidents, some of them deadly, made the public more aware of poor gig-work conditions. In 2019 a driver for Meituan fatally stabbed a clerk during a dispute over picking up something for a delivery, sparking debate about the time pressure on

ILLUSTRATION / SAM WHITNEY

Getty Images

couriers. In another notorious case, a delivery rider for Ele.me set himself on fire over the equivalent of $770 in docked payments.

Meituan spokesperson Xiang Xi told WIRED that the company has been making its order dispatch system more open and transparent and lengthening delivery times. Ele.me did not respond to a request for comment, but it has been introducing similar measures.

The majority of food delivery drivers are migrant workers from poor and rural areas, and thus they lack access to government benefits such as health, unemployment, and work insurance, which in China are tied to residency, or *hukou*. Many were once employed in the shrinking industrial sector, where long hours of repetitive work are the norm. Gig jobs offer better pay, flexibility, and autonomy. There's no boss except the algorithm in the palm of their hand, so it feels like entrepreneurship, Huang says. "I work on my own, and I am free to work overtime if I want to or work less when it suits me," the Meituan courier says.

Pressure to improve conditions for "delivery brothers," as they're often called in China, increased when they became essential workers at the onset of the Covid-19 pandemic. "Delivery drivers suddenly became heroes, and we were treating them like garbage," says Kendra Schaefer, a partner at Trivium China, a policy analysis consultancy. "There was this public outcry to treat them better." The government signaled its sympathetic stance with a viral two-minute video, in which a Beijing bureaucrat was shown working as a delivery driver for a day, earning just 41 yuan ($6), enough to pay for a modest meal but not much else.

On March 1, a new Chinese law went into effect that regulates algorithms, affecting how platforms allocate orders, pay salaries, and hand out rewards and penalties for gig workers. For example, it calls for algorithms that watch for signs of burnout rather than impose a pace that leads to it. The government has also asked gig workers to join the country's only legal union, the All-China Federation of Trade Unions, which is controlled by the Communist Party. While the union doesn't help workers with collective bargaining or strikes, it may serve as a conduit for getting worker complaints to the platforms. Indeed, calls have been mounting nationwide, including in union branches, to give more voice to platform workers on how algorithms are made.

The Meituan courier says the algorithm law hasn't affected their work much yet, but it could increase costs for the platforms. "Given that the operating profit margin of food delivery platforms is only 3.3 percent, this will be a significant challenge," says Jamie Chen, an analyst at research firm Third Bridge. Of course, the companies are likely to make the smallest adjustments possible, Schaefer adds. This would mean gig employment will remain precarious, with algorithms still in control.

But the main issue is actually not how algorithms control workers, Huang says; after all, "algorithms are just a tool used by people." Ultimately, it's about who writes the algorithm rules, protocols, and policies. W

Additional reporting by Kyle Mullin.

MASHA BORAK *(@MashaBorak) is a freelance journalist who writes about the intersection of technology with politics, business, and society.*

BY JAINA GREY | GEAR

Private Eyes

Diving into virtual reality is easier than ever—and it's finally worth it.

FOR YEARS, VIRTUAL REALITY gear has been written off as too expensive, too awkward, and too alienating to go mainstream. But now that everyone is talking about the metaverse, VR is gaining momentum. The market is bursting with new apps and games, great hardware, and even fresh use cases—a VR headset can be just as useful for work as for recreation. Here are some favorites that cover all the bases.

JAINA GREY *(@jainagrey) is a product reviewer and writer at* WIRED.

↑ BEST OVERALL

Meta Quest 2

Originally called the Oculus Quest 2, this model was renamed along with its parent company. It delivers excellent resolution in a lightweight body, and two controllers come in the box so you can jack in right away. The Quest 2 was built to run on its own, but you can plug it into a gaming rig to experience the kind of ultra-hi-def VR you can only get from dedicated PC hardware. It's also great for remote work. With Meta's Horizon Workrooms, you can set up a virtual office space and invite your coworkers' avatars over to hang out and collaborate. Plus, Meta's app store is the best one out there. The biggest drawback is that you have to sign in with a Facebook account. Not everyone will be comfortable with that, given Meta's less-than-stellar history of handling user data. Just make a burner account—you won't regret it. $299 AND UP

Must-Play Games

Find these titles on all VR platforms.

MOSS puts you in the shoes of a kindly forest spirit who's guiding an adorable mouse knight through perilous adventures. Unlike most VR games, this one can be played while standing or sitting. $30

SUPERHOT plays like a cyberpunk action movie as you fight faceless polygon men to a pulse-pounding soundtrack. The twist: Time moves only when you do, so you can control the flow and dance to dodge projectiles. $25

VADER IMMORTAL takes you on a multi-episode adventure into the Star Wars universe as a smuggler captured by the evil Empire. It's full of memorable characters, and the environments are truly gorgeous. $30

Courtesy of Meta, HTC Corporation, Polyarc, Ankarsum, Polestar, and Garmin

↑ BEST FOR CASUAL VR

HTC Vive Flow

With a form factor more like a giant pair of sunglasses than a high-performance headset, the Flow is perfect for short jaunts in the metaverse. It's made for activities like streaming videos from your phone, meditating in a virtual space, or visiting remotely with friends or colleagues. At just 6.6 ounces, it's lightweight and portable enough to throw into a carry-on. The design is my favorite of any VR headset—the display is comfy, and since there's no head strap, it's easy to wear, even with your hair up in a bun or a ponytail. Speakers are built into the temple pieces, so headphones aren't required (though you can connect Bluetooth buds). A few downsides: There are no hand controllers, it pairs only with Android devices, and you'll need to carry a 10,000-mAh battery pack to power it. This headset is really most effective as a personal movie theater, so if you care more about getting in some immersive chill time than beating your friend's high score in *Beat Saber*, go with the Flow. $499

← BEST FOR WORK

HTC Vive Focus 3

The Focus 3 is first and foremost designed for business use. It's important to say that up front because of its whopping cost. Like the Quest, it uses inside-out tracking—sensors on the headset map the room and note the position of the included hand controllers—so you don't need to set up external sensors. It's well built and comfortable, though it's quite bulky compared to the Quest, probably to accommodate the bigger battery that powers up to 15 hours of continuous use. You can even swap in fresh batteries for longer sessions. However (and this is a big one), it's not really for gaming. Sure, you can tether it to a PC running SteamVR, but I wasn't able to get games to render at the headset's full 5K resolution. It's much better at the tasks it was made for: meetings, presentations, previewing 3D models in real space, and helping you work more productively in virtual worlds. $1,300

BEAT SABER is *Guitar Hero* with lightsabers. It's a rhythm game, but instead of pushing buttons to match the notes, you slice them in half with glowing laser swords. Expect one hell of a workout. $30

WIRED RECOMMENDS

The latest picks from our reviews team.

Ankarsrum Assistent Original Stand Mixer

→RATING: 9/10 $700

WIRED
Fantastic at bread dough: unfazed by making a ton of it in its monstrous 7-quart bowl. The attachments don't spin, the *bowl* does. If you are a home baker who has pushed a conventional stand mixer till its motor burned out, the Ank just might be the one for you.

TIRED
Not for the inexperienced. Recipes are not written for this style of mixer, and the manual is a bit laissez-faire about which attachments to use for what. More into cookies, cakes, and meringues? A regular stand mixer is a safer bet. —Joe Ray

Polestar 2 EV

→RATING: 7/10 $45,900

WIRED
Quick acceleration and instant, on-demand torque at highway speeds. Sporty handling. One-pedal driving. Heated power front seats, LED headlights and taillights, touchless entry, and dual-zone automatic AC come standard. Intuitive touchscreen controls with a Google-designed UI.

TIRED
No 300-plus-mile range option—base model gets 270. Texture of the optional eco seat fabric is a bit rough for its premium price. Looming rivals like the Kia EV6 and BMW i4 eDrive40 could overtake it.
—Matt Jancer

Garmin Fenix 7S Sapphire Solar

→RATING: 8/10 $900

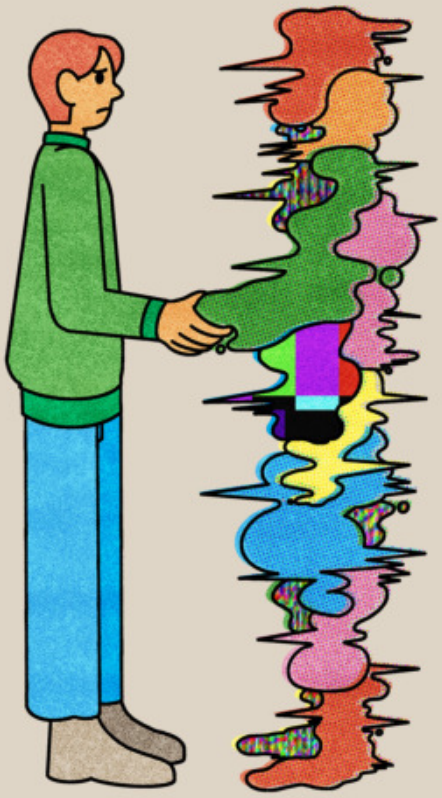
WIRED
A beautiful *and* rugged fitness tracker. Sport-specific metrics for nearly every activity under the sun (and in the gym). Speedy and accurate GPS satellite connection. Much-improved solar charging compared with previous Garmin models.

TIRED
Freakishly expensive. Some of its software-based feedback isn't really very useful for experienced athletes.
—Adrienne So

For the full reviews of these products and more, visit WIRED.com/gear.

DEAR CLOUD SUPPORT:

My Data Is Consuming My Life



Recently my laptop started glitching. I backed up 90 gigs of photos, videos, and ideas for a novel, fixed the issue, and moved everything back again. It took three weeks. Managing my digital life is becoming my life. But I don't want to lose the memories attached to these bits and bytes. What can I do? —CURATING MY LIFE

Dear Curating,

The glitching laptop is a rude awakening, not unlike a brush with death. One day you're blithely opening and saving files as though the device and everything it contained were immortal; the next, the contents of your hard drive are flashing before your eyes—wedding photos, videos of your kids, novels or dissertations in various stages of completion—and you see, with sudden clarity, the headlong folly of storing so many invaluable items in one place. I'm not being facetious. Not entirely. To watch all that information disappear, in one fell swoop, would be devastating, similar to losing all your possessions in a fire or flood, acts of God that have, at least, the compensatory benefit of endowing the victim with an aura of cosmic tragedy. The saga of a dead hard drive, on the other hand, is so commonplace, so lacking in tragic vision, that it's unlikely to garner more than a few performative murmurs of condolence, along with the inevitable question: "You didn't have backups?"

All worldly possessions are prone to attrition and decline. The more you have, the more your life becomes devoted to the vigilant, custodial work of maintenance and repair. This is why so many spiritual traditions advise against becoming attached to material things. When Christ recommended storing up one's treasure in heaven, "where neither moth nor rust consumes and where thieves do not break in and steal," he was drawing on a Jewish tradition that envisioned heaven as an eternal storehouse

Cloud Support: Spiritual Troubleshooting for the Digital Age

For philosophical guidance on encounters with technology, write to cloudsupport@WIRED.com.

for spiritual rewards. The teaching also reflects a much deeper strain of Western philosophy, one that goes back to Plato and persists today: the notion that the physical world is inferior to the unchanging realm of the immaterial, that we should not become entranced by the elusive objects here on earth but look instead to the higher, intangible things (virtue, relationships, intellectual pursuits) that are immune to the inexorable wear and tear of time.

If it seems odd to think of files and personal data as "possessions," it's because they appear to already belong to the spiritual realm. Information has no visible substance. It's not composed of matter or energy, at least not in the same sense as a table or a lump of gold. Our files, photos, and music appear magically across multiple devices, much like the Greek psyche, which could, through the mysterious work of transmigration, manifest in different physical bodies after its host had died. It's easy to believe that data will exist forever—or, at the very least, survive us, carrying our spirit (our voice, our words, our image) into the eternal ether.

This is not a particularly new delusion. Long before the advent of the digital age, information was a vehicle for immortality, the means by which artists and intellectuals attempted to live on after death. Nietzsche pointed out that the thinker who has "put the best of himself into his work" can rest easy as he watches the erosion of his own body: "It is as if he were in a corner watching a thief at his safe, while knowing that it is empty, his treasure being elsewhere." We too sleep soundly knowing that our most valued thoughts and memories reside in the cloud, our own celestial storehouse, where neither flood nor fire, moths nor malware can harm them.

I suppose what I'm trying to say, Curating, is that there appears to be a deeper, existential angst lurking within your question, one that extends beyond simple concerns about file management. Your acknowledgment that your memories are "attached to these bits and bytes" signals an awareness that your identity is mysteriously bound up with those files, that to lose them would be to lose, in a very real sense, an extension of your own mind. Would you be able to remember that trip to Europe without the photos you took? If you can never again read through the folder of journal entries you wrote in college, will you have lost that period of your life?

We are constantly offloading parts of our minds to our tools, blurring the boundaries between ourselves and our devices. The fragility of those externalized memories dawns on you slowly with age, as portions of your former selves get buried with defunct hardware or fade into the digital void from whence they came, casualties of content drift and link rot. The sudden nostalgic impulse that spurs you to Google your undergraduate blog ends at the impasse of a "Page not found." Or you sign in to a long-abandoned Yahoo account only to discover that an entire decade of email correspondence has disappeared. Even cloud storage is not immune to the indomitable forces of nature, as Google discovered when one of its data centers in Belgium was hit by a series of lightning strikes.

But I'd argue that your angst is even more complex. It's difficult to witness a device on the fritz without thinking about the fragility of your own personal OS (so to speak). Our culture's long-standing dualism endures in the popular notion that the mind is a software program running on the hardware of our physical forms. If the glitching laptop awakens you to the obvious fact that your data is entirely dependent on material processes—forcing you to recall the silicon and copper embedded in your SSD, the ghostly blue light of server farms housed in the bowels of corporate facilities—it also drives home the larger truth that all things, no matter how lofty or transcendent, depend on some kind of material substrate. Just as your data is tethered to so much ungainly hardware, so your own mind—perhaps, even, what you think of as your spirit—is fastened, as Yeats memorably put it, to a dying animal.

Poets and writers have been contending with this problem for centuries, and you might find some solace in their words. D. H. Lawrence, for example, wrote memorably about the human desire to endure, after death, as information. He was skeptical of the philosopher who believed he would live on in his work, or the saint who believed his teachings would make him immortal. Even the most prolific human "ends in his own finger-tips," and the idea that one's work can take on a life of its own is pure delusion. "The message or teaching of the philosopher or saint, isn't alive at all, but just a tremulation upon the ether, like a radio message," Lawrence wrote.

Although our technologies have since advanced, the truth of his words remains: Data is merely a fragile vibration, capable of traveling across great distances but stuck, ultimately, in a meaningless limbo so long as it is without witness. All those files you have stored on external hard drives or ensconced in the cloud are not "informative" in any meaningful sense unless they are experienced by another mind—or, as Lawrence put it, until they "reach another man alive." Perhaps you should let go of the notion that your identity is forever encrypted in your data and instead focus on communicating that information to someone else. Forward to friends those old email chains you discovered in your long-abandoned mailbox. Consider trying to finish and publish that half-completed novel that's been lingering in your files—not as some misdirected gesture toward life extension but as a genuine transmission to a good-faith reader. Ensure that your diaries and photos will be handed down to your descendants. It's only in those minds, and in those living spirits, that you will continue to exist long after your own hardware has failed.

Faithfully, Cloud

MEGHAN O'GIEBLYN *is the author, most recently, of* God, Human, Animal, Machine.

ILLUSTRATION / MARK WANG

VANITY FAIR

DYNASTY

THE HOUSE OF WINDSOR

A new podcast hosted by

KATIE NICHOLL *and* **ERIN VANDERHOOF**

**UNIMAGINABLE SECRETS. UNYIELDING POWER.
DEVASTATING RIFTS AND SHOCKING ALLEGIANCES.**

Vanity Fair's DYNASTY goes inside the complex dynamics of the royal family—from the queen's early reign up through the scandals rocking their world today—with razor-sharp insight, fresh reportage, and exclusive guests.

Listen now at
VF.COM/DYNASTY

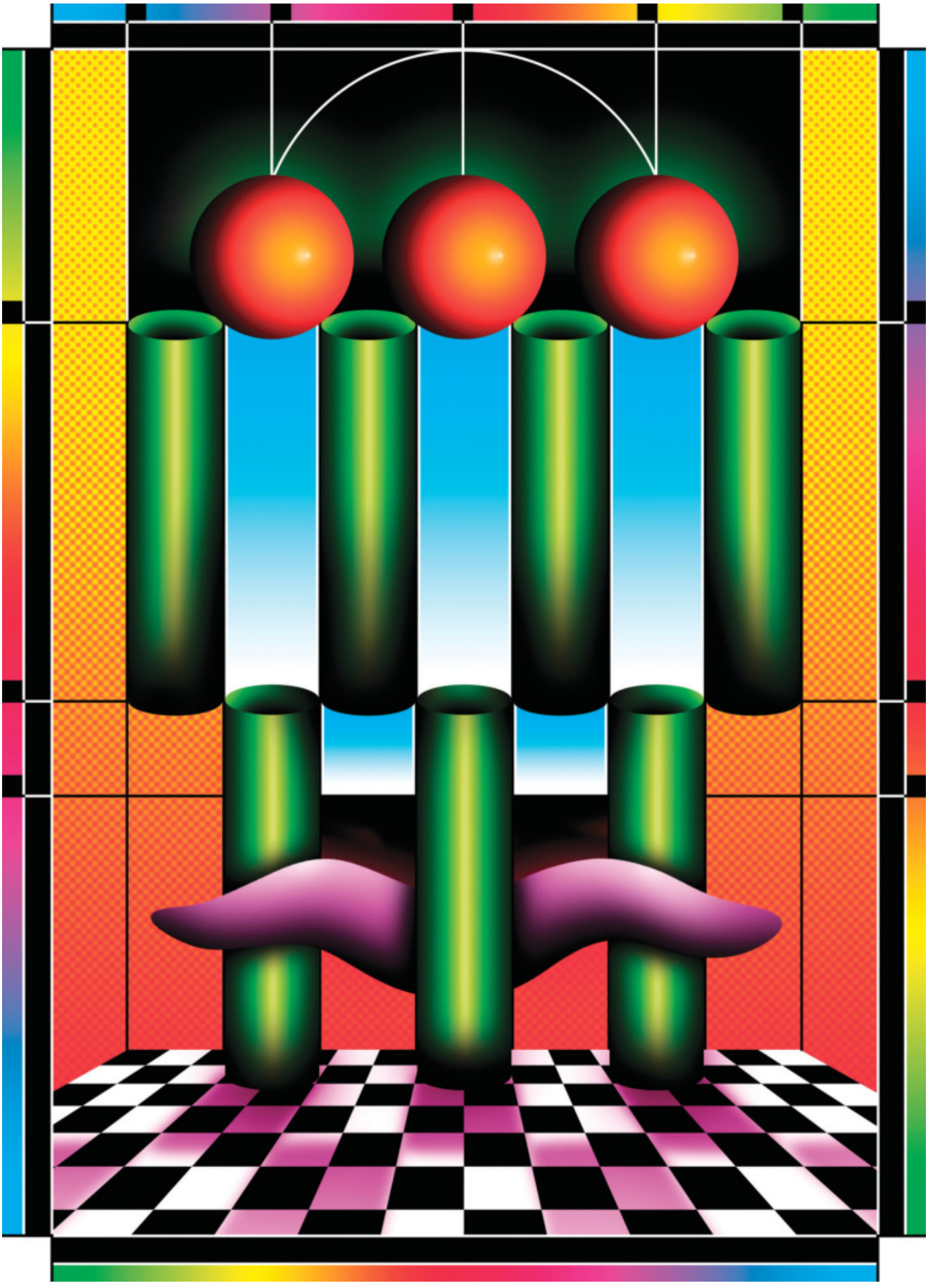
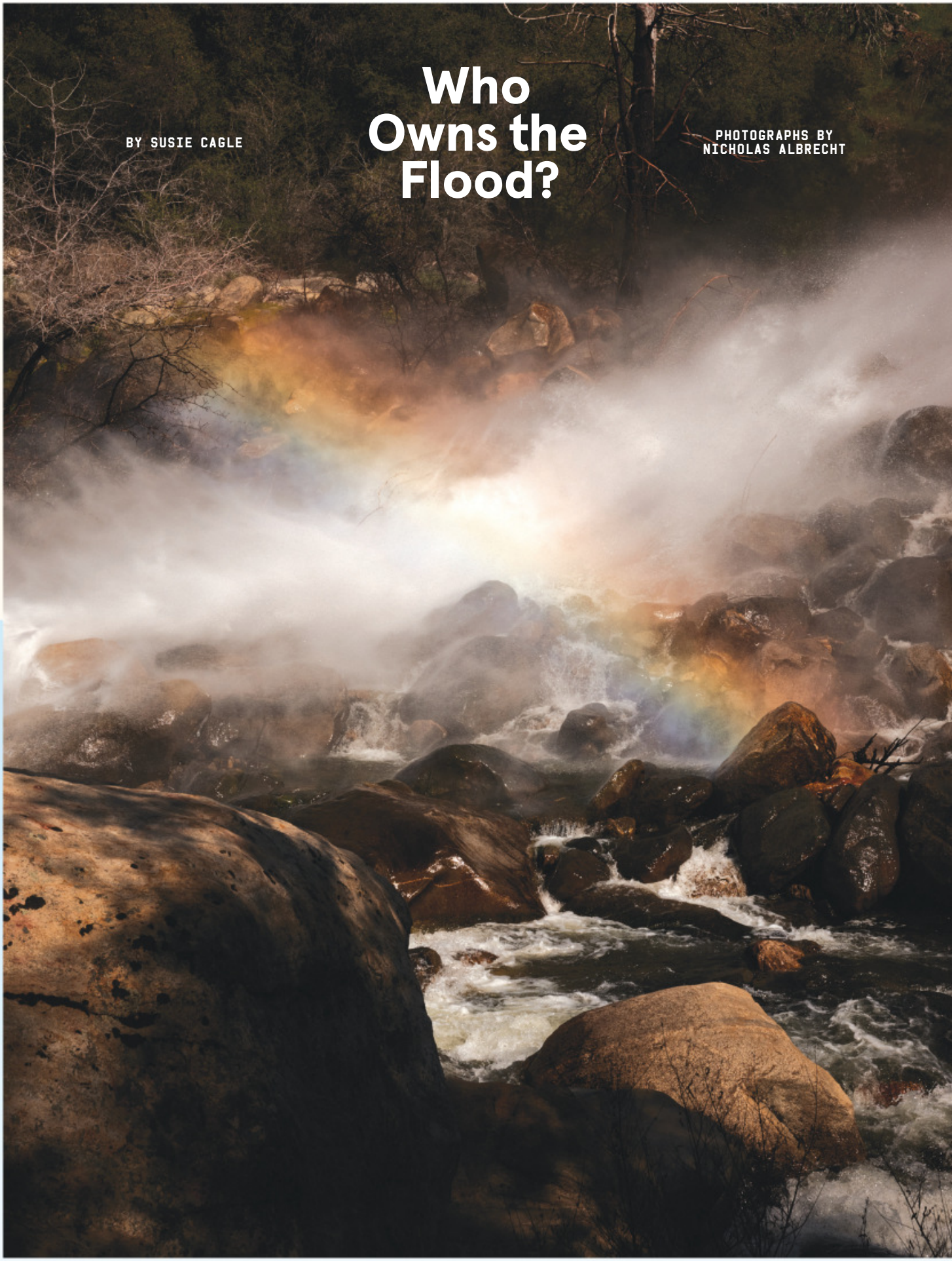


ILLUSTRATION / SAMUEL FINCH

Who Owns the Flood?

BY SUSIE CAGLE

PHOTOGRAPHS BY NICHOLAS ALBRECHT



DRIVEN BY CALIFORNIA'S INTENSIFYING CYCLES OF DROUGHT AND DELUGE, A CENTRAL VALLEY FARMER WENT ALL IN ON A TRICKLE-DOWN SURVIVAL TACTIC.

HIS IDEA COULD HELP SAVE AMERICA'S AGRICULTURAL HEARTLAND—EVEN IF HE BECOMES A CASUALTY OF THE STATE'S NEXT WATER WAR.

In the fields at Terranova Ranch, it was as if a disaster had arrived.

Don Cameron, clad in dark green waders, sloshed through the pond that had formed in his orchards and vineyards. More of his crops were underwater than at any time since he began farming in California's San Joaquin Valley—a quarter of the almonds, a third of the grapes, half the pistachios, and all of the walnuts and olives. Most of his neighbors would have been racing to pump out their fields; accepted agricultural wisdom holds that too much water will suffocate the roots. About an hour's drive southeast, farmers were so desperate to hold the flood back that they dropped sandbags from rented helicopters. At Terranova, Cameron took an entirely different tack. He measured the depth of the drink and inspected the new growth on his vines and trees. Then he ordered more water to come.

