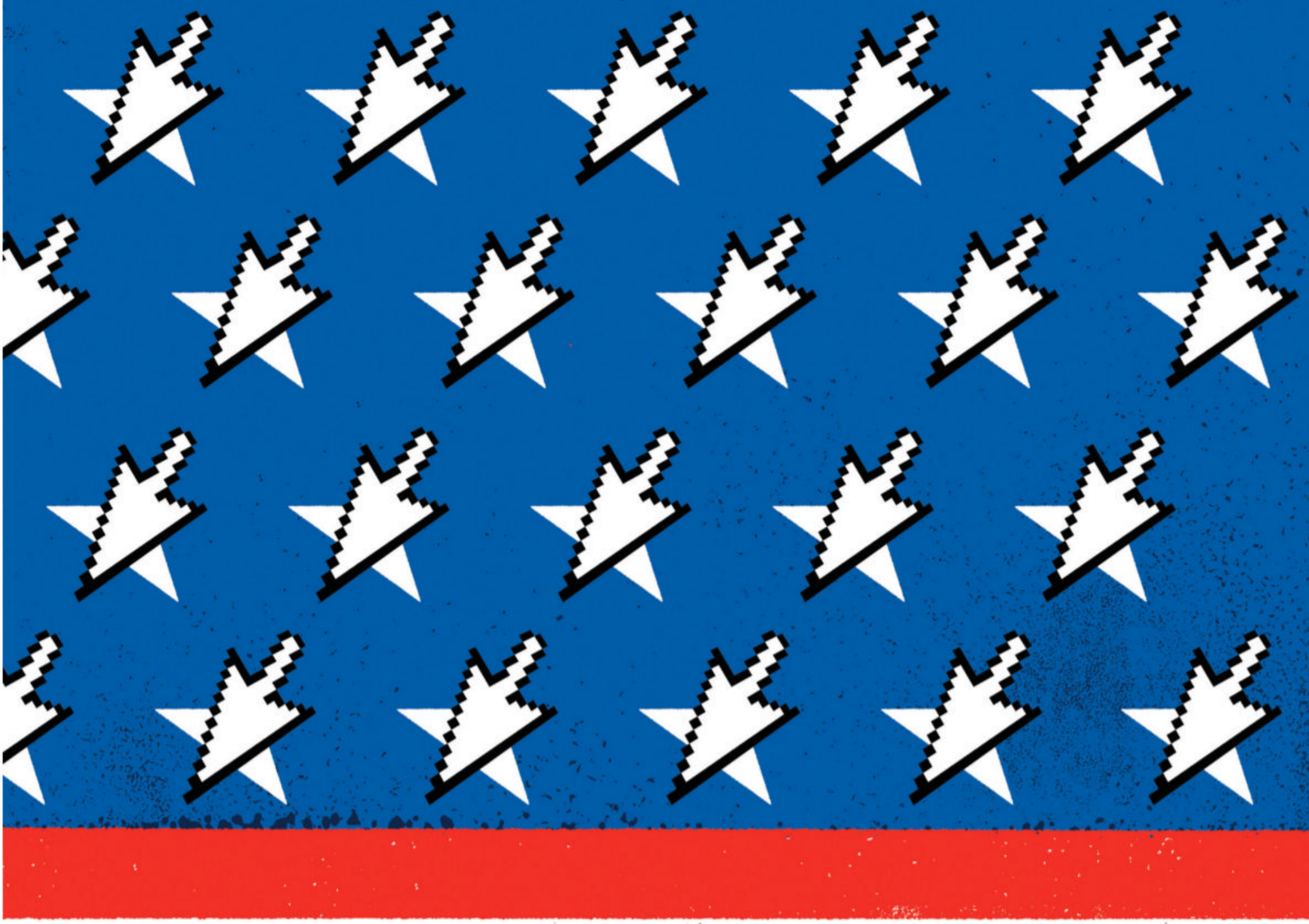
WIRED+

MEET THIS YEAR'S WIRED25

AMERICAN HUSTLE

US elections are in the middle of a major reboot. Our democracy will come out stronger.*



*It just has to survive the next few weeks.