It was early 2017, and after five years of drought the valley was in the midst of its second-wettest year on record. A total of 53 gargantuan storms, known as atmospheric rivers, soaked the West Coast. There were landslides and blackouts. Dams crested, century-old giant sequoia trees toppled, and a stretch of the Central Coast was cut off from the rest of the state. Tens of thousands of people fled their homes, and at least five died. In the peaks of the Sierra Nevada, the snowpack reached its highest level in years.

The flooding was unpredictable, but it was not unexpected. California's weather lurches between wet and dry. To calculate the state's average annual precipitation is to do a rather meaningless bit of arithmetic. This particular flood took a while to reach Cameron. From the mountains, it poured into the upper portion of the Kings River, then into Pine Flat Lake, a dammed reservoir 100 miles upstream of Terranova. By late February, the dam operators were releasing more than 400 acre-feet per hour into the lower river—enough water to flood 400 acres of grapes or almonds shin-deep. As the weather warmed, snowmelt brought a second flood. Water heaved down the Sierra slopes and roared through the canyons, pushing Pine Flat beyond capacity. At peak outflow, the reservoir was releasing nearly 1,200 acre-feet per hour.

Cameron had been dreaming of a deluge like this since 1983 and building for it since 2010, but he wasn't ready when it came. His project was years behind schedule: The pumps weren't installed; the canals weren't fully dug. The best he had been able to do was rely on rented diesel pumps and an old pipeline to pull water out of the Kings as fast as he could. From winter through spring, he managed to keep the crops wet, siphoning more than 3,000 acre-feet off the river, lamenting that he couldn't take more. One vineyard of robust Italian Barbera wine grapes that needed 2 acre-feet of water in a year got 13 acre-feet in a season. Ducks moved in as the branches flowered. Come summer harvest, the grapes were as sweet as ever.

The real success story, though, lay in the ground beneath Terranova. In a typical year, that's where most of the farm's water comes from. Cameron and his neighbors do not hold rights to any nearby river, or to the supplies piped in through government projects; they either buy from people who do or, more often, pump what they need out of the aquifers. A system of natural subterranean reservoirs stretches beneath the San Joaquin and Sacramento Valleys, which together form the Central Valley. The region is pincushioned with more than 100,000 wells. People and businesses have pumped out so much water that whole towns sink into the hollows.

While Terranova stood firm, its aquifer was in trouble. Cameron and his neighbors had taxed the ground so heavily over the years that there was a 230-foot-deep dry zone, or "cone of depression," in the water table beneath the ranch. But after the 2017 flood, after the last of the rain and snowmelt had trickled down into the aquifer, the water level rose 40 feet. Cameron swore that when the next flood came, he would be ready to gulp down even more.

Cameron didn't come up with the idea of using floodwater to refill aquifers, but he did earn a reputation as the godfather of the practice. In a valley dotted with ponds and basins built for the sole purpose of holding extra water as it percolates down into the ground, he was the first farmer foolhardy enough to experiment on his own harvest. His work earned him state and county prizes for innovation. In 2018 he was appointed president of California's agriculture board. He thought—hoped—that on-farm recharge might become one piece of the future-proofing necessary to save the country's most productive agricultural region from near-certain death.

The stakes are high: California grows more than a third of the vegetables and two-thirds of the fruits and nuts eaten in the United States, dominating pro-

Opening spread, left: *Spray from a hydroelectric plant on the Kings River in California.* Right: *Don Cameron walks some of the land he will flood in order to recharge dried-out aquifers.* This page: *Cameron in a small greenhouse outside his office at Terranova Ranch.*

duction of artichokes, avocados, broccoli, cauliflower, carrots, celery, dates, grapes, garlic, olives, plums, peaches, walnuts, pistachios, lemons, sweet rice, and lettuce. The Central Valley is America's agricultural heartland, crucially important to the state's economy and the groceries of the nation. More wine grapes are grown there than in California's wine country, more almonds than anywhere else on earth. There are more than a quarter of a million acres devoted to tomatoes, which when plucked, weighed, canned, and shipped add up to around a third of all the processed tomato stuff eaten worldwide. And that's not to mention all the region's livestock—chickens, pigs, cows.

Ever since the first crops were planted, though, people have used more water than nature could replace. In the past eight decades, more than 120 million acre-feet have been siphoned out of the aquifers. The deficit grows by an average of 1.8 million acre-feet each year. Meanwhile, climate change is poised to amp California's mercurial weather cycles to new extremes. The droughts will be drier and longer, the floods higher and faster. Unless farming and water-management practices change, the region is facing an existential crisis. A report from the Public Policy Institute of California included a stark projection: To balance the water budget and protect the groundwater on which most Californians depend, as many as 780,000 acres of farmland would need to be fallowed.

Cameron's project suggested the possibility of another path: What if you could capture one disaster and use it to mitigate the other? What if you could do what California's climate couldn't and average out the floods and droughts? The depleted aquifers beneath the Central Valley could hold an estimated 140 million acre-feet—three times more water than all the state's reservoirs combined—and they could do it for a small fraction of the price of surface storage. Water kept underground isn't lost to evaporation, which will only speed up with a hotter, drier climate. Best of all, from a farmer's perspective, Cameron's techniques wouldn't necessarily require fallowing land before flooding it.

There would be risks, sure. But for Cameron, there is no viable alternative. "I have growers tell me that there's no way in hell they're going to flood their almonds," he says. "They say, 'If I get a wind, my trees are gonna blow down.' And I say, 'Well, that's fine, you can worry about that or you can not do anything and you'll only be farming half of those trees anyway.'"

So yes, outside the Kings River Basin, Cameron is a revered farmer and business leader, hailed as a visionary at the vanguard of climate adaptation. Inside the basin, though, things aren't so simple. Here, according to his ally Matt Hurley, who runs the organization that oversees aquifer use in and around Terranova, Cameron is "probably one of the most hated people."

The problem is the flood, the excess acre-footage that Cameron needs to make his plan work. It doesn't belong to him. It might not belong to anyone. Because that water only flows every few years, it was always treated as a periodic inconvenience, if not a disaster. The flood "was something everybody wanted to get rid of," Cameron says. Then, right as he "went crazy" drowning his acres at Terranova, it became something everybody wanted. A land developer with dealings all over the state and an outside water district made a claim on it, arguing that the Kings River surge was going to waste and should instead belong to them. The river's existing rights hold-

ers were incensed; local residents were worried. Caught in the middle, Cameron's paradigm-shifting recharge project was at risk of running dry.

The outcome of the Kings River conflict will ramify throughout the Central Valley and the state. It is an early skirmish in the slow-building water war that may consume this region as the climate crisis wrings it dry. At its heart is a savage question: When drought is coming for everyone, who owns the flood?

—

THE WORST CALIFORNIA DELUGE ON record came early in the Golden State's life. Between December 1861 and January 1862, there were weeks of continuous rain and snow. Governor-elect Leland Stanford took a rowboat to his inauguration. Thousands of cattle drowned; whole towns were swept away. The flood pooled in the low, fertile valleys where farms would one day grow their riches. The capital was temporarily moved to San Francisco while Sacramento dried out. The state went bankrupt. And then everyone forgot.

In the wake of that catastrophe, settlers in the Central Valley began building their agrarian paradise. Over time, they terraformed the land, changing it beyond recognition, ruthless in their management of water. Where there was too much, they dammed it dry. Where there was not enough, they brought it in. And when it didn't come during growing season, they tapped it from below. By the turn of the last century, they had drained Tulare Lake, formerly the largest freshwater lake west of the Mississippi. They spent the next decades corralling its tributaries. The largest of these was the Kings River.

The land along the westernmost section of the river was forever marshy. The groundwater here flows from the Sierra foothills in the northeast; if the mountains are at the shallow end of a big subterranean swimming pool, this is the deep end. Unable to farm this vibrant aquatic habitat, people drilled it full of wells. When the wetlands dried up, the land became arable. This was how, after decades, a riparian swamp became Terranova Ranch.

The land that Cameron farms is just outside the town of Helm, which boasts a post office, a gas station, an elementary school, and fewer than 10 paltry inches of rain per year. It is in the McMullin Area, the only groundwater district in the Kings subbasin not served by the actual river. The end of the North Fork of the Kings runs nearby, and it still floods every few years. Most of the time, though, it is desiccated and weed-filled, an expanse of beige and ocher interrupted by scrubby bursts of pale green and gray.

This is the case in the fall of 2021, when Cameron and I drive out to the edge of the ranch. "It looks like a desert," he says. "It doesn't look like a river. But when the water comes"—he pauses in wonderment—"everything comes alive."

Standing in the dust, Cameron, 69, cuts a slim but sturdy figure. He has a medium build and a long gait, his face creased by sun and time. With his hands in his pockets and mud on his boots, he stands a few inches shy of 6 feet, the height of the four intake pipes that carry water from the river to Terranova. In a crisp long-sleeved oxford shirt and faded Levi's, he is the only blue in the landscape.

Where so many of his peers define themselves by their lineage, Cameron is a

first-generation farmer. He studied biology at the state college in Fresno, planning to work in wildlife management so he could spend his days in nature. When the local service wasn't hiring, Cameron turned to the region's dominant industry instead. Farming was work, and it was outside. Close enough. "And then it kind of got under my skin," he says. "I love the challenge."

Cameron began working at Terranova in 1981, and it has been nothing if not a challenge. The farm's two dozen or so crops (conventional and organic, so many he can't list them all off the top of his head—almonds, pistachios, bell peppers, carrots, onions, garlic, olives for oil, tomatoes for canning, grapes for wine) rely on some 55 wells. Since his first season, Cameron has seen the water table drop by a foot or more each year. But he has also seen the Kings roar with potential.

The winter of 1982–83 was the wettest ever recorded on the river. On his commute between the ranch and his home at the time in Fresno, Cameron watched with apprehension as overflow from the nearby San Joaquin River inundated a vineyard at the low point of the floodplain. But he was amazed to find that the plants weren't smothered. Every day that spring and into the summer, the vines stretched, the leaves unfurled, and the grapes grew unharmed above the flood.

At capacity, Pine Flat Lake can hold a million acre-feet of water.

Those two years, he used more than 9,000 acre-feet of spare Kings floodwater. He did the same in subsequent wet years: 1984, 1986, 1987, 1995, 1996. In 1997, the Kings River Water Association, which manages rights and records inflows and outflows, agreed to allow Terranova to sip the extra floodwater for $2 per acre-foot. Otherwise it would at best flow out to the San Francisco Bay, at worst flood someone downstream.

Still, each year the water below Terranova's fields receded deeper, further out of Cameron's reach. By 2009, he had instituted every irrigation efficiency he could think of. He set his sights on something bigger, a flood-and-recharge project that would skim the peaks off the river and send them back underground—in other words, pay down the aquifer debt. A few hours' drive to the north, in Yolo County, a lanky engineer named Philip Bachand was looking to try something similar. The two men teamed up, the match made by a mutual contact at the US Department of Agriculture, and by the end of 2010 they had a $75,000 grant from the agency. That was only enough for a shoestring budget, but how complicated could it be? "At the most basic level, it's just throwing water on land, right?" Bachand tells me.

The night that "kicked this whole thing off," Cameron recalls, was a cold evening in December 2010. He and Bachand were touring Terranova, looking for the best 1,100 acres to flood as the light was fading in the valley fog. They decided the lands that would grow the farm's carrots, peppers, and tomatoes later in the year were top contenders. Bachand would make them look like rice fields, terraced and waterlogged. But the deluge offered more water than those acres could hold. Cameron thought of 1983 and the accidentally flooded fields along the San Joaquin. He pointed at a vineyard of Barbera. "We can blitz-flood all our grapes," he said. "Let's go."

Bachand was surprised, but Cameron

insisted. He figured that the ad hoc hydroponic environment would hold enough oxygen that the grapes could still thrive. The team pumped in enough water to submerge the roots; when the soil absorbed it, they pumped in more. Cameron checked on the vines daily, looking for any sign of stress. When the new spring leaves began to develop a yellow tinge, he sent the flood somewhere else, and they darkened to cool viridian again.

By August, Bachand and Cameron had sent more than 1,000 acre-feet of water back into the aquifer. They had used twice that much just to water other crops on the ranch, preventing the groundwater debt from accruing further. By Bachand's reckoning, the water cost about a third of what Terranova would have spent pulling the same amount from underground. Having proved their concept, they secured $5 million from the California Department of Water Resources to engineer the permanent infrastructure they'd need to move floodwater across all of Terranova's 5,500 acres. They built and built for that next flood—and while they did, the state descended into another drought.

—

AGRIBUSINESS LOVES THE MESSAGE OF ON-FARM recharge. After years as water villains, growers get to be part of the solution. The Almond Board of California, whose embattled nut swallows 13 percent of all agricultural water in the state, is an especially ardent booster. But Cameron's technique is not a miracle that will deliver the San Joaquin Valley from all of its demons. Cash crops aren't alone in relying on the groundwater here. Many thousands of people do too, and they have reason to be skeptical of solutions that privilege agricultural needs.

In times of drought, farmers effectively compete with neighboring communities for water. In the race to the bottom of the valley aquifers, growers can pump so much that thousands of residential wells sputter and die. While the almond trees stay green, families wash their dishes with bottled water. Efforts to recharge more and pump less are welcome—any drop in this beleaguered bucket—but some in the valley would rather see farmers fallow the fields along riverbanks, pull back the levees, and restore the old floodplain wetlands. Fish and other wildlife would likely agree. Before the rivers were contained for society's purported benefit, flooding was a natural part of the riparian life cycle.

In the short term, groundwater recharge could worsen another of the valley's woes. The entire region is polluted with fertilizer compounds, which leach into the soil, then into the aquifers, then into the drinking water, where they can be especially harmful to infants and small children. Residential areas across the San Joaquin Valley are also hot spots for the pesticide additive 1,2,3-Trichloropropane, which likely contributes to cancer. Throwing water on the land would flush these contaminants into the aquifers much faster than otherwise. In the longer term, though, the legacy contamination would be diluted with pristine Sierra snowmelt. Cameron works with Helen Dahlke, a hydrologist at UC Davis, to measure nutrients and chemicals in Terranova's soil and water using sensors in the ground. Recent soil samples turned up residue from a handful of pesticides; more testing is needed to determine what's ending up in the water. "I'd rather know," Cameron says.

But even if on-farm recharge is proven safe, beneficial, and arguably necessary for the fish, the crops, the land, and the residents—even if all of that happens, the Terranova project could still wither on the vine. Cameron's biggest hurdle has always been politics. In 2014, mid-drought, Governor Jerry Brown signed into law the Sustainable Groundwater Management Act. The law charged locals with crafting and imposing their own groundwater sustainability plans. This involved self-organizing dozens of new agencies across 21 "critically overdrafted" basins, many of them in the San Joaquin Valley. These agencies, dominated by agricultural users, were left with two options: consume less water, or figure out where to get more.

Until that point, California law had been largely silent on the question of groundwater ownership. If the land was yours, you could drill as deep as you liked. Surface water, on the other hand, had been regulated since the Gold Rush. The rules said that if you were the first to claim the water—even if it wasn't on your land—then you had a right to it. You kept that right as

Steve Haugen, "watermaster" of the Kings River Water Association, in his office in Fresno.

Helen Dahlke tests the groundwater at an agricultural research center in Fresno County.

long as you didn't let the water go to waste. In other words: Finders keepers, and use it or lose it. On the Kings River, the first rights permit dates back to 1916, and the water was declared "fully appropriated" in 1989. But the river still flooded, and some of the flood never made it onto the books. Was it truly all appropriated, or could there be something left over? The Sustainable Groundwater Management Act put every unaccounted-for drop in play.

Seemingly no one understood the opportunity this presented better than the land developer John Vidovich. The 66-year-old grew up on the peninsula south of San Francisco as the region was changing identity, transitioning from the fruit-farming "Valley of Heart's Delight" to Silicon Valley. His father, one of the first to get wise, took the 20 acres of apricots and cherries the family farmed and turned them into a shopping center. The elder Vidovich built a regional real estate powerhouse, which the younger Vidovich grew into a statewide empire. His investment firm, Sandridge Partners, has amassed more than 100,000 acres of agricultural land in the San Joaquin Valley. Some of it is planted with almonds, but most of it Vidovich uses for its associated water rights, allocations, and access. That's where the real money lies.

Some of Vidovich's state-spanning water deals are more infamous than others. In one case, he sold a water agency near Los Angeles the rights to surface water tied to a piece of farmland, then pumped up groundwater from the same plot and sent at least some of it via clandestine pipeline to the juggernaut Wonderful Company, a major grower of mandarins, pomegranates, pistachios, and almonds.

In 2016, Vidovich signed another valley-spanning deal, this one even bigger: the Tulare Lake Storage and Floodwater Protection Project. It would route the Kings River floodwater not north toward Terranova but south, to a new reservoir that would be built on Sandridge land. Vidovich would sell the rights to use the land and build the reservoir to Semitropic, a water storage district on the southern side of the dry Tulare lake bed. Semitropic already ran a groundwater bank, a kind of underground reservoir that could stockpile as much as 1.65 million acre-feet for its account holders. It planned to pay for the new $600 million project with state funds.

Whether the idea was originally Vidovich's brainstorm or Semitropic's isn't clear; neither party responded to multiple requests for comment. Nor is it clear when they thought it up—although in mid-2014, Semitropic began pouring money into lobbying the state legislature on water storage issues. Certainly it was a good deal for Vidovich. Semitropic would pay the water mogul $40 million for the easement on the land. He would also get priority rights to floodwater—not just from the Kings but also any other tributaries—and access to the California Aqueduct, which carries water from the northern part of the state to the south. He would be able to transport groundwater across his growing empire or, some feared, sell it to someone even thirstier. (Vidovich told an interviewer in 2017, "Even if I were to move water and sell it, it would be to farming operations.")

Where the rights holders were riled by

the Semitropic proposal—"sharpening our knives" for the "pirates at the door," one told a local reporter—Steve Haugen didn't flinch. Haugen bears the weighty title of "watermaster" for the Kings River Water Association, which protects the interests of the 28 member units of the river's watered gentry, both upstream and downstream from Terranova. His nerves are cool after 30 years working on one of the largest rivers in the Sierra. "The history books are riddled with hundreds of unimplemented projects on the Kings alone," he tells me. "So yeah, hydraulically the concept works. Politically, financially, it's hard to believe that would work."

Middle-aged, with graying hair and wire-rimmed glasses, Haugen folds and refolds his hands and looks down as he speaks, measuring his statements with the same consideration he has shown in decades of measuring the river's flow. The low-ceilinged conference room next-door to his office, where the members meet, is lined with black-and-white photos of Sierra peaks covered in a thick layer of snowpack. They're lit with the reverence shown to gilded portraits of saints.

For all Haugen's calm talk, Semitropic argues that it was his agency that left the door open to a challenge. It held two water licenses from the state that covered the flood on the Kings—but didn't consistently report water use on either of them. On paper, the water went to waste, which meant that it could now be up for grabs. (See the second sacred tenet of California water law: Use it or lose it.) Semitropic had staked $40 million on what appeared to be a record-keeping gaffe.

In response, the Kings River Water Association claimed that it was all a misunderstanding. The accounting was correct; the organization had just put the numbers in the wrong places. A "simplified reporting method," the attorneys called it. Sure, the river flooded sometimes, but those were rare events, outside of their control. And anyway, now member units and local groundwater agencies had their own ambitious recharge plans.

Haugen says that he and other Kings River representatives tried to negotiate with the would-be attackers. They met around half a dozen times between late 2016 and early 2017. Haugen says they could've given a little—they had, after all, been selling that floodwater in deals like the one with Terranova for decades. But, he says, Semitropic wanted a permanent right to the extra water, which the association wasn't willing to give up for any price.

They ended up on the proverbial courthouse steps, in a battle over whether to crack open the book on the Kings for the first time in decades. In May 2017, three of the Kings River districts filed claims to a million acre-feet of water that they said they already owned—an amount equivalent to more than half the average annual run of the Kings. Sixteen days later, Semitropic filed a petition claiming that the river's "fully appropriated" status should be revoked or revised, along with an application for rights to 1.6 million acre-feet.

This all sounded to me like very bad news for Don Cameron and his big empty pipes out by Helm—which would very likely stay empty if Semitropic were to win. But he and the rest of the board at the McMullin groundwater agency couldn't join the coalition condemning Semitropic's "water grab." It would have required endorsing the claim that the river had no water to spare. And if that were true, Cameron wouldn't be the Department of Water Resources' golden godfather of recharge.

The river users were not happy that McMullin had failed to take their side. They responded with icy hostility. Haugen, the Kings' watermaster, remains unimpressed by Cameron's project. "We've been doing groundwater recharge in the service area for a century now," he tells me. "I've got plans that can fully put that water to use." If Terranova wants to help with flood control now and again, that's fine, he says. "But there are no assurances that there's ever water for a flood control project," he continues, offering a grim smile. "Folks want to see our local area sustainable. And there are ways to do it cooperatively."

But not, apparently, on the Kings. In 2020, Haugen's association canceled all the river's floodwater agreements, including the one it had maintained with Terranova for nearly 25 years. Cameron would have to find another way.

—

"There's some land out there that's better used as a parking lot than what they're attempting to grow on it."

ON THE FIRST FLOOR OF A SMALL office building, in the middle of Kerman, California—population about 16,000, one Walmart, one Starbucks—Matt Hurley is drowning in paperwork. He is the general manager of the McMullin Area Groundwater Sustainability Agency and its only full-time staff member. His reception area is cluttered with stacks of large paper maps and plans, and cardboard boxes in various stages of unpack. "I got a few demerits when I was young, and I still need to get a few brownie points to offset those, because I still may be taking the wrong elevator if I'm not careful," he says. "Hopefully, I can do good on my time left on this planet before I check out."

At 68 years old, Hurley is the personification of a strong handshake, tall and booming in a dark blue polo shirt, jeans, and black cowboy boots, with silvery white side-parted hair and a mustache that curls down around the corners. He talks fast and peppers his speech with the folksy self-deprecation of a local agriculturalist ("You'll figure out I'm wacky as a wooden watch"), which he is not.

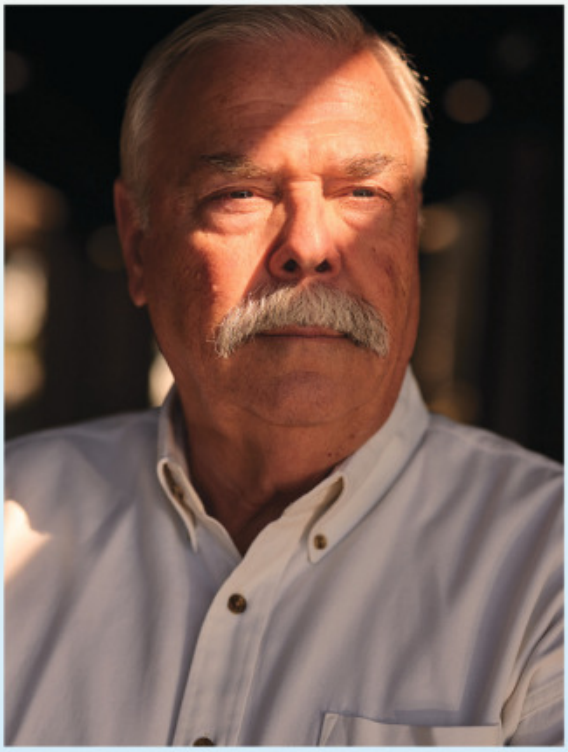
Hurley came to McMullin from a water district further south, where John Vidovich owns the majority of property. A 2017 article in *The Bakersfield Californian* reported that some considered him Vidovich's "henchman," obliged to do Sandridge's bidding. Hurley denied that the relationship was anything more than water district manager and water-wealthy ag king. Now he says that Vidovich is a longtime close family friend and his daughter's godfather, that Vidovich asked and he provided legal advice on the sale of the $40 million easement to Semitropic, and that, following other asks for other favors, they haven't spoken since April 6, 2018. Vidovich wanted him to do things that were "gray at best," Hurley tells me. "He just doesn't quite get what the whole picture looks like anymore. He's so driven by making Sandridge bigger and better."

By the time Hurley got to McMullin, he knew there was extra floodwater on the Kings—and he knew the area's depleted aquifer could in fact be a huge asset. Unlike other parts of the valley, the McMullin Area hasn't sunk into the emptied space of its exploited aquifer, making it a natural subterranean water bank. It could store nearly 2 million-acre feet underground, roughly as much as two Pine Flat Lakes.

Hurley pitched himself to Cameron and the other district board members before the job even existed. During his interviews for the position, members expressed concern about his unsavory associations, his Vidovich baggage. But in a region with such apparently grim prospects, Cameron says, they needed "a bulldog." McMullin is the only district in the basin whose landowners don't have rights to surface water; being so aquifer-dependent, it is held responsible by its neighboring agencies for three-quarters of the area's annual groundwater deficit. Without any new sources of water, or exceptional leaps in efficiency, that would mean fallowing around half the acreage in the district. And the McMullin Area farmers, some of them helming fourth-generation operations, were not content to dry up and blow away.

In his Kerman office, Hurley has a map of the McMullin Area pinned to the wall. He smiles and runs a finger around its borders. "I call this my little dragon," he says. The San Joaquin River forms the top of its head, and its chest runs along the North Fork of the Kings, at Terranova. Its snout kisses the Mendota Pool, where the two waterways meet and mix. This is the future home of the Aquaterra Water Bank—a system of both recharge and underground storage, with the canals and pipelines necessary to bring water in and deliver it out to partners potentially hundreds of miles away. "It's a complete flowering of that seed" that Cameron planted at Terranova a decade ago, Hurley tells me. Every water agency in California has to keep its stock somewhere, and using a pre-existing natural vault is far cheaper than building a new reservoir.

To get Aquaterra running, McMullin would require funding from partner agencies around the state with rights to water but nowhere to store it. As part of their payment, these agencies would leave behind a portion of the water they bring in. Hurley tells me that he approached the rest of the Kings Basin first, naturally, but so far no one has signed on. He is working with a water agency that serves much of Silicon Valley (and currently banks some of its water with Semitropic) in hopes that it will be a founding partner. If that deal works out, water could begin flowing into the bank as early as late 2023.



Matt Hurley, general manager of the McMullin Area Groundwater Sustainability Agency, outside his office in the town of Kerman.

Hurley points at a spot on the map marked in yellow, one of McMullin's best recharge zones. "If you drive out there, you'd think you're at the beach," he says. "There's a huge sand dune. We can get a foot and a half, two feet of infiltration a day"—several times more than the ground at Terranova.

The sandy wetland soils may allow for a fast drip, but it is far more expensive for McMullin to engineer this flood-catching project from scratch than it would be for the irrigation districts upstream, with their existing canals, to spread the water around the eastern part of the basin. Aquifer recharge in those areas would also immediately serve the nearby disadvantaged communities, which have seen their wells go dry drought after drought. Still, they wouldn't be able to keep the recharged water from slowly flowing downhill to McMullin. Hurley axiom: "You can continue

to put the hose in the shallow end of the swimming pool all you want, but the deep end will fill up before the shallow does."

In 2019, when the McMullin district declined to side with the rest of the basin over the Semitropic plan, "you'd have thought we had killed somebody," Hurley tells me, shaking his head. The upper river users, with their old claims, did not appreciate what the western end of the basin was working on, he says: "It was the good old boys not liking some upstart [agency] telling them what to do with their water. I believe if you put them under sodium pentothal, some of those guys would say that they own that water until it was out by the Farallones."

—

BY THE TIME THE CONFLICT FINALLY got its first official hearing before the state water board in 2021, there was a whole new office to handle disagreements about water rights. After mountains of paperwork and years of anticipation, the proceedings were held remotely last June and streamed daily on YouTube. Seven engineers and other consultants presented evidence for what water was available in the river and where it had all gone. The Kings River Water Association admitted and corrected its earlier reporting mistakes—but the accounting still showed a surplus in wet years. Attorneys for the association and its member units argued that the floods were outliers, essentially so extreme as to not be considered when calculating water availability, but also vital to the basin's ability to survive onerous new sustainability regulations.

The presiding hearing officer wouldn't allow potentially inflammatory evidence about John Vidovich's water-dealing and how he stood to benefit from the Semitropic project, nor would she consider the recharge projects that the upper river districts hope to build or the communities with precarious wells. What might happen to the water in the future wasn't yet material. All that mattered in these hearings was whether it existed and where it had gone.

When it came time for Cameron and Bachand to present the Terranova project, they told the story from the beginning, acre-foot by acre-foot and dollar by dollar, accounting for all the water they had taken in the past and their plans for the future, all the public and private investment poured into the project. They were clearly nervous. Bachand swiveled back and forth in his chair; Cameron spoke deliberately, glancing away from the camera. Attorneys for Semitropic did not object to their testimony, but attorneys for the Kings River Water Association and its member districts suddenly and passionately did, just as Bachand finished the presentation. They moved for all of it to be struck from the record. They protested to the hearing officer—how was this relevant? But they'd waited too long. "We're doing this," she told them.

Every basin in the state could be adjudicated in the coming decades. No fleeting stream would flow unclaimed.

On cross-examination, the attorneys seemed to turn their frustration on Cameron. Hadn't his agreement to use the water been canceled? And wasn't the overdraft all Terranova's fault anyway? When one attorney sarcastically referred to him as the "godfather of groundwater recharge," the other, unmuted, laughed loud enough for Zoom to push his screen to the front.

The idea of investing more and more of Terranova's resources into a water project without water rights had made Cameron nervous from the start. But even after the Kings River Water Association canceled its agreement, he and the rest of the McMullin leadership held their course. With the Terranova phase completed in 2021, they aim to grow the recharge enterprise up to 30 times the size of the pilot, covering land on neighboring farms and installing the infrastructure necessary to take in as much as 1,000 acre-feet of water a day. A $10 million grant from the state will pay for it as a flood project, money from the USDA will pay for it as a recharge project, and Cameron has augmented public and private grant funds with the ranch's own $8 million. When the ditches are dug and the four gleaming white 450-horsepower pumps at Terranova are running at full capacity—assuming the necessary water rights are in place—it will be able to scoop 20 percent of historic flood totals off the river. Last fall, the McMullin Area filed its first application to the state water board for those rights. In March, it was officially added as a party to the case, an equal alongside the Kings River Water Association and Semitropic.

When I ask Cameron about the conflict—wouldn't Semitropic's claim get in the way of Terranova's project?—he leans back on the railing above the big pipes at the start of his main canal, the one Hurley calls the "concrete monolith," crosses his arms, and smiles. "We're hopeful that we'll get a little piece of the pie," he says. "Or more."

—

RESEARCH FROM LAWRENCE BERKELEY NATIONAL LABORATORY predicts the virtual demise of the Sierra snowpack in the next half century. Historically, it held nearly a third of California's water (average: 16 million acre-feet). Daniel Swain, a climatologist at UCLA, forecasts that droughts on par with

California's worst will come around twice as often, and extreme wet years like 2017 will come two and a half times as often. "Severe" floods like those in 1862, meanwhile, will be five times as frequent by 2100. Swain calls this climate whiplash. Average annual precipitation will remain relatively unchanged, but more of it will fall as warmer rain and in disastrous bursts. The fast-subsiding San Joaquin Valley towns are at even greater risk of a deluge the further they sink. Still, given the repeating disastrous droughts, most Californians "pray for rain."

Cameron used to shy away from talking about climate change. In his cohort, he told me, it would get him "laughed out of the room." Now it's hard to talk about anything else. Every year Terranova plants its tomatoes earlier and earlier, racing against the heat. The beating sun roasts the bell peppers right on the vine. When the wildfires rage in the Sierra, the smoke flows down to the valley and blots out the sky. "It looks like the middle of winter with a fog layer," Cameron says. "The sunlight barely makes it through." The plants grow lankier, reaching for light they'll never find. Recently, two of the farm's wells ran dry. "It's been probably more stress on the system than I've ever seen," he says.

Cameron says farmers are pulling back on almonds, replacing them with less water-intensive pistachios. His friends are taking a cue from Vidovich and buying more farmland, not to grow more crops but to claim more water. McMullin is beginning to install pump meters to track and trace every cubic foot coming out of the aquifer.

Last December, ample rainfall reduced the region's drought from "exceptional" to "extreme." In some places, it even reached the relatively benign "severe." Cameron was briefly hopeful—maybe they'd see a flood this year. Then, whiplash: one of the driest Januarys on California's books. In February, the state launched a program to buy and fallow farmland, the end of the line for some of the valley's small family legacies. Cameron is under no illusions about his own lineage in agriculture: His son went into water law.

Sixteen years ago, Cameron and his wife, Elisa, moved from Fresno to the ranch. Their house is raised to protect it from flooding, and the backyard looks like a little slip of the wetlands that once covered this entire region, a lush pond dotted with aquatic plants and a rotating cast of migratory wildlife otherwise rare to this part of the valley—geese, ducks, black-crowned herons, and great blue herons.

We drive past the sandy berms along the new canals, miles of which have been planted with new elderberry, sage, milkweed, and other native plants designed to draw pollinators and strengthen the levees with their roots. This is the most excited I've seen Cameron. "We've got hummingbirds in here all year round. It's loaded with bees," he says. "It changed the whole field from strictly farm to something nicer."

Like most climate adaptation, the McMullin project is a smart, innovative, desperate thing to do. It alone won't reverse more than a century of environmental transformation. It alone won't prevent catastrophic damage from the kind of mega-flood that could fill the valley bowl like in 1862, submerging the land where millions more people live and work today.

The Department of Water Resources says there may be half a million acre-feet of extra flood and storm water available to recharge those aquifers each year, on average; the Public Policy Institute of California says it may be closer to a million. Yet even a thousand McMullin projects gulping the peaks off all the rivers would clear only about half the valley's annual deficit. There is a fundamental mismatch between where the water falls (north) and where it could be stored (south). White papers on the potential for recharge posit that the floodwater at the top of those winter peaks should be transported across the state, a proposition that could launch a thousand (or more) state water board complaints.

The good news for California is that climate change is making it more like California, which has the tools to plan for floods and droughts, and the natural underground storage to hold the water it requires to survive. The bad news for California is that climate change is making it more like California, where the water problems have always been man-made. More resources are still dedicated to building gray infrastructure than green. Meanwhile, water attorneys quietly tell me that they think every basin in the state could be adjudicated in the coming decades—a long and painful process that would account for every drop above and below and create yet more opportunities for building water wealth. No fleeting stream would flow unclaimed. Where pumping and recharge are metered and tracked, groundwater won't just be owned; it will be traded on new markets. McMullin is planning one.

Hurley says he has told farmers in McMullin that he'll do everything he can to see that they don't have to retire any acreage—though he hopes some will. "There's some land out there that's better used as a parking lot than what they're attempting to grow on it," he says. It's a decision that more and more growers are already being forced to make. Taken together, the impact of all those empty fields will ripple across the region and the nation, shrinking the local economy and raising food prices for everyone.

The Kings River conflict could trickle two or 20 years into the future—no one really knows yet. Nearly 10 months after the first hearings, there has been no ruling. In the meantime, Bachand is running more field-flooding experiments with farmers across California, who don't fear the flood like they did just a few years ago. Scientists have developed a tool to help them determine when and where to recharge the most water without contributing to a decline in quality. Taken far beyond the fields of Terranova, on-farm recharge could help perform a function rivers supplied before we bent them to our will, in a way that also works for 21st-century California. Along with it, piecemeal floodplain and wetland restoration could create habitat and recreational greenspace in one of the country's most polluted regions.

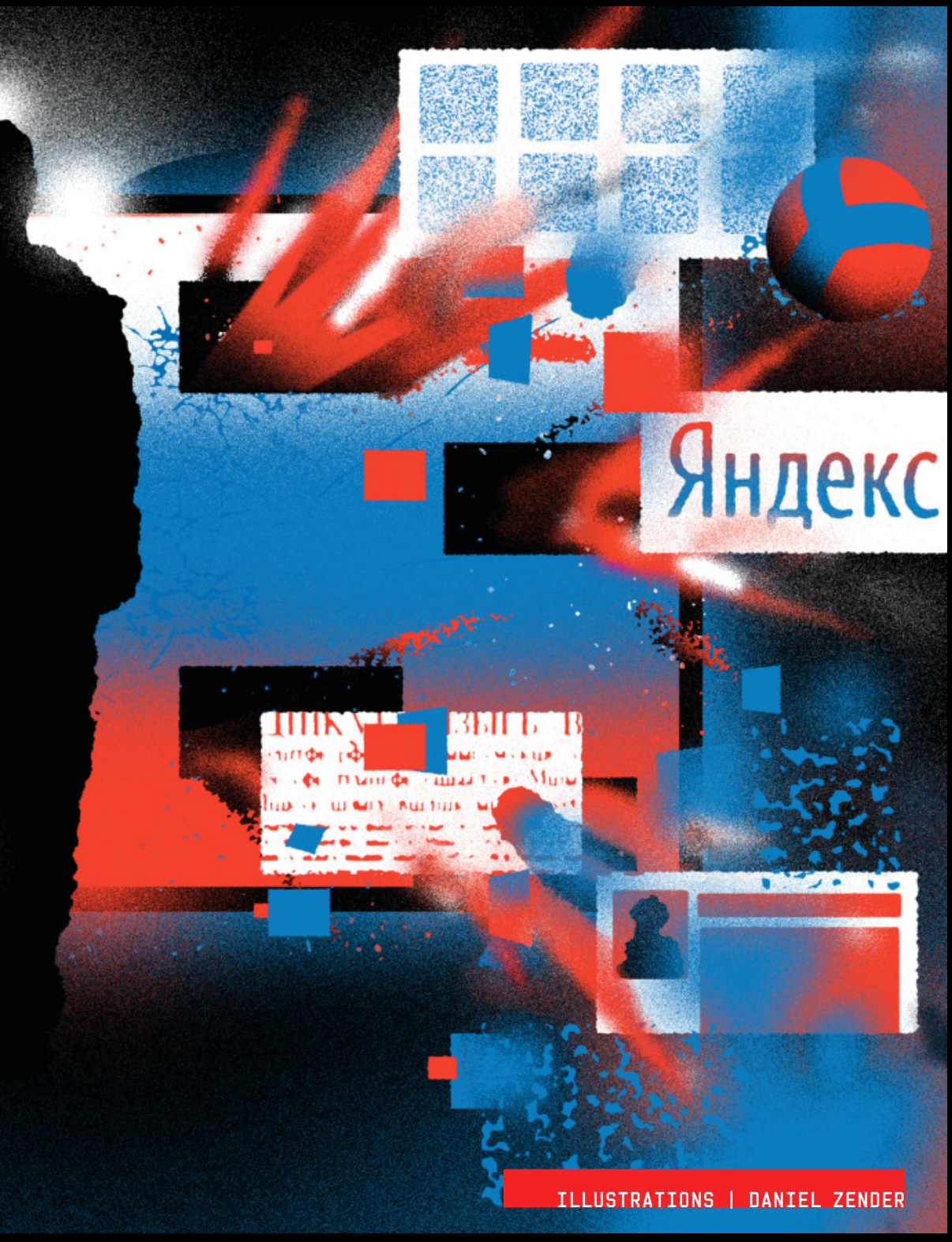
Even if none of it were to go his way—if the Kings River management won't renew Terranova's floodwater agreement, if the state water board doesn't approve McMullin's permit or grants Semitropic every drop, if the big round pumps and motors stay silent and the pipes and canals stay dry and empty—Don Cameron's innovation would still have flooded across California.

SUSIE CAGLE *(@susie_c) is a journalist in California.*

WHEN WAR CAME FOR RUSSIA'S BIGGEST TECH COMPANY

BY PAUL STAROBIN

It took 20 years for Arkady Volozh to build Yandex into the country's Google,



Uber, Spotify, and Amazon combined. It took 20 days for everything to crumble.

ARKADY YURIEVICH VOLOZH SEEMED TO BE IN GOOD SPIRITS.

It was February 11, his birthday, and the 58-year-old billionaire CEO and cofounder of Yandex, the Russian tech behemoth, was in the sort of open, engaging mood that could be called *privetliviy,* after the casual Russian word *privet* for hello. He was speaking from his car in Tel Aviv, bragging about his father—an oil geologist in his eighties who had "discovered" oil in Israel, Volozh said—as we chatted about my upcoming trip to Tel Aviv to interview him for this story.

For more than 20 years, Yandex has been known as "Russia's Google": It began as a search engine in 1997 and still has a 60 percent share of the Russian search market. But for the past decade, this tag has understated the company's inescapable ubiquity in Russians' daily life. Yandex Music is the country's leader in paid music streaming, and Yandex Taxi is the top ride-hailing app. Millions of Russians use Yandex Navigator, Yandex Market, Yandex News, and Yoo Money (formerly Yandex Wallet) to get around, shop online, read, and spend money.

Volozh had only recently begun to make his company less reliant on its Russian business—and on the whims of President Vladimir Putin—by tiptoeing westward. Yandex Taxi formed a joint venture with Uber in 2017, and in 2020 Yandex began testing self-driving cars in Ann Arbor, Michigan. Last year, the Yandex Rover robot, something of a six-wheeled Igloo cooler, began delivering food via a partnership with Grubhub to college campuses in Arizona and Ohio, with plans to expand to 250 American schools. Yandex had also launched delivery services in London and Paris. On the day of our call, Yandex had a $16 billion market capitalization on Nasdaq, and about 85 percent of its shares were traded in the United States.

Most of Yandex's 18,000 employees are still based at the company's headquarters in Moscow. But Arkady, as everyone at Yandex calls him—Western-style, shorn of the formal Russian patronymic—now more or less lives with his family in Israel. For several years, Israel has been an R&D hub for new products, especially in the transport sector, that Yandex aimed to bring to markets in Europe, the US, and the Middle East.

On our call, Volozh asked if there was anything in particular I wanted to see during my visit—the old city of Jerusalem perhaps? I've seen that, I told him. My goal was to spend as much time as possible with the reigning baron of Russia's tech sector, and to try out Yandex's new products firsthand. The company had recently acquired an electric-scooter business in Israel. How about a scooter ride? I asked. Of course, he said.

Volozh had seemed to master the high-wire act that all Russian moguls with global ambitions attempt: to accommodate Kremlin pressure while enticing Kremlin-leery investors and partners in the West. Self-effacing, cerebral, respectful, a soft voice in the boardroom with a salt-and-cinnamon goatee, he "does not come across as a driven entrepreneur," John Boynton, the American chair of Yandex's board, told me. In short, he's the opposite of the stereotypically boastful, political knife-fighting Russian oligarch. "He is more a techie than a business magnate," says Esther Dyson, an American angel investor and until recently a Yandex board member. In a country that still depends heavily on oil and gas exports, Volozh has been an unyielding visionary for the tech industry, imagining future possibilities—from natural language search to autonomous vehicles—and believing in his beloved Russian "geek community" to build those technologies.

His bent was to keep Yandex out of immediate political matters. But that abruptly

became impossible. On the morning of February 24, two days before my flight to Israel, I received a text from a Yandex PR official. "We are deeply sorry," the person began, but "events, which are beyond our control, create a great deal of uncertainty." My meeting with Volozh had been postponed, until the "situation allows."

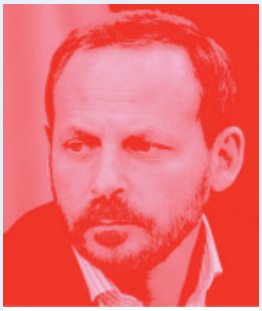
The situation was that, hours earlier, Putin had launched Russia's invasion of Ukraine. "Uncertainty" barely described the existential predicament that Volozh, Yandex, and everyone in Russian tech abruptly faced. I received the text shortly before US stock markets opened; by noon the price of Yandex shares had more than halved. In the following days, Uber announced that its three executives on the board of Yandex Taxi were resigning immediately, and the transport minister of Lithuania asked Google and Apple to remove the taxi app from their platforms.

As the doors to the West were slamming shut, Yandex was imploding at home. On March 1, Lev Gershenzon, the former head of Yandex's news division, posted an anguished note on Facebook addressed to his former coworkers. "Yandex today is a key element in hiding information about war," he wrote from his home in Berlin. At least "30 million Russian users" of Yandex's home news page "see that there is no war, there are no thousands of dead Russian soldiers, there are no dozens of civilians killed under Russian bombings." Gershenzon's post included a screenshot of Yandex's homepage that day; there was indeed no sign of carnage. Instead, the lead story highlighted Russian defense minister Sergei Shoigu's assertion that the main goal of the military's *spetzoperatziya* ("special operation") in Ukraine was to protect Russia from military threats posed by the West. "It's not too late to stop being accomplices to a terrible crime," Gershenzon wrote. "If you can't do anything—quit."

Gershenzon told me the day after his post that Volozh "is responsible for this news page." He continued, "It's the seventh day of the war, and we haven't seen any statement from him." The "great entrepreneur, excellent family guy doesn't understand his responsibility, and the awful thing is that Yandex is participating with—is cooperating with—the Russian army ... It makes me sick."

As the invasion stretched on, the Russian economy began collapsing under the weight of Western sanctions. On March 3, Yandex warned that it risked defaulting on $1.25 billion of debt. In 2020, the tech sector's weight on the Moscow stock exchange had doubled to 8 percent, close to the European average, and Yandex had been its leading light. Now hundreds of thousands of Russians were fleeing the country, many tech workers among them. Russia's broader ambitions of being a permanent part of the economies of Europe and North America were also severely damaged. "I believe Yandex's Russian business is dead, more or less," Gershenzon told me, since that business is "all based on the ability of the Russian people to spend money."

It had taken Volozh 20-plus years to demonstrate to the world that world-class technology, as good as anything created in the West, could come out of Russia. Indeed, he stood out as a refutation of the common Western trope, given voice last year by US president Joe Biden, that Russia "has nuclear weapons and oil wells and nothing else. Nothing else." I had cited that quote on my call with Volozh, stressing the importance of hearing his story directly from him. But now, as Russia laid siege to its neighbor, his life's work and aspirations seemed to be crumbling with each passing hour.



Arkady Volozh, CEO and cofounder of Yandex.

Getty Images

II

BORN IN 1964, Volozh was raised primarily in Almaty, the capital of Soviet Kazakhstan. Both his father, the oil geologist, and his mother, a music teacher, were Jewish. In the 1970s, many Soviet Jewish families, faced with persecution, secured exit visas to begin new lives in the West; this was how the family of 6-year-old Sergey Brin, the future cofounder of Google, made it to suburban Maryland.

But Volozh stayed in the Soviet system, attending a special school for gifted students in mathematics. It was there that he formed a close friendship with an equally precocious youngster, Ilya Segalovich. Both headed to Moscow for college in the 1980s—Volozh at an institute of oil and gas and Segalovich at a similar institute for geological prospecting. Volozh graduated with a degree in applied mathematics and, together with Segalovich, began launching a series of small information technology companies.

In the 1990s, a newly privatized post-Soviet economy began to take shape, largely ruled by a group of predatory oli-

garchs. Many had Boris Yeltsin's Kremlin in their grip, amassing their fortunes through rigged privatization auctions. Volozh and Segalovich, however, were more akin to the founders of a scrappy Silicon Valley startup: tinkering with thought experiments about the possible but unproven commercial potential of the internet.

Starting around 1993, the duo set out to build a digital search program for scientific patents, the Bible, and Russian classical literature. The name, according to the company's official history, came from Volozh and Segalovich "brainstorming around the words 'search' and 'index.'" They arrived at Yandex, an abbreviation of "yet another indexer," and soon expanded the software to be able to search the entirety of the Russian internet, then 5,000 sites and 4 gigabytes of text. Their search engine went live in September 1997, "almost a year before Google," Volozh would proudly point out years later.

As chaotic as Russia's economy was in the 1990s, there were still plenty of Western investors. In 2000 the private equity firm Baring Vostok, founded by the American businessman Michael Calvey, made a seed capital investment of $5 million in the young company—enough to secure a 35 percent stake. At the time, Yandex had only $72,000 in annual revenue and was losing $2 million a year.

By 2003, the global tech world was well aware of Yandex's prowess in search, particularly in natural language processing and in calculating the distance between searched keywords. That year, Google founders Brin and Larry Page visited Volozh and Segalovich in Moscow and proposed to buy Yandex for $100 million. It was a tempting offer, but the pair decided they would rather keep control of their company than effectively become Google employees. When Google later tried to enter the Russian market, Yandex still performed better at capturing the idiosyncrasies of the Russian language, such as the fact that the same word can have many different endings.

By 2009, Yandex had a 56 percent share of the Russian-language search market, more than double Google's. The Russian economy had stabilized, and ad revenues poured into the company's coffers. Yandex quickly expanded into email, maps, online shopping, and the spam blocker Spamooborona. There was a good deal of truth in Volozh's boast that no other company in the world had competed with Google "and survived and beat it."

Yandex also grew, in part, by managing to not alienate Vladimir Putin, who became president at the end of 1999. Under Putin's rules, business figures and companies were expected to be loyal to the Kremlin. If not, the moguls could be arrested, and their companies' assets could be confiscated. In one striking example, the oil baron Mikhail Khordorkovsky, then the richest person in Russia, was arrested in 2003 and jailed, and his company, Yukos, was taken over by the state. The reasons remain murky, but they were thought to include his support for opposition politicians and pro-democracy causes.

Volozh and Segalovich, by contrast, largely kept a low profile. Occasionally, they even helped Putin cultivate his everyman image with the Russian public. In 2006, Yandex hosted a live chat with the president, unscripted and televised to the nation. A participant asked Putin, "When did you have sex for the first time?" The president replied, "I don't remember, but I certainly remember the last."

Still, there was room at the margins for dissent, and though Volozh and Segalovich were both politically liberal, they responded differently to the Kremlin's relentless efforts to establish control over Russia's politics. In 2011, Segalovich, but not Volozh, took part in public protests against the results of parliamentary elections that delivered a majority of seats in the Russian Duma to Putin's United Russia party. (The European Court of Human Rights later ruled that Putin's party had rigged the election.) Some Yandex employees joined Segalovich in the demonstrations. "Ilya was seen as the beating engine of the company, the heart," says Gershenzon, who joined Yandex in 2005. Segalovich, he says, was "charismatic by example" and set the "moral standard" for Yandex. Volozh, by contrast, made "too many compromises" with the Kremlin, Gershenzon says. "When good people have a lot of business with awful people, they start to try to understand them. It's like a disease."

Others see the distinction between the two founders less starkly. "Ilya was not radical," but he "supported the opposition" to Putin, says Alexey Sokirko, a software engineer who worked at Yandex from 2005 to 2018 and attended political rallies with

[redacted]

Putin's visit to the Moscow office certainly looked like the bestowal of his blessing on Yandex and its leader.

Yet the president remained wary of his country's largest tech company.

Segalovich. He added, "Arkady within the company contrasted him a little, urging everyone not to politicize Yandex."

Their differences were also in part a function of their roles at the company; Segalovich served as chief technology officer, Volozh as CEO. As with any Russian CEO of the Putin era, it was Volozh's job to oversee business strategy and to develop personal relationships with officials in and around the Kremlin. (Alexander Voloshin, a former chief of staff to Putin who resigned from the government around the time of the Yukos saga, serves on Yandex's board.) Such relationships proved beneficial when Yandex needed help warding off an anticipated takeover attempt in 2008 by a metals oligarch, Alisher Usmanov, who was looking to expand into tech.

In 2011, Yandex raised $1.3 billion in a public offering on Nasdaq—then the biggest IPO since Google's. Peter Loukianoff, a Russian-American whose venture capital firm Almaz Capital had been an early investor in Yandex, told *The New York Times* that the moment signaled a new era "of intellectual wealth creation in Russia"—an era that Volozh and Segalovich had given birth to. "Russia now has a Steve Jobs and Steve Wozniak," Loukianoff gushed. But even at the time, his comment was a reach. In its public offering prospectus, Yandex explicitly warned that "high-profile businesses in Russia, such as ours, can be particularly vulnerable to politically motivated actions."

III

ILYA SEGALOVICH WAS diagnosed with stomach cancer in 2012 and died the following year, at age 48, leaving behind his wife and five children. "Ilyusha and I have been friends since school; we sat at the same desk for four years," Volozh wrote on a Yandex page that collected memories of Segalovich. "I don't know what can replace his encyclopedic [knowledge of] technology and clear vision of the product."

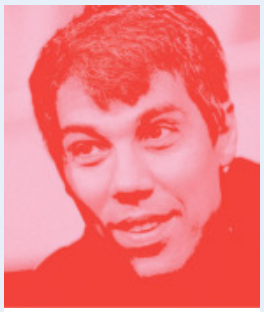
Segalovich's death marked the start of a new chapter for Volozh, bereft of his childhood friend and closest business partner, and for Yandex, bereft of the man whose "ethical standards," as Volozh wrote, "set the standard for all of us." In a 2017 *Moscow Times* op-ed, Russian journalist Elizaveta Osetinskaya wrote of this new phase: "Yandex's company culture has changed as Russia's political momentum has gravitated towards conservatism and isolationism." Putin's implacable opponent, the anti-corruption activist Alexei Navalny, had complained that Yandex News was hiding reports about his activities from its news feed. Yandex, Osetinskaya wrote, insisted that "its results are automatically generated by algorithms." (The Navalny movement has long posed a challenge for Yandex. In 2011 the Federal Security Service had required the company to disclose details about financial contributors to Navalny through Yandex's money service.)

The environment Yandex operated in was also becoming increasingly nationalistic. In 2014, after months of protests in Ukraine forced a pro-Russian president out of office, Putin engineered the annexation of Ukraine's Crimean Peninsula and stoked a violent separatist movement in the country's Donbas region. In this darkening climate, dissent from the Kremlin line was more unwelcome than ever.

At a media conference a few weeks after Crimea's annexation, Putin famously told reporters that the internet was a "CIA project." He singled out Yandex for being "developed with Western influence" and suggested that its registration in the Netherlands was "not only for tax reasons but for other considerations too."

Not long after, Sergey Petrenko, the head of Yandex's operation in Ukraine, the company's second-biggest market, went on "indefinite leave" after posting on Facebook his support for what he called a "purge" of pro-Russian separatists from his home city of Odesa. Petrenko later posted on Facebook that during Russia's takeover of Crimea he had "called Arkady and said literally 'This is a war between our countries, we need to do something, we need to go out and say that it can't be done, we have an audience of millions who need to know this.'" But "nothing happened afterwards."

To mark the company's 20th anniversary in 2017, Putin visited Yandex's Moscow offices, as Volozh's guest. "I don't have friction with the state," Volozh told WIRED UK several months before the visit. "Just like I don't have friction with the weather." Ahead of Putin's arrival, employees were reportedly told not to take bathroom breaks, and the Kremlin recommended they dress casually, to appear "as close to real life as possible," sources told the Russian outlet *The Bell*. Sokirko, the software engineer, who had publicly vowed to spit on Putin if given the chance, was asked by his supervisors not to come to the office that day. "It's not all that important," he wrote on Facebook at the time. "I have a pretty good job."



Ilya Segalovich, Yandex's cofounder, who died in 2013.

Indeed, despite the Kremlin's growing presence, as Osetinskaya noted in her *Moscow Times* article, the ambiance at Yandex remained largely congenial: "As is the norm at other leading tech companies, Yandex staff enjoy a free atmosphere of creativity, informal dress code, open-space offices, and hip cafés where employees play video games."

Putin's visit, during which he chatted with Alisa, Yandex's voice assistant, and watched a demo of Yandex's self-driving technology, certainly looked like the bestowal of his blessing on Yandex and its leader. Yet the president remained wary of his country's largest tech company.

In 2019, after arduous negotiations with the Kremlin, Yandex put in place a new corporate governance structure. As the *Financial Times* reported, the Kremlin initially demanded veto power over Yandex's entire board and control over its Dutch holding company. It ended up settling for two seats on the board and a Kremlin-friendly foundation with a "golden share" in the company that, the *FT* wrote, gave it "the power to block transactions and temporarily remove Yandex's management if it deems it in the national interest."

"It was sort of a deal with the devil," says Esther Dyson, who joined the Yandex board in 2006. (She stressed, though, that Yandex had been transparent throughout the process, and that the company issued a public statement on the restructuring.) Though Volozh rarely so much as hinted at frustration with the state, he must have found these negotiations unpleasant. One can only speculate whether Segalovich, had he been alive, would have pushed back against the golden share deal. But Segalovich was gone, and Putin's grasp was only tightening.

IV

LEV GERSHENZON LEFT Yandex in 2012, one year after its IPO, using the proceeds from the sale of his stock options to start a tech company in Berlin. He departed in part because he thought that Yandex was overly preoccupied with its business in Russia, at the expense of opportunities abroad. The company, he says, "wasn't ready to aggressively penetrate foreign markets and invest in global expansion."

But though it might not have been fast enough for Gershenzon, change was happening. Volozh had been slowly making Yandex into what he called a "trans-local company," bringing products proven in Russia into markets where competitors were weak. Yandex set up its first international office in 2005, in Ukraine, and in the following years it expanded into Turkey, Kazakhstan, and Belarus. In 2009 it established its first toehold in America, opening Yandex Labs in Palo Alto, a 10-minute drive from the Googleplex. The idea, in part, was to hire 20 or so engineers who could share with Moscow the latest trends in Silicon Valley.

Like many of his California peers, Volozh more recently got interested in autonomous transportation. In 2018, Yandex launched what it called "the world's first robo-taxi service," in Russia's high-tech city of Innopolis. The 4,000 or so residents of the city could hail one of Yandex's driverless taxis free of charge. "Everything which is easy to automate should be automated," Volozh said in a speech in Armenia the following year.

In an early sign of its designs on the American market, Yandex demonstrated a self-driving vehicle in 2019 at CES, the annual consumer electronics trade show in Las Vegas. And in 2020, the company announced the selection of Ann Arbor as "the perfect testing ground for innovations in transportation," with the city's "wealth

Getty Images

of research and engineering facilities and many bright young minds."

Volozh framed his vision of Yandex's global expansion in terms of target metropolises, not nations. For services like taxis, scooters, food delivery, and ecommerce, "you analyze the market by cities," he told an Israeli interviewer last November. For Yandex the key cities were Paris, London, Tel Aviv, and Dubai.

In January, ahead of my expected meeting with Volozh in Tel Aviv, I had lunch in Concord, Massachusetts, with John Boynton, president of the investment firm Firehouse Capital and chair of the Yandex board. He told me he had become interested in the Soviet Union on a trip to Moscow and Leningrad in the early 1980s with his Concord High School classmates. He met Volozh in 1990 and was one of Yandex's first investors. Volozh "operates on a very high plane," says Boynton. And because "Arkady is typically several steps ahead" of everyone else at Yandex, part of Boynton's job has been to "help translate" Volozh's vision into action.

That vision, Boynton was eager to tell me, was rapidly materializing in America and beyond. Press coverage for the Rover robot had been a PR dream. In a local Tucson news segment called "Ordering the Future," a University of Arizona administrative official gushed about "students taking selfies" with the Rovers and "kind of petting them as they go on their way." Yandex's fourth generation of autonomous vehicles—Hyundai Sonatas equipped with the company's own software and sensors—were being tested on the streets of Ann Arbor. In the global race for preeminence in self-driving, Yandex was betting on its proprietary lidar sensors, the latest of which, developed to cope with Russia's often frigid, unforgiving driving conditions, could develop a real-time image of the road up to 550 yards ahead. Yango Deli, Yandex's 15-minute delivery app for produce and snacks, was up and running in Paris and London. In November 2021, Yandex had announced a partnership with the Middle Eastern operator for the French global grocery chain Carrefour to make deliveries to Carrefour customers in Dubai using autonomous robots.

This global game plan "was clearly driven by Arkady," Ilya Strebulaev, a professor at Stanford Business School and until recently a Yandex board member, told me.

Perhaps, though, the strategy was belated. Around the same time, Yandex leaders were realizing that the company's growth prospects in Russia were limited. For one thing, Yandex increasingly faced competition in Russia's information economy, not least from government-controlled Sberbank, which is run by German Gref, a Putin associate and a former Yandex board member. Sberbank's major focus is transport, including self-driving cars—exactly the business Yandex was trying so hard to develop. With its government ties, Boynton told me ruefully, Sberbank could draw on more or less unlimited resources; the company was luring talented Yandex workers with offers to triple their pay.

Yandex also faced the perpetual problem of Russia's best young tech minds leaving for jobs in the West. To try to keep them, Yandex had developed its own training and education programs in conjunction with Russian universities, and in Moscow the company paid salaries high enough to compete with Western firms like Google. If a Yandex worker did leave for a job abroad, Boynton told me, the company went to considerable effort to understand "exactly why." In Volozh's vision, a Yandex job in Moscow should be on par with a position in Silicon Valley.

In a note announcing his resignation, Ruslan Musaev wrote on Facebook, "I consider the company's actions a crime and complicity in war and murders and I don't want to be a part of it."

V

IN THE FIRST week of the Ukraine invasion, Gershenzon was not the only former or current Yandex employee to denounce the company for "hiding information" about the war. "I celebrate the deafening silence of Yandex. What a blessing that Ilya Segalovich doesn't hear this," wrote Sergey Petrenko, the former head of Yandex Ukraine, in a sarcastic Facebook post on February 28. Three days later, he posted again about his former employer: "All I'm going to say is that among the human vices, I believe cowardice is one

of the main ones." That line, he later told me from Odesa over Facebook Messenger, was a reference to the Mikhail Bulgakov novel *The Master and Margarita*, which he expected his former Yandex colleagues to be familiar with. "I understand that Arkady started this long path of compromise with the Russian state," Petrenko said. "But I feel sorry for Arkady, mainly because no one could have guessed how it would turn out."

In a note announcing his resignation, Ruslan Musaev, a project manager, wrote on Facebook, "I consider the company's actions a crime and complicity in war and murders and I don't want to be a part of it." Sokirko, the former Yandex engineer, told me that probably "90 percent of Yandex employees are against the war." He had been jailed for his participation in antiwar protests in Moscow and then released.

By March 5, ten days into the conflict, there had still been no public word from Volozh. I sent him an email. It was a Saturday in Israel. "Shabbat Shalom," I greeted him. "I cannot begin to imagine the circumstances you now face. I am reaching out now in hopes of engaging in a conversation."

The questions I planned to ask him were obvious enough. Why was he maintaining a public silence? How did he respond to Musaev's post branding the company complicit in "war and murders?" Had he communicated his views on the war to anyone in the Kremlin? What was Yandex's future in Russia and beyond?

I imagined him frantically working through the night with his team in Moscow to keep Yandex from collapsing. Just six days into the war, *Forbes* reported, the market capitalization of Yandex had plunged from its November 2021 peak of $30 billion to below $7 billion, while Volozh's net worth, recently as high as $2.6 billion, was down to $580 million. (On February 28, Nasdaq halted trading in Yandex shares.)

Meanwhile, Western partners were continuing to undo ties with the company. Grubhub terminated its partnership with Yandex. The future of the self-driving research operation in Ann Arbor was uncertain. DuckDuckGo, the privacy-focused search engine that had sourced its results in part from Yandex's index, paused its partnership with the company. In the UK, a spokesperson for the Liberal Democratic party compared Yandex to Huawei in China and said "any company that is in any way propping up the Putin regime is potentially on the sanctions list."

Volozh could have joined the brain exodus from the Soviet Union and tried to make his fortune in the West. Instead he made his fortune in Russia, and he now stands to lose a big portion of it there.

Then Dyson and Strebulaev resigned from the board, releasing a joint statement: "In the current political environment in Russia, it has become impossible for the team to continue to provide a free and open platform for information for the Russian public without breaking the law and putting the company and its employees at risk."

While Volozh remained publicly silent, Yandex's Moscow-based executive director, Tigran Khudaverdyan, who had been Volozh's number two since 2019, assumed the role of the company's voice. "What is happening is unbearable," he wrote on March 2 in a Facebook post. "War is a monstrous thing. Today, many people are demanding that the company immediately get up on top of an armored car and loudly state its position. I believe that any actions we take should be dictated not by emotional impulses, but by key priorities." The two most important ones, he said, were "employees' safety" and "keeping key services for Yandex users operational." Services like search, taxis, and food delivery, he argued, were "as essential" to Russians "as electricity and water supply." (On March 4, the Russian government blocked Russians' access to both Facebook and Twitter, and passed a law that criminalized the use of words like "war" and "invasion" to describe its attack on Ukraine.)

Still, the company strove for normalcy. When I talked to Boynton by phone on March 8, he told me that "everyone is coping" as best they can at Yandex. A Moscow source in a position to know told me the company was planning a "big party" for its workers in celebration of International Women's Day, always a major festivity in Russia.

And while the US and European governments were sanctioning other Russian business figures with Kremlin ties, Yandex executives were seemingly spared—that is, until March 15, when the EU slapped an asset freeze and travel ban on Khudaverdyan. The EU's official journal cited Gershenzon's post about Yandex "hiding information" and revealed that on the day Russia invaded Ukraine, the Yandex deputy CEO and other Russian business leaders had met with Putin at the Kremlin to discuss an action plan in the wake of Western sanctions. Khudaverdyan resigned immediately.

PAUL STAROBIN *is a former Moscow bureau chief for* Business Week *and is currently writing a book on Russia.*

VI

WITH THE RUSSIAN economy in shreds and Putin rapidly closing anything left of a free internet, the tech-worker brain drain was becoming a frantic mass exodus. Thousands of those who could afford to were fleeing a country that was "flying into an abyss," as one Russian tech executive told the *Financial Times,* escaping to Cyprus, Armenia, and beyond. Some 25,000 Russians had reportedly arrived in Georgia within the first two weeks of the invasion. For the many more left behind, including untold thousands of Yandex workers, there's the very real prospect that the Russian economy and tech sector will be isolated for years or decades, leaving them without a livelihood.

One conceivable way for Yandex to protect and retain at least some of its workers might be to bring them from Moscow to Israel. The country has a bustling tech industry, and it does not appear to want to restrict Yandex's business activities there. Israel might also be a base for Yandex's bid to deepen its presence in the United Arab Emirates, with which Israel has friendly relations and which has so far not imposed sanctions on Russia. The Israeli newspaper *Haaretz* reported that Yandex had approached the government about bringing over 800 workers, but an Israeli foreign ministry spokesperson told me, "it seems no such requests were submitted by the company."

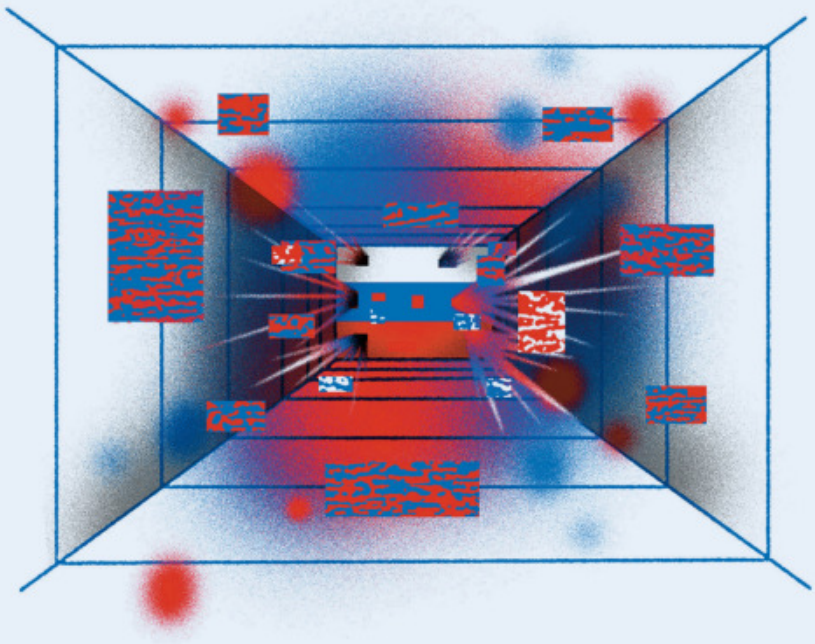
The company could still stabilize in an increasingly isolated Russia, even if its global ambitions are dashed. With Apple Pay now shut off to some Russian customers, Yandex Pay could gain market share, and the same might go for other services where Yandex no longer faces foreign competition. A Chinese buyer might make an offer for parts of the company or even all of it. Alternatively, a Kremlin-controlled firm like Sberbank could take it over, a fulfillment of the Kremlin's apparent designs on Yandex as, in effect, a national-security property. Yandex will perhaps sell Yandex News to a Kremlin-friendly Russian buyer: There are reportedly talks of a sale to the social network VKontakte. More ominous still, Russian officials might stage a trumped-up case of tax fraud or the like against the company, as they did against Khodorkovsky and Yukos years ago, and then insist on the forfeiture of Yandex's assets to the state.

On March 11, I heard from Yandex that Volozh wanted to talk. A spokesperson arranged for a Zoom call with him that day. Twelve minutes before the call was supposed to begin, the spokesperson texted me that she'd have to postpone the meeting. "Something urgent has come up," she said, without elaborating. There has been no word since.

I spoke with Strebulaev a few days after he resigned from the board, and asked whether he thought it was all over for the company. "I don't know," he replied. But Volozh, two years shy of 60, could move on with a new venture, he said. "If Arkady decides to do something else, maybe in Israel, I think he is going to be successful. People love him. People believe in him," and "people will follow." He reflected on his first meeting with Volozh, over a two-hour lunch in London in 2018, the conversation spilling over into Volozh's avid interest in Israeli archaeology. Volozh is "always teeming with ideas," Strebulaev said. "He kind of lives in the future."

Volozh reportedly has a Maltese passport and an Israeli one; it's now likely he will live the rest of his years outside of Russia. Still, his career and even his life might be framed as "the one who stayed behind." He could have joined the brain exodus from the Soviet Union and post-Soviet Russia and tried to make his fortune in the West. Instead he made one in Russia, and he now stands to lose a big portion of it there. The duality he tried for so long to maintain, as both Russian and Western, has collapsed—always the risk in the implicit bargain he made with Putin's Kremlin.

As to whether his apparent passivity in the face of the war in Ukraine amounts to a moral stain on his reputation, history and his own conscience will judge. It is tempting, though, to offer him the sort of line from Russian classical literature that the Yandex search engine was invented to find. *"Shtob umno postupat', odnovo uma—malo,"* Dostoevsky wrote in *Crime and Punishment*: "It takes more than just intelligence to act intelligently."



by Rowan Moore Gerety
Photographs by Alfonso Duran

A Mil Lit Pie

A lion tle ces

Nearly half of the world's reefs have been wiped out since 1950. One entrepreneur is on a mission to rebuild them—by speed-growing tiny slices of coral in hyperefficient farms.

Lisa Carne was swimming through a bed of seagrass in northern Belize

when she saw a hunk of elkhorn coral lying loose on the sandy bottom. She paused to look at it. With its rich amber color and antler-like branches, the fragment seemed alive despite having broken off from its mother colony. A professional diver, Carne was struck with an idea: What if she picked this up and moved it to a patch of dead reef? What if she did it over and over again? Could she help the reef recover more quickly?

Carne kept thinking about the fragment as she finished up her dive. The reefs close to her home, near Laughing Bird Caye National Park, in southern Belize, had recently been decimated by a hurricane. When she returned home, she sat down at her computer and started searching online for anything she could find on reef restoration.

A few years later, she began to fashion an underwater nursery near Laughing Bird Caye. Borrowing techniques from academic research, she used rebar and steel mesh to make a pair of underwater tables. She would swim around the reefs she had identified as resilient with a pair of pruning shears, cutting small chunks from healthy colonies. She brought each one to the shallows long enough to glue it to a concrete disk, then "planted" the fragments underwater on her metal tables. Slowly, they grew. Then she started transplanting her corals directly onto the reef.

Today, Carne's nonprofit, Fragments of Hope, works with local fishers to identify promising spots and track the fate of every piece of coral they place on the reef. And it ranks among the most successful and longest-running coral restoration programs in the world. When I spoke to Carne on Zoom last fall, she had set her virtual background to show the fate of her first plantings on the dull gray rubble of dead reef. Branching corals the color of mustard filled the frame. "You can't count that!" she said proudly, gesturing at the dense thicket behind her.

Yet for all of its success, Fragments of Hope's program is still incredibly small. It has taken Carne and her team more than a decade to plant 160,000 coral fragments on less than 9 acres of reef. Worldwide, reefs cover an area millions of times that size. As Greg Asner, a researcher at Arizona State University who directs a global coral mapping program, put it, "No coral restoration projects of any kind or anywhere have been done at a scale that would really save a reef. Coral restoration has not summed up to even 1/100,000th of the area of shallow coral reefs worldwide."

Coral reefs anchor some of the most vibrant ecosystems on the planet, home to a quarter of the oceans' biodiversity in a tiny fraction of their total area. Half a billion people worldwide depend directly on reefs to protect their coastlines, support local fish populations, and attract tourists. But in the past 70 years, pollution, overfishing, and climate change have killed off half of the world's reefs. By the end of this century, we may be speaking about healthy coral reefs in the past tense.

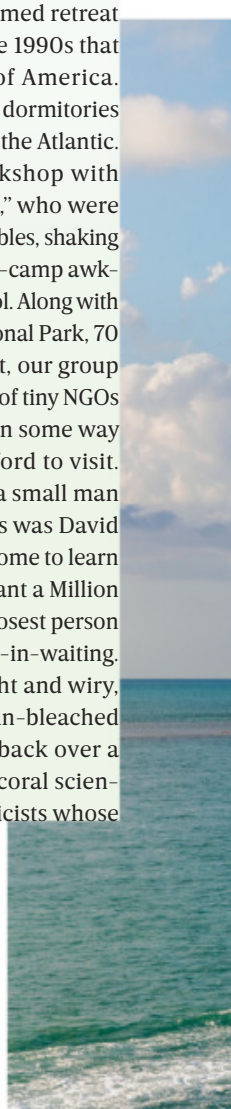
For years, Carne and others in the coral restoration field struggled to attract major funding for their efforts. That appears to be changing. In 2020, the insurance company Swiss Re crafted a policy to pay out nearly $1 million to send teams of divers to stabilize and replant corals that had been ripped out by a hurricane along the shoreline near Cancún, Mexico. Last year, the United States' Defense Advanced Research Projects Agency issued a request for multimillion-dollar proposals for reef-building projects to protect US military installations.

Scientists, too, are coming around to the idea of large-scale experiments that might improve reefs' resilience. For a long time, the sheer scale of reef systems made many people reluctant to contemplate regrowing corals. "It seemed like it was poking around the edges of the problem," says Joanie Kleypas, who studies reefs and climate change at the National Center for Atmospheric Research.

Emboldened, scientists have been cross-breeding wild specimens taken from hundreds of miles apart to try to create hardier, heat-resistant variants. They have been freezing key samples of genetic material so that the scientists of the future can try to bring back some of the genetic diversity lost due to climate change. Ruth Gates, the late coral biologist and director of the Hawai'i Institute of Marine Biology, told the *The New Yorker* in 2016 that she couldn't bear the idea that future generations may not experience coral reefs: "We're at this point where we need to throw caution to the wind and just try." To rebuild reefs at scale takes a different kind of effort—and, perhaps, a different kind of person.

It was a balmy December evening at the Florida Sea Base, a STEM-themed retreat built in the Florida Keys in the 1990s that belongs to the Boy Scouts of America. Pastel-colored boys' and girls' dormitories overlooked a canal leading to the Atlantic. I was there to attend a workshop with 19 fledgling "coral gardeners," who were seated at a row of long picnic tables, shaking off that first-night-of-summer-camp awkwardness with pizza and alcohol. Along with a team from Dry Tortugas National Park, 70 miles offshore from Key West, our group mostly consisted of emissaries of tiny NGOs from beautiful places reliant in some way on the people who could afford to visit. They were listening, rapt, to a small man with a Santa Claus beard. This was David Vaughan, the man we had all come to learn from. As the founder of the Plant a Million Corals Foundation, he is the closest person the field has to an industrialist-in-waiting.

Vaughan, who is 68, is slight and wiry, with intense blue eyes and sun-bleached shoulder-length hair swept back over a large bald spot. While many coral scientists are ecologists and geneticists whose



field work is a balance of lab and reef study, Vaughan likes to say he spent his career as an aquaculture scientist "diving in 5 feet of muddy water," honing techniques to grow shellfish bigger, faster, and cheaper. Between sips from a mug of red wine, he blitzed through his 40-year career as a businessman learning how to cultivate oysters, shrimp, and fish and turn a profit. His goal today is still, simply, scale; only this time he wants to bring the principles of industrial production to coral restoration.

In 2003, Vaughan became the director of the Keys outpost of the Mote Marine Lab, an independent research and education nonprofit headquartered in Sarasota. At first, the lab grew racks of coral the way aquarium hobbyists often did: Start with a piece the size of a golf ball, cut it in two and mount the halves on small ceramic discs, and wait months or even years for the pieces to grow back.

One day, Vaughan was cleaning an aquarium tank when he noticed a stray piece of coral the size of a silver dollar toward the back. He yanked it and heard a crack. A fragment came free in his hand, and a dozen polyps were left behind where the coral had fused to the glass. "Cracked into pieces, waving their tentacles at me," Vaughan said. He figured the polyps were goners. He placed the fragment he'd broken off in another tank, where he thought it was large enough to perhaps survive and regrow. A few weeks later, he checked on it. Instead of seeing the ragged edge of bare, white coral skeleton, he found that new coral had completely grown over the damage—far faster than he'd imagined possible. He ran through the lab to see the old tank; each of those single polyps had multiplied, and the colony had grown to the size of a dime in weeks instead of years. "Like any good scientist," he says, "I grabbed a scalpel, and I did it again."

Vaughan called this technique "micro-fragmenting," and he quickly sought

○ Great star coral polyps [previous spread] cut using micro-fragmentation.

● Summerland Key, Florida, is home to the nonprofit Plant a Million Corals.

● David Vaughan [right] often uses unconventional materials to fabricate his coral nursery. He uses salad bowls [below] to make cement mounts for coral plugs.

to reproduce the results with as many species of coral as possible. It turned out that researchers at other labs had noticed a similar pattern—cutting coral into smaller pieces could boost its growth rate. Still, it took years for the significance of these early experiments to sink in. When Vaughan and colleagues at the Hawai'i Institute of Marine Biology published a joint paper in 2015, they found that micro-fragmenting could make some corals grow as much as 40 times faster than they otherwise would.

One morning, Vaughan led the group outside, past the boys' and girls' showers to the edge of the mangroves lining the canal. Gravel crunched underfoot as we approached three rows of rectangular, blue plastic tanks resembling elevated kiddie pools. Vaughan explained that this was the "coral nursery" he'd built for the Sea Base. Peering down through a few inches of gently burbling saltwater, I saw what looked like trays of miniature hors d'oeuvres on porcelain plates—thousands of pieces of brown and purple coral, each the size of a large nailhead, their tiny barbed tentacles reaching toward the surface.

As we squinted to make out individual polyps, Vaughan marveled out loud about the quirks of coral biology. "A coral is a plant, an animal, and a microbe all mixed into one," he explained, oversimplifying a bit—the algae in corals are not technically plants. Coral colonies are made up of genetically identical polyps, with tentacles to grab nutrients suspended in the water and digestive systems that secrete a skeleton beneath them as they grow. Corals provide a safe, well-lit habitat for symbiotic algae called zooxanthellae that use photosynthesis to produce essential nutrients and sugars for their hosts, and thousands of types of microbes. Moving water, Vaughan said, keeps the whole ballet going, providing the energy to push nutrients and gases across the mucous membranes of every coral cell.

Vaughan has been refining his micro-fragmenting process for 15 years, chasing both speed and savings, but he ran into issues with the basic supplies for the trade. For starters, the tanks were all wrong. "A farmer wants to see his crops all the time," he complained; his tanks were made of opaque blue plastic. Since corals are factories for photosynthesis, the tanks should be clear, shaped in a way that allows you to mimic the ebb and flow of the surf.

While Sea Base staffers explained how to monitor and clean the tanks, Vaughan hovered around the edges, talking a novice through the proper technique to siphon debris out with a hose. ("Outside, now go low? Yeah, that's it.") He slid around a picnic table to peer through a microscope at the mucus on a newly cut micro-fragment. ("Let me see how that coral's doing.") He wore black Crocs sandals, synthetic khakis with zip-off lower legs, and a nylon safari shirt, unbuttoned halfway down his chest and embroidered with the logo of Plant a Million Corals.

Nothing got Vaughan so excited as recounting the hacks he'd developed to make things cheaper. At first he'd used ceramic plugs that aquarium suppliers sold for 25 cents apiece, until he took stock of the implications: "To plant a million corals, I'd have to raise a quarter of a million dollars!" he said with alarm. He decided to make his own plugs, but he needed the right mold.

One day, Vaughan was stewing on that challenge, bored while some students and interns were cutting corals, when he looked down at the perforated black rubber floor mat underfoot, like the ones you see in restaurant kitchens. "I go, 'There it is!' So I picked up the mat, and we poured the little holes, popped 'em out, then the next day we poured the big holes, put the stems we had back in, and we were making coral plugs at one quarter of a cent each"—a hundredth of the cost. Now he's trying to shrink the size of the ceramic plugs so he can fit more of them into each tank and cut down on the operation's biggest costs—the tanks themselves and the labor to keep them running.

With 12 trays per tank, that meant close to 4,000 corals in each one. The numbers matter, because Vaughan wants to make these nurseries fully modular—an affordable, off-the-shelf kit for coral farming. By packing all the necessary tanks, plumbing, and solar power to run the equipment into a shipping container, he hopes to make it possible to start cutting and growing corals anywhere with a water supply in a matter of days. Early prototypes of his Coral Restoration Units cost upwards of $200,000; he wants to cut the costs in half.


PLANT
a MILLION Corals

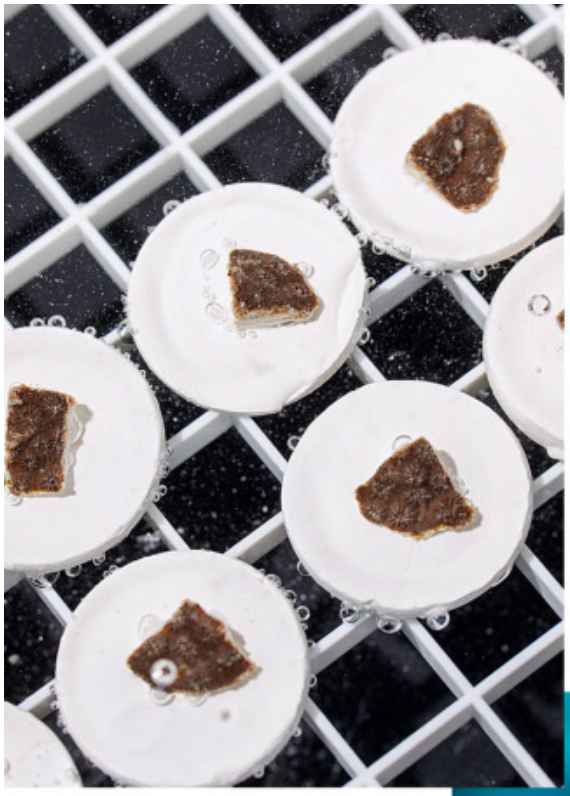
One afternoon, Vaughan played crossing guard as he jogged us across US Route 1 into an open field that had once been the site of a large shrimp hatchery where he hoped to build a roadside demonstration farm. The Keys' landmass is made of ancient, fossilized reef, and some of its polyps and striations were visible through the grass. Near a stand of Australian pines were three half-packed shipping containers holding the guts of three future Restoration Units.

One of Vaughan's first customers, Marissa Myer, had come to the workshop to see how her planned nursery, destined for Puerto Rico, was coming together. Vaughan enlisted volunteers to set up the tanks so he could visualize the plumbing he'd need. On her phone, Myer showed the group a digital rendering of the nursery she'd used to try to persuade the homeowner's association of an upscale housing development to lease coastal land to her. In the image, string lights twinkled over an array of tanks perched on white sand and flanked by potted plants.

Most of the rest of the group was still figuring out how to pay for a Restoration Unit, or determining if it made sense to try a land-based nursery at all. There were the two Canadian marine biologists who'd landed in Antigua and started a field nursery with money they'd raised from patrons at an exclusive country club. An artist was building an electrified underwater coral sculpture as a memorial for her patron's late daughter.

The person whose project came closest to marrying Vaughan's methods with the money to pull it off was marine biologist Andrea Caicedo Gonzalez, who was preparing for "A Million Corals for Colombia," an initiative of Colombia's president, Iván Duque, and its Ministry of Environment and Sustainable Development. The nonprofit where she works, Corales de Paz, had 16 months to go from an underwater nursery that produced 25,000 corals a year to building a network of trainees doing micro-fragmentation across a dozen sites. Caicedo Gonzalez couldn't help but notice that the project didn't budget yet for "outplanting" the corals they grew in nurseries back onto reefs. She was debating the ethics of taking money from oil and cement companies, but she hoped to line up another grant from Chevron to finish the work.

The landscape of coral restoration funding has a take-what-you-can-get quality. Vaughan has discussed a dive and documentary with Leonardo DiCaprio and Richard Branson. And he's consulted for Mohammed bin Salman, the crown prince of Saudi Arabia, who is now at work on a project set to add 2 million coral pieces to nearly 300 acres of reef. If only the process were cheaper, the money might be easier to find—and easier to say yes to.



●● Freshly cut mountainous star coral fragments are placed on each plug.

●●● The plug will be placed in the nursery to begin growing.

● In micro-fragmentation, corals are cut using a diamond band saw.

●●●● Vaughan fits a coral stem into a cement mount.

David Vaughan grew up in suburban New Jersey and spent as much of each summer as he could with his head in the Atlantic Ocean, near his family's house in Cape May. Vaughan's father worked in fundraising for Fairleigh Dickinson University, and when Vaughan was 13, he tagged along with a group of scientists on a research trip to the US Virgin Islands. "We started going around Saint Croix, looking for new species and knocking pieces off with a prospector's hammer," Vaughan said. (Most major laws that protect marine species were not passed until the 1970s.) He came home mesmerized by coral.

Vaughan earned his PhD in botany at Rutgers, studying algae and seagrass. He soon discovered that his work on microalgae was directly relevant to the nascent industry of farm-grown clams, which feed on the tiny organisms. Vaughan began drafting plans to build a hatchery. When his efforts to create a million-dollar facility ran into roadblocks, he decided to try rigging together a temporary clam farm inside three shipping containers. To his surprise, his DIY operation produced three times as many juvenile clams as the hatchery's business plan had called for. Vaughan scrapped his original vision and stuck with shipping containers. "It became one of the first ways I was able to say, 'We can do this cheaper,'" Vaughan told me.

He spent most of the first half of his career at Harbor Branch Oceanographic Institute, a marine research center with a small business incubator he started on Florida's Treasure Coast. He developed a reputation there for being pragmatic, entrepreneurial, and a bit quirky; during one field project, he and his wife and young daughter spent the season living out of an Airstream van and sleeping in a loft on the back.

At Harbor Branch, he oversaw construction of a new 30-acre aquaculture campus, with hatcheries for oysters, clams, and shrimp. As Florida's clam industry ballooned, Harbor Branch became its largest hatchery.

One day, someone left a freshwater hose running overnight in a saltwater shrimp tank. When Vaughan discovered the hose in the morning, he expected the shrimp

to be dead. Instead, they were doing fine. Shrimp have been known to tolerate low-salinity water during the rainy season, though it hampers their growth and makes them more susceptible to infections. "Dave looked at it differently," said John Scarpa, a shellfish biologist who worked at Harbor Branch. Vaughan didn't need the shrimp to lead long, full lives—he simply needed them to reproduce. Using freshwater or low-salinity water meant he could start growing shrimp not just on expensive coastal land but in the middle of Florida.

In the late 1990s, Vaughan learned that Aqua Life, an ornamental-fish-breeding operation on a small island in the Bahamas, was shutting down. Harbor Branch made a bid to buy what was left, and a month later, 22,000 orange and white clown fish in different stages of development arrived in Florida by plane, while 380 tanks made their way over on a chartered barge. Vaughan decided to sell the aquarium fish directly to pet stores. When *Finding Nemo* caused a spike in demand for clown fish in 2003, Vaughan's company ended up selling 25,000 of them a month. It also got into the coral business.

One day, Vaughan gave a tour of his aquaculture operation to the conservationist and filmmaker Philippe Cousteau Jr., grandson of Jacques, the famous French ocean explorer. When Cousteau got to the coral tanks, he was struck to see rows and rows of hand-sized fragments destined for pet stores, when most of the corals in the nearby Florida Keys were dead. As Vaughan recalled, Cousteau said, "Dude, you don't get it. You need to be doing this for the reef."

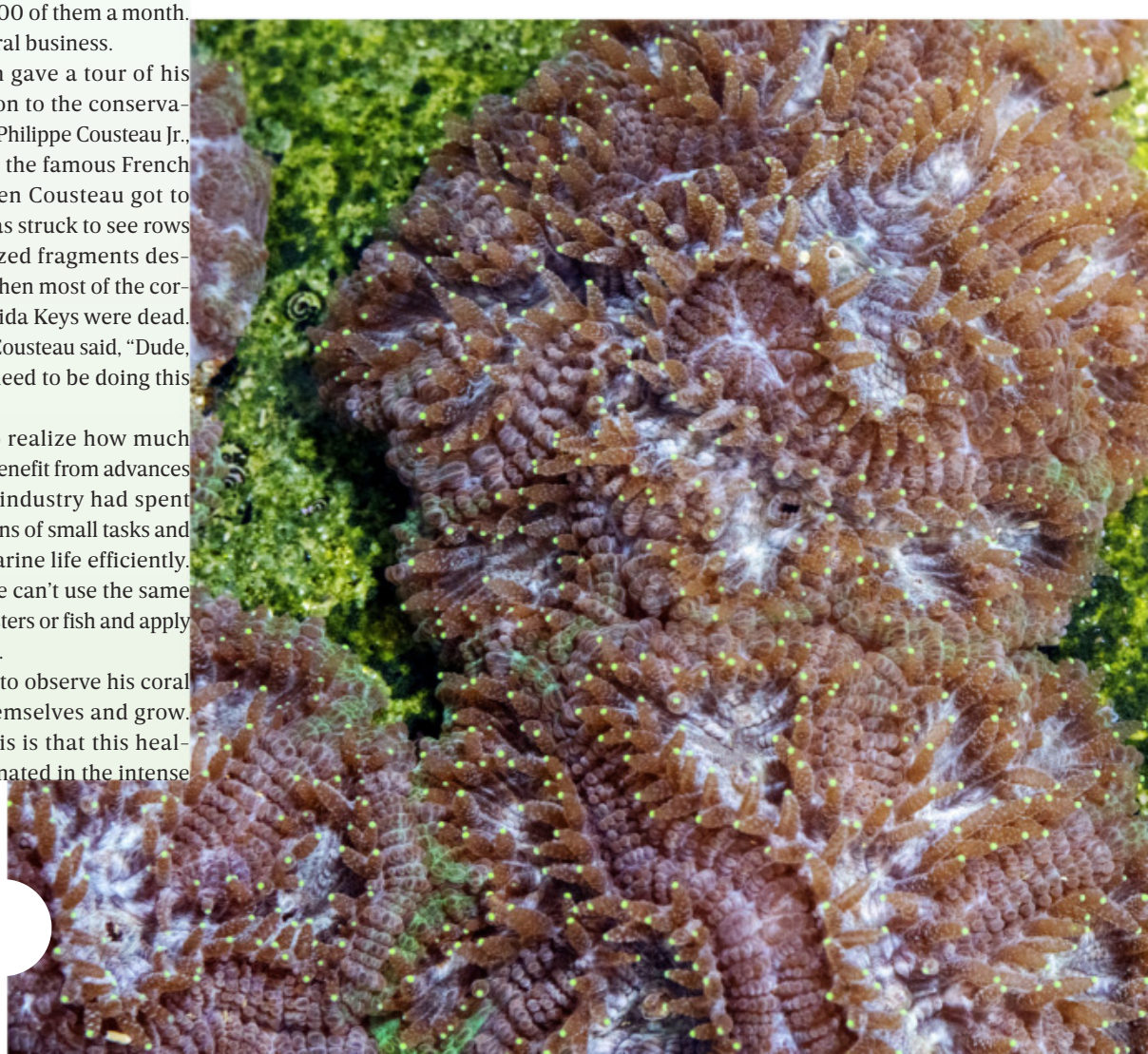
Vaughan began to realize how much coral research could benefit from advances in aquaculture. The industry had spent decades refining dozens of small tasks and processes to raise marine life efficiently. "There's no reason we can't use the same model for clams or oysters or fish and apply it to coral," he told me.

He's been amazed to observe his coral fragments repair themselves and grow. Vaughan's hypothesis is that this healing mechanism originated in the intense competition between life forms on a reef. Parrotfish, which can graze on algae that grow on the surface of polyps, sometimes bite off a chunk of the coral itself; perhaps corals evolved a way to repair the damage as quickly as possible, so that sponges and algae couldn't gain a foothold in the center of a colony.

But for all of Vaughan's success in growing coral quickly, cheaply, and effectively in plastic tanks, coral fragments still need to survive once you put them back in the sea.

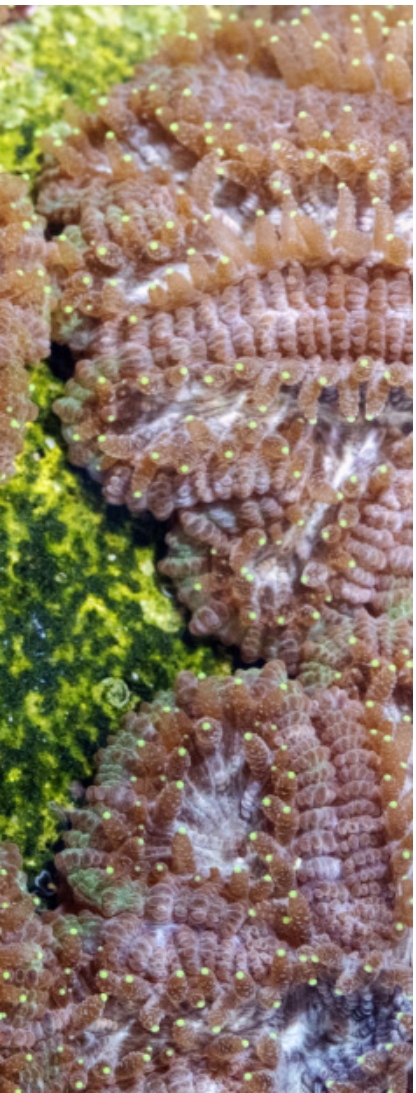
Vaughan discovered that if he planted many micro-fragments of the same genotype next to one another, they'd eventually fuse together. In 2013, he got permission to try this technique on bleached stony corals off the coast of Big Pine Key and led a team that planted 1,300 micro-fragments in clusters. More than 80 percent survived an outbreak of stony coral tissue loss disease, a mysterious pathogen that has affected populations of more than 30 species across the Caribbean. Over the years the clusters completely fused together, and in August of 2020 they spawned, unleashing a wave of tiny pink coral gametes under a full moon. Vaughan marveled at the achievement. "They're the age of a kindergartner, but somehow they got together and circulated the message to start making genetic material."

But the odds of survival are not in coral's favor. Even where the threats of disease or bleaching aren't as urgent, the mechanisms underlying successful coral restoration can be hard to pinpoint. In Indonesia, where many coral restoration projects have been undertaken since the 1990s, the marine biologist Tries Razak says most amounted to "just putting concrete on the sea bottom." Razak is in the middle of a three-year survey visiting sites all over the country. In some cases, the reasons for failure are obvious:



● These brain coral polyps [below] took six months to fuse into a mass the size of a large grapefruit. In the wild, coral this size would be 15 to 20 years old.

●● Micro-fragments of mountainous star coral [right] grow in a tank in Vaughan's coral nursery.



Corals were planted on piles of unstable rubble left behind by dynamite fishing or massive storms and were quickly buried in sediment.

Others are more mysterious. Razak showed me a triptych of photos from a research study that included sites in Indonesia's Komodo National Park, all taken five years after divers had assembled rock piles on the sea floor to create new reef habitat. In one, the underlying structure was scarcely visible, with huge plate corals and branching corals covering its surface in resplendent pinks and yellows. At another site, it was as though the rocks had been piled up the day before, covered only in a thin layer of algae. The third was completely buried in sediment.

Lisa Carne has brought Vaughan down to Belize three times to lead trainings on coral restoration and aquaculture. But where he focuses on trying to "plant a million corals," she says, "we're looking backwards at our data and talking about the opposite: If you pick the right site and the right corals, and everything else lines up, you shouldn't have to keep adding in one spot." In other words, what's the minimum amount of coral you can outplant on a given reef to help nature take its course?

Vaughan, Carne, and others are all trying to find ways to improve corals' odds of survival, tracking the performance of different genotypes, or the influence of current, depth, temperature, and the presence of fish and other aquatic species on the fragments they outplant. Depending on your point of view, coral restoration is either a profoundly pessimistic or optimistic undertaking. To some it suggests we're past hoping humans will act forcefully enough to curb water pollution, designate new marine protected areas, or, above all, slash emissions to help natural reef systems withstand global warming. To others, restoration serves as penance for the damage we've already done, and a way to maximize our chances of shepherding corals through the Anthropocene.

In the grand scheme of things, corals will survive. Reefs are as old as almost any life in the sea, going back to the very first photosynthetic organisms on the planet—cyanobacteria that began secreting calcium carbonate more than 2 billion years ago. The photosynthesis on these early reefs drove the creation of an oxygen-rich atmosphere that would sustain advanced life. Corals have undergone mass diebacks before, and in geologic time, they rebound quickly. But quickly is measured in millions of years.

Vaughan sees his tinkering with coral as being in the service of a world where humans are willing to address the root causes of its distress. When he imagines people visiting his future roadside attraction, it isn't to make them see the wonders of micro-fragmenting but rather to understand the bigger picture. "You want to know that when they go home they're going to vote correctly, or recycle better, or lower their thermostat, or eat down the food chain," he says. Like polar bears or any species in peril, corals are simply an indicator, Vaughan says. "And what that's saying is, 'you're next.'" ▮

ROWAN MOORE GERETY *(@rowanmg) is a reporter and audio producer based in Phoenix, Arizona.*

THE CRYPTO TRAP

INSIDE THE BUST OF THE LARGEST KNOWN CHILD SEX ABUSE SITE IN HISTORY—AND HOW IT SHREDDED THE MYTH OF BITCOIN'S UNTRACEABILITY.

BY ANDY GREENBERG

ILLUSTRATION / MIKE McQUADE

CHAPTER

01

DIVINING ROD

CONTENT WARNING: The story told here includes references to suicide and child abuse, though the abuse is not graphically described.

EARLY ONE FALL morning in 2017, in a middle-class suburb on the outskirts of Atlanta, Chris Janczewski stood alone inside the doorway of a home he had not been invited to enter.

Moments earlier, armed Homeland Security Investigations agents in ballistic vests had taken up positions around the tidy two-story brick house, banged on the front door, and when a member of the family living there opened it, swarmed inside. Janczewski, an Internal Revenue Service criminal investigator, followed quietly behind. Now he found himself in the entryway, in the eye of a storm of activity, watching the agents search the premises and seize electronic devices.

They separated the family, putting the father, an assistant principal at the local high school and the target of their investigation, in one room; his wife in another; the two kids into a third. An agent switched on a TV and put on *Mickey Mouse Clubhouse* in an attempt to distract the children from the invasion of their home and the interrogation of their parents.

Janczewski had come along on this raid only as an observer, a visitor flown in from Washington, DC, to watch and advise the local Homeland Security team as it executed its warrant. But it had been Janczewski's investigation that brought the agents here, to this average-looking house with its well-kept yard among all the average-looking houses they could have been searching, anywhere in America. He had led them there based on a strange, nascent form of evidence. Janczewski had followed the links of Bitcoin's blockchain, pulling on that chain until it connected this ordinary home to an extraordinarily cruel place on the internet—and then connected that place to hundreds more men around the world. All complicit in the same massive network of unspeakable abuse. All now on Janczewski's long list of targets.

Over the previous few years, Janczewski, his partner Tigran Gambaryan, and a small group of investigators at a growing roster of three-letter American agencies had used this newfound technique, tracing a cryptocurrency that once seemed untraceable, to crack one criminal case after another on an unprecedented, epic scale. But those methods had never led them to a case quite like this one, in which the fate of so many people, victims and perpetrators alike, seemed to hang on the findings of this novel form of forensics. That morning's search in the suburb near Atlanta was the first moment when those stakes became real for Janczewski. It was, as he would later put it, "a proof of concept."

From where Janczewski was positioned at the front of the house, he could hear the Homeland Security agents speaking to the father, who responded in a broken, resigned voice. In another room, he overheard the agents questioning the

man's wife; she was answering that, yes, she'd found certain images on her husband's computer, but he'd told her he had downloaded them by accident when he was pirating music. And in the third room he could hear the two grade-school-age children—kids about as old as Janczewski's own—watching TV. They asked for a snack, seemingly oblivious to the tragedy unfolding for their family.

Janczewski remembers the gravity of the moment hitting him: This was a high school administrator, a husband and a father of two. Whether he was guilty or innocent, the accusations this team of law enforcement agents were leveling against him—their mere presence in his home—would almost certainly ruin his life.

Janczewski thought again of the investigative method that had brought them there like a digital divining rod, revealing a hidden layer of illicit connections underlying the visible world. He hoped, not for the last time, that it hadn't led him astray.

ON A SUMMER'S DAY in London a few months earlier, a South Africa–born tech entrepreneur named Jonathan Levin had walked into the unassuming brick headquarters of the UK's National Crime Agency—Britain's equivalent to the FBI—on the south bank of the Thames. A friendly agent led him to the building's second floor and through the office kitchen, offering him a cup of tea. Levin accepted, as he always did on visits to the NCA, leaving the tea bag in.

The two men sat, cups in hand, at the agent's desk in a collection of cubicles. Levin was there on a routine customer visit, to learn how the agent and his colleagues were using the software built by the company he'd cofounded. That company, Chainalysis, was the world's first tech firm to focus solely on a task that a few years earlier might have sounded like an oxymoron: tracing cryptocurrency. The NCA was one of dozens of law enforcement agencies around the world that had learned to use Chainalysis' software to turn the digital underworld's preferred means of exchange into its Achilles' heel.

When Bitcoin first appeared in 2008, one fundamental promise of the cryptocurrency was that it revealed only which coins reside at which Bitcoin addresses—long, unique strings of letters and numbers—without any identifying information about those coins' owners. This layer of obfuscation created the impression among many early adherents that Bitcoin might be the fully anonymous internet cash long awaited by libertarian cypherpunks and crypto-anarchists: a new financial netherworld where digital briefcases full of unmarked bills could change hands across the globe in an instant.

Satoshi Nakamoto, the mysterious inventor of Bitcoin, had gone so far as to write that "participants can be anonymous" in an early email describing the cryptocurrency. And thousands of users of dark-web black markets like Silk Road had embraced Bitcoin as their central payment mechanism. But the counterintuitive truth about Bitcoin, the one upon which Chainalysis had built its business, was this: Every Bitcoin payment is captured in its blockchain, a permanent, unchangeable, and entirely *public* record of every transaction in the Bitcoin network. The blockchain ensures that coins can't be forged or spent more than once. But it does so by making everyone in the Bitcoin economy a witness to every transaction. Every criminal payment is, in some sense, a smoking gun in broad daylight.

Within a few years of Bitcoin's arrival, academic security researchers—and then companies like Chainalysis—began to tear gaping holes in the masks separating Bitcoin users' addresses and their real-world identities. They could follow bitcoins on the blockchain as they moved from address to address until they reached one that could be tied to a known identity. In some cases, an investigator could learn someone's Bitcoin addresses by transacting with them, the way an undercover narcotics agent

This story is excerpted from the forthcoming book TRACERS IN THE DARK: The Global Hunt for the Crime Lords of Cryptocurrency, *available November 15, 2022, from Doubleday. Andy Greenberg (@a_greenberg) is a senior writer at* WIRED.

might conduct a buy-and-bust. In other cases, they could trace a target's coins to an account at a cryptocurrency exchange where financial regulations required users to prove their identity. A quick subpoena to the exchange from one of Chainalysis' customers in law enforcement was then enough to strip away any illusion of Bitcoin's anonymity.

Chainalysis had combined these techniques for de-anonymizing Bitcoin users with methods that allowed it to "cluster" addresses, showing that anywhere from dozens to millions of addresses sometimes belonged to a single person or organization. When coins from two or more addresses were spent in a single transaction, for instance, it revealed that whoever created that "multi-input" transaction must have control of both spender addresses, allowing Chainalysis to lump them into a single identity. In other cases, Chainalysis and its users could follow a "peel chain"—a process analogous to tracking a single wad of cash as a user repeatedly pulled it out, peeled off a few bills, and put it back in a different pocket. In those peel chains, bitcoins would be moved out of one address as a fraction was paid to a recipient and then the remainder returned to the spender at a "change" address. Distinguishing those change addresses could allow an investigator to follow a sum of money as it hopped from one address to the next, charting its path through the noise of Bitcoin's blockchain.

Thanks to tricks like these, Bitcoin had turned out to be practically the *opposite* of untraceable: a kind of honeypot for crypto criminals that had, for years, dutifully and unerasably recorded evidence of their dirty deals. By 2017, agencies like the FBI, the Drug Enforcement Agency, and the IRS's Criminal Investigation division (or IRS-CI) had traced Bitcoin transactions to carry out one investigative coup after another, very often with the help of Chainalysis.

The cases had started small and then gained a furious momentum. Investigators had traced the transactions of two corrupt federal agents to show that, before the 2013 takedown of Silk Road, one had stolen bitcoins from that dark-web market and another had sold law enforcement intel to its creator, Ross Ulbricht. Next they tracked down half a billion dollars of bitcoins stolen from the Mt. Gox exchange and showed that the proceeds had been laundered by the Russian administrator of another crypto exchange, BTC-e, eventually locating the exchange's servers in New Jersey. And finally, they followed bitcoin trails to nail down the identity of the founder of AlphaBay, a dark-web market that had grown to 10 times the size of Silk Road. (In fact, even as Levin was sitting in London talking to the NCA agent, a coalition of half a dozen law enforcement agencies was converging in Bangkok to arrest AlphaBay's creator.)

Levin was, as always, on the lookout for Chainalysis' next big investigation. After running through a few open cases with him, the NCA agent mentioned an ominous site on the dark web that had recently come onto the agency's radar. It was called Welcome to Video.

The NCA had stumbled across the site in the midst of a horrific case involving an offender named Matthew Falder. An academic based in Manchester, England, Falder would pose as a female artist and solicit nude photos from strangers on the internet, then threaten to share those images with family or friends unless the victims recorded themselves carrying out increasingly demeaning and depraved acts. Ultimately he'd force his victims to commit self-harm and even sexually abuse others on camera. By the time he was arrested, he had targeted 50 people, at least three of whom had attempted suicide.

On Falder's computers, the NCA had found he was a registered user of Welcome to Video, a criminal enterprise that, by its sheer scale, put even Falder's atrocities in the shade. This evidentiary lead then wended its way from the NCA's child exploitation investigations team to the computer crime team, including the cryptocurrency-focused agent at whose desk Levin now sat. Welcome to Video, it seemed, was among the rare sites that sold access to clips of child sexual abuse in exchange for bitcoin. It was clear at a glance that its library of images and videos was uncommonly large, and it was being accessed—and frequently refreshed with brand-new material—by a sprawling user base around the globe.

Sometimes known as "child pornography," the class of imagery that was trafficked on Welcome to Video has increasingly come to be called "child sexual abuse material" by child advocates and law enforcement, so as to strip away any doubt that it involves acts of violence against kids. CSAM, as it is usually abbreviated, had for years represented a massive undercurrent of the dark web, the collection of thousands of websites protected by anonymity software like Tor and I2P. Those anonymity tools, used by millions of people around the world seeking to avoid online surveillance, had also come to serve as the shadow infrastructure for an abhorrent network of abuse, which very often foiled law enforcement's attempts to identify CSAM sites' visitors or administrators.

The NCA agent showed Levin a Bitcoin address that the agency had determined was part of Welcome to Video's financial network. Levin suggested they load it in Chainalysis' crypto-tracing software tool, known as Reactor. He set down his cup of tea, pulled his chair up to the agent's laptop, and began charting out the site's collection of addresses on the Bitcoin blockchain, representing the wallets where Welcome to Video had received payments from thousands of customers.

He was taken aback by what he saw: Many of this child abuse site's users—and, by all appearances, its administrators—had done almost nothing to obscure their cryptocurrency trails. An entire network of criminal payments, all intended to be secret, was laid bare before him.

Over the years, Levin had watched as some dark-web operators wised up to certain of his firm's crypto-tracing tricks. They would push their money through numerous intermediary addresses or "mixer" services designed to throw off investigators, or use the cryptocurrency Monero, designed to be far harder to track. But looking at the Welcome to Video cluster in the NCA office that day, Levin could immediately see that its users were far more naive. Many had simply purchased bitcoins from cryptocurrency exchanges and then sent them directly from their own wallets into Welcome to Video's.

The contents of the website's wallets, in turn, had been liquidated at just a few exchanges—Bithumb and Coinone in South Korea, Huobi in China—where they were converted back into traditional currency. Someone seemed to be continually using large, multi-input transactions to gather up the site's funds and then cash them out. That made it easy work for Reactor to instantly and automatically cluster thousands of addresses, determining that they all belonged to a single service—which Levin could now label in the software as Welcome to Video. What's more, Levin could see that the constellation of exchanges surrounding and connected to that cluster likely held the data necessary to identify a broad swath of the site's anonymous users—not simply who was cashing out bitcoins from the site, but who was buying bitcoins to put into it. The blockchain links between Welcome to Video and its customers were some of the most clearly incriminating connections that Levin had ever witnessed.

These child sexual abuse consumers seemed to be wholly unprepared for the modern state of financial forensics on the blockchain. By the standards of the cat-and-mouse game Levin had played for years, Welcome to Video was like a hapless rodent that had never encountered a predator.

As he sat in front of the NCA agent's laptop, it dawned on Levin, perhaps more clearly than ever before, that he was living in a "golden age" of cryptocurrency tracing—that blockchain investigators like those at Chainalysis had gained a significant lead over those they were targeting. "We've created something extremely powerful, and we're a step ahead of these types of operators," he remembers thinking. "You've got a heinous crime, a terrible thing happening in the world, and in an instant our technology has broken through and revealed in very clear logic who's behind it."

Seeing that someone was cashing out the majority of Welcome to Video's revenues through the two exchanges in South Korea, Levin could already guess that the administrator was very likely located there. Many of the site's users seemed to be paying the site directly from the addresses where they'd purchased the coins, on exchanges like Coinbase and Circle, based in the United States. Taking down this global child abuse network might only require getting another law enforcement agency in either the US or Korea involved, one that could demand identifying details from those exchanges. And Levin had just the agency in mind.

"I have some people who would be interested," he told his NCA host.

But first, as he prepared to leave, Levin silently memorized the first five characters of the Welcome to Video address the agent had shown him. Chainalysis' Reactor software included a feature that could autocomplete Bitcoin addresses based on their first few unique numbers or letters. Five would be enough—a single short password to unlock the living map of a global criminal conspiracy.

※

HE WAS TAKEN ABACK BY WHAT HE SAW: AN ENTIRE NETWORK OF CRIMINAL PAYMENTS, ALL INTENDED TO BE SECRET, WAS LAID BARE BEFORE HIM.

CHAPTER

02

"SERACH VIDEOS"

IT WAS EVENING in Thailand when Levin spoke with Chris Janczewski and Tigran Gambaryan. That night in early July 2017, the two IRS Criminal Investigation special agents were sitting in Bangkok's Suvarnabhumi Airport, stewing over the frustration of being sidelined from the biggest dark-web market takedown in history.

The IRS, by 2017, had come to possess some of the most adept cryptocurrency tracers in the US government. It was Gambaryan, in fact, who had traced the bitcoins of the two corrupt agents in the Silk Road investigations and then cracked the BTC-e money laundering case. Working with Levin, Gambaryan had even tracked down the AlphaBay server, locating it at a data center in Lithuania.

Yet when Gambaryan and Janczewski had come to Bangkok for the arrest of AlphaBay's administrator, the French-Canadian Alexandre Cazes, they had been largely excluded from the inner circle of DEA and FBI agents who ran the operation. They hadn't been invited to the scene of Cazes' arrest, or even to the office where other agents and prosecutors watched a video livestream of the takedown.

For Gambaryan and Janczewski, the story was utterly typical. IRS-CI agents did shoe-leather detective work, carried guns, and made arrests, just like their FBI and DEA counterparts. But because of the IRS's dowdy public image, they often found that fellow agents treated them like accountants. "Don't audit me," their peers from other law enforcement branches would joke when they were introduced in meetings. Most IRS-CI agents had heard the line enough times that it warranted an instant eye roll.

At loose ends in Bangkok, Gambaryan and Janczewski spent much of their time idly contemplating what their next case should be, browsing through Chainalysis' blockchain-tracing software Reactor to brainstorm ideas. Dark-web markets like AlphaBay seemed to have been reduced to a shambles by the Thailand operation, and they'd take months or even years to recover. The agents considered taking on a dark-web gambling site. But illegal online casinos hardly seemed worth their attention.

On the day of their departure from Thailand, Gambaryan and Janczewski arrived at the airport only to find that their flight to DC was badly delayed. Stuck in the terminal with hours to kill, they sat half-awake and bored, literally staring at the wall. To pass the hours, Gambaryan decided to try calling Chainalysis' Levin to discuss next cases. When Levin picked up the phone, he had news to share. He'd been looking into a website that didn't fit among the IRS's usual targets but that he hoped they'd be willing to check out: Welcome to Video.

Child sexual exploitation cases had traditionally been the focus of the FBI and Homeland Security Investigations, certainly not the IRS. In part, that was because child sexual abuse images and videos were most often shared without money changing hands, in what investigators described as a "baseball card trading" system—which put them outside the IRS's domain. Welcome to Video was different. It had a money trail, and it seemed to be a very clear one.

Soon after they arrived back in DC, Gambaryan and Janczewski enlisted a technical analyst named Aaron Bice from a contract technology firm called Excygent, with whom they'd investigated the crypto exchange BTC-e. Together, they charted out Welcome to Video in Reactor and saw what Levin had recognized right away: how glaringly it presented itself as a target. Its entire financial anatomy was laid before them, thousands of clustered bitcoin addresses, many with

ILLUSTRATION / PARTY OF ONE STUDIO

barely concealed pay-ins and cash-outs at exchanges they knew they could squeeze for identifying information. It did indeed look, as Levin said, like "a slam dunk." In short order, Janczewski brought the case to Zia Faruqui, a federal prosecutor, who was instantly sold on the idea of taking on Welcome to Video and formally opened an investigation.

Gambaryan, Janczewski, Bice, and Faruqui made an unlikely team to focus on busting a massive child exploitation network. Janczewski was a tall Midwestern agent with a square jaw, like a hybrid of Sam Rockwell and Chris Evans, who wore horn-rimmed glasses when looking at a computer screen. He'd been recruited to the DC computer crimes team from the IRS office in Indiana after proving his mettle in a grab bag of counterterrorism, drug trafficking, government corruption, and tax evasion cases. Bice was an expert in data analysis and was, as Janczewski described his computer skills, "part robot." Faruqui was a seasoned assistant US attorney with a long history of national security and money laundering prosecutions. He had an almost manic focus and intensity, spoke in a comically rapid patter, and, it seemed to his colleagues, barely slept. And then there was Gambaryan, an agent with buzzed hair and a trim beard who by 2017 had made a name for himself as the IRS's cryptocurrency whisperer and dark-web specialist. Faruqui called him "Bitcoin Jesus."

Yet none of the four had ever worked a child sexual exploitation case. They had no training in handling images and videos of child abuse, whose mere possession, in the hands of normal Americans, represented a felony. They had never even seen these sorts of radioactively disturbing materials, and they had no emotional or psychological preparation for the graphic nature of what they were about to be exposed to.

Still, when the two agents showed Faruqui what they saw in the blockchain, the prosecutor was undeterred by their collective inexperience in the realm of child exploitation. As an attorney who focused on money-laundering cases, he saw no reason why, with the evidence of criminal payments Janczewski and Gambaryan had handed him, they couldn't approach Welcome to Video as, fundamentally, a financial investigation.

"We're going to treat this case like we would any other," he said. "We are going to investigate this by following the money."

※

"YOU CANNOT LET A CHILD BE RAPED WHILE YOU GO AND TRY TO TAKE DOWN A SERVER IN SOUTH KOREA." SIMPLY PULLING THE SITE OFFLINE COULDN'T BE THEIR FIRST PRIORITY.

W

WHEN JANCZEWSKI AND Gambaryan first copied the unwieldy web address, mt3plrzdiyqf6jim.onion, into their Tor browsers, they were greeted by a bare-bones site with only the words "Welcome to video" and a login prompt, a minimalism Janczewski compared to the Google homepage. They each registered a username and password and entered.

Past that first greeting page, the site displayed a vast, seemingly endless collection of video titles and thumbnails, arrayed in squares of four stills per video, apparently chosen automatically from the files' frames. Those small images were a catalog of horrors: scene after scene of children being sexually abused and raped.

The agents had steeled themselves to see these images, but they were still unprepared for the reality. Janczewski remembers the blank shock he felt at the parade of thumbnails alone, the way his brain almost refused to accept what it was seeing. He found that the site had a search page with the misspelled words "Serach videos," written at the top of it. Below the search field, it listed popular keywords users had entered. The most popular was an abbreviation for "one-year-old." The second most popular was an abbreviation for "two-year-old."

Janczewski at first thought he must have misunderstood. He had expected to see recordings of the sexual abuse of young teenagers, or perhaps preteens. But as he scrolled, he found, with mounting revulsion and sadness, that the site was heavily populated with videos of abuse of toddlers and even infants.

"This is a thing, really? No," Janczewski says, numbly recounting his reactions as he first browsed the site. "Oh, there's this many videos on here? No. This can't be real."

The two agents knew that, at some point, they would have to actually watch at least some of the advertised videos. But, mercifully, on their first visits to the site they couldn't access them; to do so, they'd have to pay bitcoins to an address the site provided to each registered user, where they could purchase "points" that could then be traded for downloads. And since they weren't undercover agents, they didn't have the authorization to buy those points—nor were they particularly eager to.

At the bottom of several pages of the site

was a copyright date: March 13, 2015. Welcome to Video had already been online for more than two years. Even at a glance, it was clear that it had grown into one of the biggest repositories of child sexual abuse videos that law enforcement had ever encountered.

As Janczewski and Gambaryan analyzed the site's mechanics, they saw that users could obtain points not just by purchasing them but also by uploading videos. The more those videos were subsequently downloaded by other users, the more points they would earn. "Do not upload adult porn," the upload page instructed, the last two words highlighted in red for emphasis. The page also warned that uploaded videos would be checked for uniqueness; only new material would be accepted—a feature that, to the agents, seemed expressly designed to encourage more abuse of children.

The element of the site that Gambaryan found most unnerving of all, though, was a chat page, where users could post comments and reactions. It was filled with posts in all languages, offering a hint at the international reach of the site's network. Much of the discussion struck Gambaryan as chillingly banal—the kind of casual commentary one might find on an ordinary YouTube channel.

Gambaryan had hunted criminals of all stripes for years now, from small-time fraudsters to corrupt federal law enforcement colleagues to cybercriminal kingpins. He usually felt he could fundamentally understand his targets. Sometimes, he'd even felt sympathy for them. "I've known drug dealers who are probably better human beings than some white-collar tax evaders," he mused. "I could relate to some of these criminals. Their motivation is just greed."

But now he'd entered a world where people were committing atrocities that he didn't understand, driven by motivations that were entirely inaccessible to him. After a childhood in war-torn Armenia and post-Soviet Russia and a career delving into the criminal underworld, he considered himself to be familiar with the worst that people were capable of. Now he felt he had been naive: His first look at Welcome to Video exposed and destroyed a hidden remnant of his idealism about humanity. "It killed a little bit of me," Gambaryan says.

AS SOON AS THEY had seen firsthand what Welcome to Video truly represented, Gambaryan and Janczewski understood that the case warranted an urgency that went beyond that of even a normal dark-web investigation. Every day the site spent online, it enabled more child abuse.

Gambaryan and Janczewski knew their best leads still lay in the blockchain. Crucially, the site didn't seem to have any mechanism for its customers to pull money out of their accounts. There was only an address to which they could pay for credits on the site; there didn't even seem to be a moderator to ask for a refund. That meant that all the money they could see flowing out of the site—more than $300,000 worth of bitcoins at the time of the transactions—would almost certainly belong to the site's administrators.

Gambaryan began reaching out to his contacts in the Bitcoin community, looking for staff at exchanges who might know executives at the two Korean exchanges, Bithumb and Coinone, into which most of Welcome to Video's money had been cashed out, as well as one US exchange that had received a small fraction of the funds. He found that the mere mention of child exploitation seemed to evaporate the cryptocurrency industry's usual resistance to government intervention. "As libertarian as you want to be," Gambaryan says, "this is where everybody kind of drew the line." Even before he sent a formal legal request or subpoena, staff at all three exchanges were ready to help. They promised to get him account details for the addresses he had pulled from Reactor as soon as they could.

In the meantime, Gambaryan continued to investigate the Welcome to Video site itself. After registering an account on the site, he thought to try a certain basic check of its security—a long shot, he figured, but it wouldn't cost anything. He right-clicked on the page and chose "View page source" from the resulting menu. This would give him a look at the site's raw HTML before it was rendered by the Tor Browser into a graphical web page. Looking at a massive block of code, anyway, certainly beat staring at an infinite scroll of abject human depravity.

He spotted what he was looking for almost instantly: an IP address. In fact, to Gambaryan's surprise, every thumbnail image on the site seemed to display, within the site's HTML, the IP address of the server where it was physically hosted: 121.185.153.64. He copied those 11 digits into his computer's command line and ran a basic traceroute function, following its path across the internet back to the location of that server.

Incredibly, the results showed that this computer wasn't obscured by Tor's anonymizing network at all; Gambaryan was looking at the actual, unprotected address of a Welcome to Video server. Confirming Levin's initial hunch, the site was hosted on a residential connection of an internet service provider in South Korea, outside of Seoul.

Welcome to Video's administrator seemed to have made a rookie mistake. The site itself was hosted on Tor, but the thumbnail images it assembled on its homepage appeared to be pulled from the same computer without routing the connection through Tor, perhaps in a misguided attempt to make the page load faster.

Gambaryan couldn't help it: Sitting in front of his computer screen in his DC cubicle, staring at the revealed location of a website administrator whose arrest he could feel drawing closer, the agent started to laugh.

CHAPTER

03

OCTOPUS

JANCZEWSKI WAS AT a firing range in Maryland, waiting his turn in a marksmanship exercise, when he got an email from the American cryptocurrency exchange his team had subpoenaed. It contained identifying information on the suspected Welcome to Video administrator who had cashed out the site's earnings there.

The email's attachments showed a middle-aged Korean man with an address outside of Seoul—exactly corroborating the IP address Gambaryan had found. The documents even included a photo of the man holding up his ID, apparently to prove his identity to the American exchange.

For a moment, Janczewski felt as though he were looking at Welcome to Video's administrator face-to-face. But he remembers thinking that something was off: The man in the picture had noticeably dirty hands, with soil under his fingernails. He looked more like a farm worker than the hands-on-keyboard type he'd expected to be running a site on the dark web.

Over the next days, as the other exchanges fulfilled their subpoenas, the answer began to come into focus. One Korean exchange and then the other sent Gambaryan documents on the men who controlled Welcome to Video's cash-out addresses. They named not just that one middle-aged man but also a much younger male, 21 years old, named Son Jong-woo. The two men listed the same address and shared the same family name. Were they father and son?

The agents believed they were closing in on the site's administrators. But they had come to understand that merely taking down the site or arresting its admins would hardly serve the interests of justice. The constellation of Bitcoin addresses that Welcome to Video had generated on the blockchain laid out a vast, bustling nexus of both consumers and—far more importantly—producers of child sexual abuse materials.

By this point, Faruqui had brought on a team of other prosecutors to help, including Lindsay Suttenberg, an assistant US attorney with expertise in child exploitation cases. She pointed out that even taking the site offline shouldn't necessarily be their first priority. "You cannot let a child be raped while you go and try to take down a server in South Korea," as Faruqui summed up her argument.

The team began to realize that, as simple as this "slam dunk" case had seemed at first, after the easy identification of the site's admins, it was actually massive in its complexity. They would need to follow the money not to just one or two web administrators in Korea, but also from that central point to hundreds of potential suspects—both active abusers and their complicit audience of enablers—around the entire globe.

Gambaryan's right-click discovery of the site's IP address and the quick cooperation from crypto exchanges had been lucky breaks. The real work still lay ahead.

PHOTOGRAPH / TABITHA SOREN

JUST TWO WEEKS after Levin passed along his tip, the team of IRS-CI agents and prosecutors knew almost exactly where Welcome to Video was hosted. But they also knew they'd need help to go further. They had neither connections to the Korean National Police Agency—which had a reputation for formality and impenetrable bureaucracy—nor the resources to arrest what could be hundreds of the site's users, an operation that would require far more personnel than the IRS could muster.

Faruqui suggested they bring Homeland Security Investigations in on the case, partnering with a certain field office across the country, in Colorado Springs. He'd chosen that agency and its far-flung outpost because of a specific agent there whom he'd worked with in the past, an investigator named Thomas Tamsi. Faruqui and Tamsi had together unraveled a North Korean arms trading operation a year earlier, one that had sought to smuggle weapon components through South Korea and China. In the course of that investigation, they'd flown to Seoul to meet with the Korean National Police, where, after some introductions by an HSI liaison there, they spent an evening with Korean officers drinking and singing karaoke.

At a particularly memorable point in the night, the Korean agents had been ribbing the US team for their alleged hot-dog-and-hamburger diets. One agent mentioned *sannakji*, a kind of small octopus that some Koreans eat not merely raw but alive and writhing. Tamsi had gamely responded that he'd try it.

A few minutes later, a couple of the Korean agents had brought to the table a fist-sized, living octopus wrapped around a chopstick. Tamsi put the entire squirming cephalopod in his mouth, chewed, and swallowed, even as its tentacles wriggled between his lips and black ink dripped from his face onto the table. "It was absolutely horrible," Tamsi says.

The Koreans found this hilarious. Tamsi gained near-legendary status within certain circles of the Korean National Police, where he was thereafter referred to as "Octopus Guy."

Like most of their group, Tamsi had no experience in child exploitation cases. He had never even worked on a cryptocurrency investigation. But Faruqui insisted that to make inroads in Korea, they needed Octopus Guy.

NOT LONG AFTERWARD, Tamsi and a fellow HSI agent authorized for undercover operations flew to Washington, DC. They rented a conference room in a hotel, and as Janczewski watched, the undercover agent logged on to Welcome to Video, paid a sum of bitcoins, and began downloading gigabytes of videos.

The strange choice of location—a hotel rather than a government office—was designed to better mask the agent's identity, in case Welcome to Video could somehow track its users despite Tor's protection, and also so that, when it came time to prosecute, the DC attorney's office would be given jurisdiction. (The HSI agent did, at least, use a Wi-Fi hot spot for his downloading, to avoid siphoning the web's most toxic content over the hotel's network.)

As soon as the undercover agent's work was complete, they shared the files with Janczewski, who, along with Lindsay Suttenberg, would spend the following weeks watching the videos, cataloging any clues they could find to the identities of the people involved while also saturating their minds with enough images of child abuse to fill anyone's nightmares for the rest of their lives.

Suttenberg's years as a child exploitation prosecutor had left her somewhat desensitized; she would find that other attorneys on the team couldn't stand to even hear her describe the contents of the videos, much less watch them. "They would ask me to stop talking, to put it in writing," she remembers, "and then they'd tell me that was even worse."

Janczewski, as lead agent on the case, was tasked with putting together an affidavit that would be used in whatever charging document they might eventually bring to court. That meant watching dozens of videos, looking for ones that would represent the most egregious material on the site, and then writing technical descriptions of them for a jury or judge. He compares the experience to a scene from *A Clockwork Orange*: an unending montage from which he constantly wanted to avert his gaze but was required not to.

He says watching those videos altered him, though in ways he could only describe in the abstract—ways even he's not sure he fully understands. "There's no going back," Janczewski says, vaguely. "Once you know what you know, you can't unknow it. And everything that you see in the future comes in through that prism of what you now know."

IN THE FIRST weeks of fall 2017, the team investigating the Welcome to Video network began the painstaking process of tracing every possible user of the site on the blockchain and sending out hundreds of legal requests to exchanges around the world. To help analyze every tendril of Welcome to Video's cluster of Bitcoin addresses in Reactor, they brought on a Chainalysis staffer named Aron Akbiyikian, an Armenian-American former police officer from Fresno whom Gambaryan knew from childhood and had recommended to Levin.

Akbiyikian's job was to perform what he called a "cluster audit"—squeezing every possible investigative clue out of the site's cryptocurrency trails. That meant manually tracing payments back from one prior address to another, until he found the exchange where a Welcome to Video customer had bought their bitcoins—and the identifying information that the exchange likely possessed. Plenty of Welcome to Video's users had made his job easy. "It was a beautiful clustering in Reactor," Akbiyikian says. "It was just so clear." In some cases, he would trace back chains of payments through several hops before the money arrived at an exchange. But for hundreds of users, he says, he could see wallet addresses receive money from exchanges and then put the funds directly into Welcome to Video's cluster, transactions that had created, as Akbiyikian put it, "leads as clean as you could want."

As responses from exchanges with those users' identity information began to pour in, the team started the process of assembling more complete profiles of their targets. They began to collect the names, faces, and photos of hundreds of men—they were almost all men—from all walks of life, everywhere in the world. Their descriptions crossed boundaries of race, age, class, and nationality. All these individuals seemed to have in common was their gender and their financial connection to a worldwide, hidden haven of child abuse.

By this time, the team felt they'd pinned down the site's Korean administrator with confidence. They'd gotten a search warrant for Son Jong-woo's Gmail accounts and many of his exchange records, and they could see that he alone seemed to be receiving the cashed-out proceeds from the site—not his father, who increasingly seemed to the investigators like an unwitting participant, a man whose son had hijacked his identity to create cryptocurrency accounts. In Son Jong-woo's emails, they found photos of the younger man for the first time—selfies he'd taken to show friends where he'd chipped a tooth in a car accident, for instance. He was a thin, unremarkable-looking young Korean man with wide-set eyes and a Beatles-esque mop-top of black hair.

But as their portrait of this administrator took shape, so too did the profiles of the hundreds of other men who had used the site.* A few immediately stuck out to the investigative team: One suspect, to the dismay of Thomas Tamsi and his Homeland Security colleagues, was an HSI agent in Texas. Another, they saw with a different sort of dread, was the assistant principal of a high school in Georgia. The school administrator had posted videos of himself on social media singing duets, karaoke-style, with teenage girls from his school. The videos might otherwise have been seen as innocent. But given what they knew about the man's Bitcoin payments, agents who had more experience with child exploitation warned Janczewski that they might reflect a form of grooming.

These were men in privileged positions of power, with potential access to victims. The investigators could immediately see that, as they suspected, they would need to arrest some of Welcome to Video's users as quickly as possible, even before they could arrange the takedown of the site. Child exploitation experts had cautioned them that some offenders had systems in place to warn others if law enforcement had arrested or compromised them—code words or dead man's switches that sent out

** For several reasons, we've chosen not to identify the defendants in the Welcome to Video case by name, with the exception of the site's administrator. In some instances, at the time of this writing, a defendant's case had not been fully adjudicated. In other cases, we left out names at the request of prosecutors, to avoid providing information that might inadvertently identify victims. We applied the same standard to the rest, to avoid singling out some offenders while others went unnamed.*

alerts if they were absent from their computer for a certain period of time. Still, the Welcome to Video investigation team felt they had little choice but to move quickly and take that risk.

Another suspect, around the same time, came onto their radar for a different reason: He lived in Washington, DC. The man's home, in fact, was just down the street from the US attorneys' office, near the capital's Gallery Place neighborhood. He happened to live in the very same apartment building that one of the prosecutors had only recently moved out of.

That location, they realized, might be useful to them. Janczewski and Gambaryan could easily search the man's home and his computers as a test case. If that proved the man was a Welcome to Video customer, they would be able to charge the entire case in DC's judicial district, overcoming a key legal hurdle.

As they dug deeper, though, they found that the man was a former congressional staffer and held a high-level job at a prestigious environmental organization. Would arresting or searching the home of a target with that sort of profile cause him to make a public outcry, sinking their case?

Just as they trained their sights on this suspect in their midst, however, they found that he had gone strangely quiet on social media. Someone on the team had the idea to pull his travel records. They found that he had flown to the Philippines and was about to fly back to DC via Detroit.

This discovery led the agents and prosecutors to two thoughts: First, the Philippines was a notorious destination for sex tourism, often of the kind that preyed on children—the HSI office in Manila constantly had its hands full with child exploitation cases. Second, when the man flew back to the US, Customs and Border Protection could legally detain him and demand access to his devices to search for evidence—a bizarre and controversial carve-out in Americans' constitutional protections that, in this case, might come in handy.

Would their DC-based suspect sound the alarm and tear the lid off their investigation, just as it was getting started?

"Yes, this all had the potential to blow up our case," Janczewski says. "But we had to act."

※

JANCZEWSKI SPOTTED SOMETHING THAT GAVE HIM A JOLT: THE GIRL IN THE VIDEO HAD A RED FLANNEL SHIRT TIED AROUND HER WAIST.

IN LATE OCTOBER, Customs and Border Protection at the Detroit Metropolitan Airport stopped a man disembarking from a plane from the Philippines on his way back to Washington, DC, asking him to step aside and taking him into a secondary screening room. Despite his vehement protests, the border agents insisted on taking his computer and phone before allowing him to leave.

A few days later, on October 25, the prosecutor who had lived in the same DC apartment block as the suspect saw an email from her old building's management; she'd remained on the distribution list despite having moved out. The email noted that the parking garage ramp in an alley at the back of the tower would be closed that morning. An unnamed resident, it explained, had landed there after jumping to their death from the balcony of their apartment.

The prosecutor put two and two together. The jumper was their Welcome to Video "test case." Janczewski and Gambaryan immediately drove to the apartment tower and confirmed with management: The very first target of their investigation had just killed himself.

Later that day the two IRS-CI agents returned to the scene of the man's death with a search warrant. They rode the elevator up to the 11th floor with the building's manager, who was deeply puzzled as to why the IRS was involved, but wordlessly unlocked the door for them. Inside they found an upscale, moderately messy apartment with high ceilings. There were suitcases still not fully unpacked from a trip. The man had ordered a pizza the night before, and part of it remained uneaten on the table.

Janczewski remembers feeling the somber stillness of the man's empty home as he imagined the desperate choice he had faced the night before. Looking down 11 floors from the balcony, the agent could see the spot in the alleyway below where the pavement had recently been hosed off.

DC's metropolitan police offered to show the agents a security cam video of the man falling to his death. They politely declined. The Customs and Border Protection office in Detroit, meanwhile, confirmed that they had searched the computer seized from the man at the airport—some of its storage was encrypted, but other parts were not—and found child exploitation videos, along with surreptitiously recorded videos of adult sex. Their decision to target the man had served its purpose: Their test case had come back positive.

The prosecutors in DC paused their work briefly to meet and acknowledge the surreal shock of the man's death—their investigation of a site hosted halfway around the world had already led someone to kill themselves, just blocks away. "It was just a reminder of how serious what we were investigating was," Faruqui says. Still, the group agreed: They couldn't let the suicide distract them from their work.

"We've got to focus on the victims here," Faruqui remembers them telling each other. "That provides clarity."

Janczewski says he would have much preferred that the man be arrested and charged. But he had, by this point, been forced to watch hour after hour of child sexual abuse videos. He had put aside his emotions early on in the case, and he had few sympathies to spare for an apparent customer of those materials.

If he felt anything, he admits, it was relief, given the time that the suicide had saved him: They still had hundreds more Welcome to Video customers to pursue.

N

NEXT ON THEIR list was the high school assistant principal. Just days later, Janczewski flew down to Georgia and joined a tactical team of HSI agents as they carried out their search. For the first time, he came face-to-face with an alleged Welcome to Video client in his own home.

In spite of his stoicism, this second test case affected Janczewski more than the DC target had. The tidy, well-kept brick two-story house. The parents questioned in separate rooms. The kids the same age as Janczewski's own, watching *Mickey Mouse Clubhouse*. As he stood in the entryway of that house outside of Atlanta, the full toll of the investigation hit him—the fact that every name on their list was a person with human connections and, in many cases, a family. That even accusing suspects of such an unforgivable crime had an irreversible impact on their lives—that it was "a scarlet letter for someone that just cannot be undone," as he put it.

Janczewski and the HSI agents stayed at the home long enough to search it, to question the man, and to seize his devices for analysis. In addition to the evidence of the man's payments for material on Welcome to Video, Faruqui says that the man also admitted to "inappropriately touching" students at his school. The man would later be charged with sexual assault of minors—though he would plead not guilty.

For Janczewski, at least, any last doubts he had felt after his first confrontation with a suspect based on cryptocurrency tracing alone were dispelled in a matter of hours. "At the end of the day, I felt more confident," he says. "We were correct." The blockchain had not lied.

T

THE TEAM WAS steadily working their way through their short list of high-priority Welcome to Video targets and test cases. But in December 2017, they came upon a different sort of lead—one that would scramble their priorities yet again.

As they followed Welcome to Video's financial trails, investigators had been careful to record the full contents of the site's chat page, where users were still posting a steady stream of comments against a backdrop of spam and trolling typical of any anonymous web forum. The site seemed to be entirely unmoderated: There was not so much as an admin email or help contact visible anywhere. But Janczewski began to notice repeated messages from one account that seemed to offer the closest thing the site had to that missing help-desk contact: "Contact the admins," the messages read, "if you want assistance in fixing error." It included an address on Torbox, a privacy-focused Tor-based email service.

Was this an actual moderator on the site? Or even the administrator himself—the owner of the site, who they now believed to be Son Jong-woo?

As Janczewski tried to decipher who was behind those messages, he checked the username before the "@" in the Torbox address, a unique-looking string of six characters, to see if it matched a user on Welcome to Video. Sure enough, he found that someone with that same handle had uploaded more than a hundred videos.

Excygent's Aaron Bice had the idea to

run this Torbox email address against a database seized from BTC-e during IRS-CI's probe of the crypto exchange, to search for clues in its treasure trove of criminal underworld user data. Bice found a match: One account on BTC-e had been registered with an email address that included that same unique string of six characters. It wasn't the Torbox email address, but one from a different privacy-focused email service called Sigaint.

Janczewski knew that Torbox and Sigaint, both dark-web services themselves, wouldn't respond to legal requests for their users' information. But the BTC-e data included IP addresses for 10 past logins on the exchange by the same user. In nine out of 10, the IP address was obscured with a VPN or Tor. But in one single visit to BTC-e, the user had slipped up: They had left their actual home IP address exposed. "That opened the whole door," says Janczewski.

A traceroute showed that the IP address led to a residential internet connection—not in Korea this time, but in Texas. Was there a second Welcome to Video admin, this one based in the US? Janczewski and Bice continued pulling the thread with increasing urgency, subpoenaing the user's account information from their internet service provider.

It was a Friday morning in early December, and Janczewski was drinking coffee at his desk in the IRS-CI office when he got back the results of that subpoena. He opened the email to find a name and a home address. The man was an American in his thirties who lived in a town outside of San Antonio—an unlikely collaborator for a 21-year-old Korean managing a child exploitation site from 15 time zones away. But the man's employment, when Janczewski looked it up, was even more jarring: He was another Department of Homeland Security staffer—this time a Border Patrol agent.

Janczewski quickly began to assemble public information about the agent from his social media accounts. He first found a Facebook page for the man's wife, and later an account for the man himself, with his name written backwards to obscure it. Bice dug up his Amazon page, too, where he seemed to have left reviews on hundreds of products and put others on a "wish list"—including external storage devices that could hold terabytes of videos, hidden cameras, and other cameras designed to be snaked through small spaces, like holes drilled in a wall.

Finally, with a creeping sense of dread, Janczewski saw that the Border Patrol agent's wife had a young daughter—and that he had created a crowdfunding page on GoFundMe to raise money to legally adopt the girl as his stepdaughter. "*Fuck*," Janczewski thought to himself. "Did he upload videos of the daughter?"

Janczewski looked back at Welcome to Video and saw that some of the thumbnails of the videos uploaded by the person with this username showed the sexual assault of a young girl about the daughter's age. He realized he now had a duty to separate this Border Patrol agent from his victim as swiftly as possible.

For the next 10 days, Janczewski barely left his desk. He'd drive home, eat dinner quickly with his family in their small Arlington, Virginia, townhouse, then drive back to the office to work late, often calling Bice and Faruqui well into the night.

"You are rarely in a situation where your time is zero-sum," Faruqui says. "Every moment we were not working on that case, a little girl could be getting raped."

Janczewski asked their undercover HSI agent to download the videos that had been uploaded by the Texas agent, and he began the grueling process of watching them one by one. A few videos in, he spotted something that jolted the pattern-matching subroutines of his brain: At one point in the recording, the girl in the video had a red flannel shirt tied around her waist. He looked back at a photo of the girl posted to the GoFundMe page and saw it: She was wearing the same red flannel.

Was this Border Patrol agent an admin on Welcome to Video? A moderator? It hardly mattered. Janczewski had found the identity of an active child rapist who lived with his victim and had been recording and sharing his crimes with thousands of other users. The Texas man had earned a place at the very top of their target list.

T

TWO WEEKS BEFORE Christmas, on the 10th day after he'd identified the Border Patrol agent, Janczewski flew to southern Texas, along with HSI's Thomas Tamsi and his team's child-exploitation-focused prosecutor, Lindsay Suttenberg. On a cool, dry evening about a hundred miles from the Mexican border, Tamsi and a group of Texas State Police officers tailed their target as he drove home from work and pulled him over. Together with a group of FBI agents, they took the man to a nearby hotel for questioning.

Meanwhile Janczewski and a group of local Homeland Security investigators entered the man's house and began to search for evidence. The two-story home was run-down and messy, Janczewski remembers—with the exception of the man's well-organized home office on the second floor, where they found his computer. Down the hall from that office he came to the girl's bedroom and immediately recognized it as the scene where the videos uploaded by the man had been filmed. On the wall he noticed a poster he'd seen in the recordings and momentarily felt as though he'd fallen through the screen of his own computer into the set of a horror film.

※

THE TEAM'S INITIAL LIST OF HIGH-PRIORITY SUSPECTS WAS FINALLY CHECKED OFF. THEY COULD MOVE ON TO THEIR PRIMARY TARGET: SON JONG-WOO.

The IRS agent and prosecutor had brought with them an FBI interviewer with child exploitation experience, who separated the girl from the agents searching her home and took her to a safer location. The girl eventually detailed to the interviewer the abuse she'd endured.

Shortly after the search of the Border Patrol agent's home, Janczewski arrived at the hotel room where other agents were questioning their suspect. He saw, for the first time, the target of his last week-and-a-half's obsession. The man was tall and burly, still in his uniform, with thinning hair. He initially refused to talk about any physical abuse he might have committed, Janczewski says, but he eventually confessed to possessing, sharing, and—finally—making child sexual abuse videos.

Janczewski was struck by the dispassionate, almost clinical way the man described his actions. He gave his interrogators the password to his home computer, and an agent still at the house began pulling evidence from the machine and sending it to Janczewski. It included detailed spreadsheets of every child sexual exploitation video the man had both amassed on his hard drives and, by all appearances, filmed in his own home.

Another spreadsheet from the man's computer contained a long list of other Welcome to Video users' login credentials. Under questioning, the man explained his scheme: He would pose as an administrator in messages he posted to the site's chat page, then ask users who took the bait to send him their usernames and passwords, which he'd use to log in to their accounts and access their videos.

The Border Patrol agent had never been a Welcome to Video administrator or moderator at all, only a particularly devious visitor to the site, willing to scam his fellow users to support his own appetites.

After an intense 10 days, they'd identified and arrested another alleged child abuser, even rescued his victim. But as he flew back to DC, Janczewski knew that Welcome to Video's vastly larger network of abuse remained very much intact. And until they took the site itself down, it would continue to serve its videos—including the very ones the Border Patrol agent had uploaded from his Texas home office—to an anonymous throng of consumers just like him.

CHAPTER

04

KOREA

IN EARLY JANUARY of 2018, the DC investigators got word from Thomas Tamsi that he and the team had arrested the other federal law enforcement customer of Welcome to Video, the HSI agent who'd shown up early in their blockchain tracing and subpoenas. Though seemingly unconnected to the Border Patrol agent case, this second agent had been based in Texas, too, less than an hour away from the home of the man they had just raided.

Aside from that grim coincidence, the news of the HSI agent's arrest also meant that the DC team's initial list of high-priority suspects was finally checked off. They could move on to their primary target, Son Jong-woo—and the Welcome to Video server under his control.

By February, that Korea-focused operation was coming together. Before the Texas arrests, Janczewski, Gambaryan, Faruqui, and Tamsi had flown to Seoul to meet the Korean National Police Agency. At a dinner set up by the local HSI attaché, the director of the KNPA himself told Tamsi—whose octopus-eating reputation preceded him—that the Americans would have the help of his "best team." Soon they had Son Jong-woo under constant surveillance as he came and went from his home, an apartment two and a half hours south of Seoul in the province of South Chungcheong.

Now, in the depths of winter on the Korean peninsula, just a week after Korea had hosted the Olympics in Pyeongchang, the American agents arrived in Seoul again. Gambaryan had to stay behind for a badly timed conference where the agency's director had volunteered him to speak. But Janczewski and Faruqui brought with them Aaron Bice and Youli Lee, a Korean-American computer crime prosecutor on their team. By this point, too, a growing international force had assembled around the case. The UK's National Crime Agency, which had launched its own investigation into Welcome to Video just after Levin's London visit, sent two agents to Seoul, and the German Federal Police also joined the coalition. It turned out the Germans had been pursuing the site's administrators independently, even before they'd learned about the IRS's investigation, but they'd never been able to secure the cooperation of the Korean National Police.

At one point Faruqui remembers a German official asking him, as they stood in the cold outside the Seoul hotel where they were staying, how the Americans had gotten the Koreans on board so quickly. "Oh, Octopus Guy," Faruqui had explained. "You don't have Octopus Guy. We have Octopus Guy."

FOR THEIR FIRST days in Seoul, the takedown team met repeatedly in the Korean National Police offices to talk through their plans. Their tracing of the IP address, based on Gambaryan's fortu-

ILLUSTRATION / HOKYOUNG KIM

itous right-click, seemed to show that the site's server was located, bizarrely, not in any web-hosting firm's data center but in Son Jong-woo's own apartment—the evidentiary hub of a massive child sexual abuse video network, sitting right in his home. That made things simple: They would arrest him, tear his site offline, and use that evidence to convict him. The team made a plan to grab him in his apartment early on a Monday morning.

Then, on the Friday before, Janczewski got a cold. He spent much of the weekend with prosecutor Youli Lee, dazedly wandering between markets and stores in Seoul trying to pronounce *gaseubgi*, the Korean word for humidifier. On Sunday evening, he took a dose of what he hoped was a Korean equivalent of Nyquil—he couldn't read the label—with the intention of getting some sleep and recovering in time to be at full strength for the arrest.

That's when the KNPA alerted the team that the plan had changed: Son had unexpectedly driven into Seoul for the weekend. Now the team following his whereabouts believed he had begun a late-night drive back to his home south of the city.

If the police could drive down to Son's home that night and stake it out, perhaps they could be there when he returned, ready to arrest him at his door. That way he couldn't destroy evidence or—another looming concern after the death of their Washington, DC, target—commit suicide. "We had to scramble," Janczewski says.

That evening, Faruqui insisted the group put their hands in for a "Go team!" cheer in their hotel lobby. Then he and Lee went up to their rooms to go to bed. Janczewski—sick, half asleep from cold medication, and clutching a pillow from his hotel room—walked out into the pouring rain and got in a car with the HSI liaison to start the long night-drive south. The HSI agent had begged Janczewski to take the wheel of another car in the caravan, instead of an elderly Korean man on his team who was, the agent said, a notoriously bad driver. But Janczewski insisted he was far too medicated to navigate the dark, wet highways of a country 7,000 miles from his home.

A few hours later, the team arrived in the parking lot of Son's apartment—a 10-story tower with a few small buildings on one side and a vast, empty rural landscape on the other—to begin their long stakeout in the rain. It was well past midnight when they saw Son's car finally pull into the parking garage of the complex.

A group of Korean agents had been waiting there for him. One particularly imposing officer, whom the HSI agents referred to as "Smiley"—because he never smiled—led a team of plainclothes police, sidling into the elevator next to Son as he got inside. The agents silently rode the elevator up to Son's floor with him and stepped out when he did. They arrested him, without resistance, just as he reached his front door.

Throughout that arrest and the hours-long search of Son's apartment that followed, Janczewski and the other foreigners remained stuck in their cars in the rain-drenched parking lot. Only the National Police had authorization to lay hands on Son or enter his home. When the Korean officers had the young Welcome to Video admin handcuffed, they asked him if he'd consent to letting Janczewski or any of the Americans come in as well. Son, unsurprisingly, said no. So Janczewski was limited to a tour via FaceTime of the small and unremarkable apartment that Son shared with his divorced father, the man with the soiled

hands in the first photo they'd examined, as the Korean agents scoured it for evidence and seized his devices.

The Korean agent showing Janczewski around eventually pointed the phone's camera at a desktop computer on the floor of Son's bedroom, a cheap-looking tower-style PC with its case open on one side. The computer's guts revealed the hard drives that Son seemed to have added, one by one, as each drive had filled up with terabytes of child exploitation videos.

This was the Welcome to Video server.

"I was expecting some kind of glowing, ominous thing," Janczewski remembers, "and it was just this dumpy computer. It was just so strange. This dumpy computer, that had caused so much havoc around the world, was sitting on this kid's floor."

ON THE RETURN TRIP, Janczewski learned exactly why the HSI liaison had wanted him to drive the other car. The elderly HSI staffer behind the wheel of the other vehicle in their caravan was somehow so disoriented after a sleepless night that he turned the wrong way down a highway exit ramp, narrowly avoiding a high-speed collision and terrifying his passenger, Aaron Bice.

After barely averting that disaster, as the sun began to rise and the rain let up, the group pulled over at a truck stop along the highway to have a breakfast of gas-station instant ramen. Janczewski, still sick and utterly exhausted, was struck by how anticlimactic it all seemed. His team had located and extricated both the administrator and the machine at the epicenter of the malevolent global network they were investigating. He had been anticipating this moment for more than six months. But he felt no elation.

There were no high fives, no celebrations. The agents got back in their cars to continue the long drive back to Seoul.

※

THERE WERE MORE THAN 250,000 VIDEOS ON THE SERVER—MORE CONTENT BY VOLUME THAN IN ANY CHILD SEXUAL ABUSE MATERIALS CASE IN HISTORY.

THE NEXT DAY, after finally getting some sleep, Janczewski began to see past the dreariness of the previous night's operation to understand just how lucky they had been. He learned from the forensic analysts who had examined Son Jong-woo's computers that Son hadn't encrypted his server. Everything was there: all of Welcome to Video's content, its user database, and the wallets that had handled all of its Bitcoin transactions.

The scale of the video collection, now that they could see it in its entirety, was staggering. There were more than 250,000 videos on the server, more content by volume than in any child sexual abuse materials case in history. When they later shared the collection with the National Center for Missing and Exploited Children (NCMEC), which helps to catalog, identify, and take down CSAM materials across the internet, NCMEC found that it had never seen 45 percent of the videos before. Welcome to Video's uniqueness check and incentive system for fresh content appeared to have served its purpose, motivating countless new cases of recorded child abuse.

The real prize for the investigators, however, was the site's user information. The Korean National Police gave the US team a copy of Welcome to Video's databases, and they got to work in a US Embassy building in Seoul, reconstructing those data collections on their own machine. Meanwhile, to avoid tipping off the site's users to the takedown, they quickly set up a look-alike Welcome to Video homepage on their own server, using the private key pulled from the real server to take over its dark-web address. When users visited the site, it now displayed only a message that it was under construction and would be back soon with "upgrades," complete with typos to mimic

Son's shoddy English spelling.

Bice spent two days with his head down, rebuilding the site's user data in a form they could easily query—with Janczewski and Faruqui standing behind him, pestering him to see if the system was ready yet. When Bice was finished, the US team had a full directory of the site's pseudonymous users, listed by their Welcome to Video usernames. They could now link every Bitcoin payment they had initially mapped out on the blockchain with those usernames and look up exactly what content each of those users had uploaded or downloaded.

By the time the Americans were ready to go home at the end of February, they had integrated the de-anonymized identities from their cryptocurrency exchange subpoenas into a searchable database. It mapped out the entire Welcome to Video network, complete with users' real-world names, photos, and—for those who had paid into the site—the record of those payments and the exact child abuse videos those customers had bought access to. "You could see the whole picture," Janczewski says. "It was like a dictionary, thesaurus, and Wikipedia all put together."

They had, arrayed before them, the fully revealed structure of Welcome to Video's global child exploitation ring—hundreds of exquisitely detailed profiles of consumers, collectors, sharers, producers, and hands-on abusers alike. Now the final phase of the case could begin.

※

IF NOT FOR CRYPTOCURRENCY, AND THE YEARS-LONG TRAP SET BY ITS PURPORTED UNTRACEABILITY, MOST OF THE 337 PEDOPHILES ARRESTED IN THE CASE—AND THEIR RESCUED VICTIMS—LIKELY NEVER WOULD HAVE BEEN FOUND.

O

OVER THE WEEKS that followed, Thomas Tamsi's team in Colorado began sending their Welcome to Video dossiers to HSI agents, local police, and foreign police agencies around the world. These "targeting packages" included descriptions of the suspects, the record of their transactions, any other evidence they'd assembled about them, and—given that they were being sent out to law enforcement agents who had in some cases never been involved in a cryptocurrency-related investigation—short primers on how Bitcoin and its blockchain worked.

There would be no coordinated, global takedown, no attempt to create shock and awe with simultaneous arrests. The case's defendants were far too distributed and international for that kind of synchronized operation. Instead, searches, arrests, and interviews began to roll out across the globe—prioritized by those they'd learned might be active abusers, then uploaders, and finally downloaders. Slowly, as Welcome to Video's users were confronted, one by one, the DC team began to hear back about the results of their work—with harrowing, sometimes gratifying, often tragic outcomes.

A Kansas IT worker—whose arrest they'd prioritized when they found that his wife ran an at-home daycare for infants and toddlers—had deleted all of his child abuse videos from his computer before the agents arrived. Prosecutors say he later confessed when remnants of the files in the computer's storage matched their records from the Welcome to Video server.

When the agents came for a twenty-

something man in New York, his father blocked the door of their apartment, thinking at first that it was a break-in. But when agents explained what their warrant was for, he turned on his son and let them in. The son, it later turned out, had sexually assaulted the daughter of a family friend and surreptitiously recorded another young girl through her webcam, according to prosecutors.

A repeat offender in Washington, DC, tried to commit suicide when the HSI team entered his home; he hid in his bathroom and slit his own throat. One of the arresting agents happened to have training as an Army medic. He managed to slow the bleeding and keep the man alive. They later found 450,000 hours of child abuse videos on his computers—including recordings of the girl in Texas that had been uploaded by the Border Patrol agent.

As months passed, the stories continued to pile up, a mix of the sordid, sad, and appalling. An elderly man in his seventies who had uploaded more than 80 child abuse videos. A man in his early twenties with traumatic brain damage, whose medication had heightened his sexual appetites and reduced his impulse control, and who was deemed to have the same level of cognitive development as the preteens whose abuse he'd watched. A New Jersey man whose communications, when they were revealed through a search warrant, seemed to show his negotiations to purchase a child for his own sexual exploitation.

Thomas Tamsi, as the lead HSI agent on the case, coordinated more Welcome to Video arrests than anyone else—more than 50, by his count—and was present for enough of them that they became a blur in which only the most jarring moments remain distinct in his mind. The mostly nude defendant he found in a basement. The suspect who told him he had been involved in the Boy Scouts and that "children had always been attracted" to him. Parents of victims who vehemently denied that a family friend could have done the things Tamsi described, and whose faces then went white as he slid printouts of redacted screenshots across the table.

The cases spanned the globe, well beyond the US. Dozens of Welcome to Video users were arrested in the Czech Republic, Spain, Brazil, Ireland, France, and Canada. In England, where the entire case had started with an agent's tip to Levin, the country's National Crime Agency arrested one 26-year-old who had allegedly abused two children—one of whom they found naked on a bed in his home—and uploaded more than 6,000 files to the site. In another international case, a Hungarian ambassador to Peru who downloaded content from Welcome to Video was found to have more than 19,000 CSAM images on his computer. He was quietly removed from his South American post, taken to Hungary, and charged; he pleaded guilty.

For the DC team, many of the international cases fell into a kind of black hole: One Saudi Arabian Welcome to Video user returned to his home country and was captured by that country's own law enforcement. Faruqui and Janzewski say they never heard what happened to the man; he was left to the Saudis' own justice system, which sentences some sex criminals to the Sharia-based punishments of whipping or even beheading. When agents searched the car of a Chinese national living near Seattle with a job at Amazon, they found a teddy bear, along with a map of playgrounds in the area, despite the man having no children of his own. The man subsequently fled to China and, as far as prosecutors know, was never located again.

In each of the hundreds of intelligence packets that the team sent out, Chris Janczewski's contact was listed as the number to call with any questions. Janczewski found himself explaining the blockchain and its central role in the case again and again, to HSI agents and local police officers around the US and the world, many of whom had never even heard of Bitcoin or the dark web. "You get this lead sent to you that says, 'Here's this website and this funny internet money,'" Janczewski says, imagining how those on the receiving end of the intelligence packets must have seen it, "and now you need to go arrest this guy because some nerd accountant says so."

In total, Janczewski traveled to six countries and spoke to more than 50 different people to help explain the case, often multiple times each—including one US prosecutor and agent team with whom he had more than 20 conversations. ("Some were a little more high maintenance, respectfully, than others," he says.) Bice, who oversaw the reconstructed server data, says he spoke to even more agents and officers—well over a hundred, by his count.

Ultimately, from the beginning of the case through the year and a half that followed the server seizure, global law enforcement would arrest no fewer than 337 people for their involvement with Welcome to Video. They also removed 23 children from sexually exploitative situations.

Those 337 arrests still represented only a small fraction of Welcome to Video's total registered users. When the US team examined their copy of the server data in Korea, they had found thousands of accounts on the site. But the vast majority of them had never paid any bitcoins into the site's wallets. With no money to follow, the investigators' trail usually went cold.

If not for cryptocurrency, in other words, and the years-long trap set by its purported untraceability, the majority of the 337 pedophiles arrested in the Welcome to Video case—and their rescued victims—likely never would have been found.

CHAPTER

05

CODA

THE IRS AND the US attorneys' office in DC had taken an unprecedented approach, treating a massive child sexual abuse materials case as a financial investigation, and it had succeeded. Amidst all their detective work, it had been Bitcoin's blockchain that served as their true lodestar, leading them through a landmark case. Without crypto tracing, Faruqui argues, they would never have managed to map out and identify so many of the site's users.

"That was the only path through this darkness," he says. "The darker the darknet gets, the way that you shine the light is following the money."

Throwing money-laundering investigators into the deep end of the internet's CSAM cesspool, however, had taken its toll. Almost every member of the team had children of their own, and almost all of them say they became far more protective of those children as a result of their work, to the degree that their trust in the people around their family has been significantly damaged.

Janczewski, who after the case moved from DC to Grand Rapids, Michigan, won't let his children ride their bikes to school on their own, as he himself did as a child. Even seemingly innocent interactions—like another friendly parent who offers to watch his kids at the other end of a swimming pool—now trigger red alerts in his mind. Youli Lee says she won't allow her 9- and 12-year-old children to go into public bathrooms by themselves. Nor will she allow them to play at a friend's house unless the friend's parents have top-secret security clearances—an admittedly arbitrary rule, but one she says ensures the parents have at least had a background check.

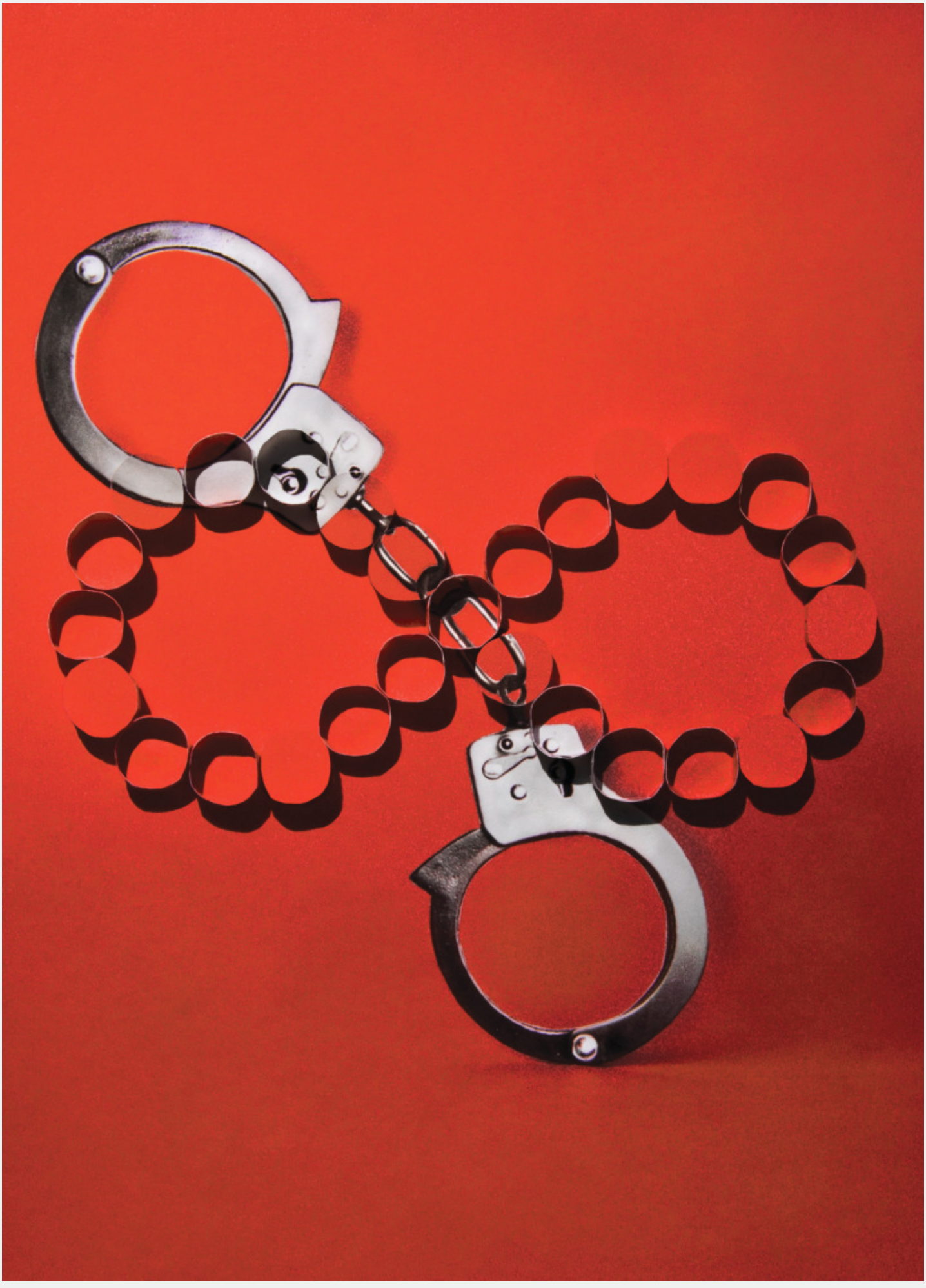
Faruqui says the 15 or so videos he watched as part of the investigation remain "indelibly seared" into his brain and have permanently heightened his sense of the dangers the world presents to his children. He and his wife argue, he says, about his overprotective tendencies. "You always see the worst of humanity, and so you've lost perspective," he quotes his wife telling him. "And I say, '*You* lack perspective, because you don't know what's out there.'"

Gambaryan's wife Yuki says the Welcome to Video case was the only time her hard-shelled, Soviet-born husband ever discussed a case with her and confessed that it had gotten to him—that he was struggling with it emotionally. Gambaryan says that it was, in particular, the sheer breadth of the cross-section of society that participated in the site's abuse that still haunts him.

"I saw that everybody's capable of this: doctors, principals, law enforcement," he reflected. "Whatever you want to call it, evil, or whatever it is: It's in everybody—or it can be in anybody."

PHOTOGRAPH / JOOEUN BAE

Getty Images (handcuffs)



IN EARLY JULY of 2020, Son Jong-woo walked out of a Seoul penitentiary wearing a black long-sleeve T-shirt and carrying a green plastic bag of his belongings. He had spent, due to Korea's lenient laws on child sexual abuse, just 18 months in prison.

US prosecutors, including Faruqui, had argued that he should be extradited to the United States to face charges in the American justice system, but Korea had denied their request. Welcome to Video's convicted creator and administrator was free.

The DC-based team that worked the Welcome to Video case remains deeply dissatisfied with Son's mystifyingly light sentence for running, by some measures, the biggest child sexual abuse materials website in history. But Janczewski says he's comforted by the outcry in Korean society over the case. The country's social media exploded in anger over Son's quick release. More than 400,000 people signed a petition to prevent the judge in the case from being considered for a seat on the country's supreme court. One Korean lawmaker put forward a bill to allow appeals to extradition judgments, and the country's National Assembly introduced new legislation to strengthen punishments for sexual abuse online and downloading child sexual abuse materials.

In the US, meanwhile, the ripple effects of the case continued for years. Janczewski, Bice, and Suttenberg say that they still get calls from law enforcement officials following the leads they assembled. On the computer of the DC investigators' very first test case—the former congressional staffer who committed suicide—they found evidence in a cryptocurrency exchange account that he'd also paid into a different source of dark-web sexual materials. They followed those payments to a site called Dark Scandals, which turned out to be a smaller but equally disturbing dark-web repository of sexual abuse recordings.

Janczewski, Gambaryan, and the same group of prosecutors pursued that Dark Scandals case in parallel with the tail end of the Welcome to Video investigation, similarly following blockchain leads to trace the site's cash-outs. With the help of the Dutch national police, they arrested the site's alleged administrator in the Netherlands, a man named Michael Rahim Mohammad, who went by the online handle "Mr. Dark." He faces criminal charges in the US, and his case is ongoing.

From the perspective of Welcome to Video's money-laundering-focused agents and prosecutors, perhaps the most interesting of the ripple effects of the case stemmed from the fate of the HSI agent they had arrested in Texas, just before their trip to carry out the site takedown in Korea. The Texan man had taken a rare approach to his legal defense: He'd pleaded guilty to possession of child sexual abuse materials, but he also appealed his conviction. He argued that his case should be thrown out because IRS agents had identified him by tracking his Bitcoin payments—without a warrant—which he claimed violated his Fourth Amendment right to privacy and represented an unconstitutional "search."

A panel of appellate judges considered the argument—and rejected it. In a nine-page opinion, they explained their ruling, setting down a precedent that spelled out in glaring terms exactly how far from private they determined Bitcoin's transactions to be.

"Every Bitcoin user has access to the public Bitcoin blockchain and can see every Bitcoin address and its respective transfers. Due to this publicity, it is possible to determine the identities of Bitcoin address owners by analyzing the blockchain," the ruling read. "There is no intrusion into a constitutionally protected area because there is no constitutional privacy interest in the information on the blockchain."

A search only requires a warrant, the American judicial system has long held, if that search enters into a domain where the defendant has a "reasonable expectation of privacy." The judges' ruling argued that no such expectation should have existed here: The HSI agent wasn't caught in the Welcome to Video dragnet because IRS agents had violated his privacy. He was caught, the judges concluded, because he had mistakenly believed his Bitcoin transactions to have ever been private in the first place.

CHRIS JANCZEWSKI SAYS the full impact of the Welcome to Video case didn't hit him until the day in October 2019 when it was finally announced in public and a seizure notice was posted to the site's homepage. That morning, Janczewski received an unexpected call from the IRS commissioner himself, Charles Rettig.

Rettig told Janczewski that the case was "this generation's Al Capone"—perhaps the highest compliment that can be bestowed within IRS-CI, where the story of Capone's takedown for tax evasion holds almost mythical status.

That same day, the Justice Department held a press conference to announce the

investigation's results. US attorney Jessie Liu gave a speech to a crowd of reporters about what the case represented—how following the money had allowed agents to score a victory against "one of the worst forms of evil imaginable."

Chainalysis' Jonathan Levin sat in the audience. Afterward, an IRS official named Greg Monahan, who had supervised Gambaryan and Janczewski, came over to thank Levin for his role in the case. It had all started, after all, with Levin's tip to two bored IRS agents in the Bangkok airport. Monahan told Levin that it was the most important investigation of his career, that he could now retire knowing he had worked on something truly worthwhile.

Levin shook the IRS-CI supervisor's hand. Neither he nor Monahan could know, at that time, of the cases still to come: that IRS-CI and Chainalysis would together go on to disrupt North Korean hackers, terrorism financing campaigns, and two of the largest bitcoin-laundering services in the world. Or that they would track down close to 70,000 bitcoins stolen from the Silk Road and another 120,000 stolen from the exchange Bitfinex, totaling a value of more than $7.5 billion at today's exchange rates, the largest financial seizures—crypto or otherwise—in the Department of Justice's history.

But as he answered Monahan, Levin thought again of the blockchain's bounty of evidence: the countless cases left to crack, the millions of cryptocurrency transactions eternally preserved in amber, and the golden age of criminal forensics it presented to any investigator ready to excavate them.

"There's so much more to do," Levin said. "We're just getting started."

COLOPHON

Traps That Helped Get This Issue Out:

Acting like the pandemic is over; thinking that maybe this time I'll enjoy being social; moving my phone far enough from me at night to ensure I'll get out of bed in the morning the first time the alarm goes off, not the fifth; #ukraine doomscrolling; the TikTok user Canopy Cat Rescue; playing *Fortnite* instead of reading literature; "Overpass Graffiti" by Ed Sheeran; a community garage sale outside Daytona Beach, Florida; getting stranded on Lake Oroville in a solar boat; "Sure, you go to Europe for two weeks while I stay home and take care of the kids"; my first massage (focusing on my … traps); subscription auto-renewals; getting my hand stuck while trying to recover the last dollop of detergent from the bottle; imagining myself younger by riding BMX; when the foster dog puts his head in my lap while I eat, because he knows I'll cave.

WIRED is a registered trademark of Advance Magazine Publishers Inc. Copyright ©2022 Condé Nast. All rights reserved. Printed in the USA. Volume 30, No. 5. WIRED (ISSN 1059–1028) is published monthly, except for combined issues in December/January and July/August, by Condé Nast, which is a division of Advance Magazine Publishers Inc. Editorial office: 520 Third Street, Ste. 305, San Francisco, CA 94107-1815. Principal office: Condé Nast, 1 World Trade Center, New York, NY 10007. Roger Lynch, Chief Executive Officer; Pamela Drucker Mann, Chief Revenue & Marketing Officer, US; Jackie Marks, Chief Financial Officer. Periodicals postage paid at New York, NY, and at additional mailing offices. Canada Post Publications Mail Agreement No. 40644503. Canadian Goods and Services Tax Registration No. 123242885 RT0001.

POSTMASTER: Send all UAA to CFS (see DMM 707.4.12.5); NONPOSTAL AND MILITARY FACILITIES: Send address corrections to WIRED, PO Box 37617, Boone, IA 50037-0662. For subscriptions, address changes, adjustments, or back issue inquiries: Please write to WIRED, PO Box 37617, Boone, IA 50037-0662, call (800) 769 4733, or email subscriptions@wiredmag.com. Please give both new and old addresses as printed on most recent label. First copy of new subscription will be mailed within eight weeks after receipt of order. Address all editorial, business, and production correspondence to WIRED Magazine, 1 World Trade Center, New York, NY 10007. For permissions and reprint requests, please call (212) 630 5656 or fax requests to (212) 630 5883. Visit us online at www.wired.com. To subscribe to other Condé Nast magazines on the web, visit www.condenastdigital.com. Occasionally, we make our subscriber list available to carefully screened companies that offer products and services that we believe would interest our readers. If you do not want to receive these offers and/or information, please advise us at PO Box 37617, Boone, IA 50037-0662, or call (800) 769 4733.

WIRED is not responsible for the return or loss of, or for damage or any other injury to, unsolicited manuscripts, unsolicited artwork (including, but not limited to, drawings, photographs, and transparencies), or any other unsolicited materials. Those submitting manuscripts, photographs, artwork, or other materials for consideration should not send originals, unless specifically requested to do so by WIRED in writing. Manuscripts, photographs, artwork, and other materials submitted must be accompanied by a self-addressed, stamped envelope.

IN SIX WORDS, WRITE A STORY ABOUT AN EXTRAORDINARY COINCIDENCE:

"THAT'S ME!" SHE EXCLAIMED, CROSSING DIMENSIONS.

—Joyce, via email

Honorable Mentions

YOU'RE FROM TEST TUBE 698GX10A TOO?
—AMY STEWART, VIA EMAIL

I HAVE NOT BECOME MY MOTHER.
—@R58TREE, VIA INSTAGRAM

METAVERSE ROME BUILT IN ONE DAY.
—@THESEAISGREEN_, VIA INSTAGRAM

SEPARATED AT BIRTH, THEY DIED SIMULTANEOUSLY.
—@ZEYNABALLEE, VIA INSTAGRAM

OF ALL THE GALILEAN MOON JOINTS ...
—ALISON BOLEYN, VIA EMAIL

THE ANDROID HAD MY HUSBAND'S EYES.
—@HRHBLAKEKNIGHT, VIA INSTAGRAM

YOU HAVE A CLONED T-REX TOO!
—@EMAILABDULLA, VIA INSTAGRAM

WIRED CHOOSES TO PUBLISH THIS STORY.
—@CONNORGERBRANDT, VIA INSTAGRAM

Every month, we ask for a new six-word story on Facebook, Twitter, and Instagram. Submit your ideas there, along with the hashtag #WIREDSIXWORD. And visit the archive at WIRED.com/six-word to see how we've illustrated our favorites.

ILLUSTRATION / VIOLET REED

Give the Perfect Gift to Dads and Grads.

EVERY BOX WORTH $200+

GQ BOX

Use code **GIFT20** for 20% off all gift subscriptions. He'll get the latest GQ-approved essentials every single season.

GQ.COM/WIRED

Order by June 1, 2022 for Father's Day delivery.


RALPH LAUREN'S
POLO SHIRT
THE POLO SHIRT
Polo
by Ralph Lauren
RIZZOLI
NEW YORK
Polo
RALPH LAUREN
POLO
USA