打赏 - JUST FOR FUN

> - 支持分享! 一杯咖啡钱, 打赏金额随意，感谢大家~ :)

支付宝	微信
	

资源来自：https://github.com/hehonghui/the-economist-ebooks

Søme
communñications
kompånies
sēem tö spæk
an.other
langüage.

We speak simple.

That means you can understand our
Unified Communications without
needing a PhD.
Or set up a Contact Center
without having to contact a Contact Center.
Or get customizable Communications APIs that aren't

Absolutely
Pucking
Infuriating.

We want to maximize the impact
and minimize the jargon.

We don't care about making
our tech sound smart,
it just needs to be smart.
Because you shouldn't need to be a developer
to keep your business developing.

So, we'll keep the language of
Business Communications the
way it should be.

Smart,
simple,
and straightforward.

Now we're talking.

VONAGE

INTRODUCING THE **NEW** SLEEP NUMBER 360® SMART BED

The first bed in the world designed to help you fall asleep faster and proven to provide more restful sleep. Enjoy your own personal microclimate as it gently balances surface temperature to keep you both blissfully asleep.

Quality sleep can help boost your immunity, increase energy and improve recovery. Compared to average sleepers, Sleep Number® bed owners enjoy almost an hour more sleep per night.*

NEW Smart 3D fabric is up to 50% more breathable for a cooler sleep surface†

Adjustable comfort on each side

Automatically responds to you

Personalized insights for even better sleep

15-Year Limited Warranty‡

100-Night Trial§

sleep number®

REQUEST SPECIAL OFFERS | 1-877-316-3922 | sleepnumber.com/wired

TOTALLY WIRED

NOTES FROM OUR STAFF

As it did for all of us, 2020 changed Bill Gates' plans. Forgoing his usual agenda of global travel, meetings with world leaders, and speaking at prestigious venues, Gates has been at home. But he's more in demand than ever. That's because, for many years, his foundation has been making huge investments in vaccines, treatments, and testing. In 2015 he now-famously warned us of a coming pandemic. Since it arrived, he's become one of our most credible voices on the matter. He also became a target of the plague of misinformation afoot in the land. He and I connected in mid-August—remotely, of course—to talk about the new coronavirus.

Gates didn't hide his disappointment in the US for failing both to prepare before a pandemic hit and to adequately test for the SARS-CoV-2 virus after it arrived. But, he said, "we can do the postmortem at some point. We still have a pandemic going on, and we should focus on that."

The Bill and Melinda Gates Foundation has been working on an easy self-test for Covid-19, and when I asked why we still have to wait so long for results, Gates' voice reflected his disgust. "The majority of all US tests are completely garbage, wasted." The insurance reimbursement system, he said, was to blame. "If you don't care how late the date is, and you reimburse at the same level, of course they're going to take every customer. Because they are making ridiculous money." If the federal government would pay "a little bit extra for 24 hours, pay the normal fee for 48 hours, and pay nothing" if test results come later, then the insurance companies would "fix it overnight," he said.

Gates is up against another problem that defies an easy fix: a pervasive anti-science view of the world. "The irony is that it's digital social media that allows this kind of titillating, oversimplistic explanation of, 'OK, there's just an evil person, and that explains all of this.'" He still has faith in the capacity of science and scientists to prevail, however. "You have to admit there's been trillions of dollars of economic damage done, and a lot of deaths," he said. "But the innovation pipeline on scaling up diagnostics, on new therapeutics, on vaccines is quite impressive. And that makes me feel like, for the rich world, we should largely be able to end this thing by the end of 2021, and for the world at large by the end of 2022."

He remains very concerned that the US isn't "showing up" on a crucial point. We have to "be able to tell the vaccine companies to build extra factories for the billions of doses" needed, he said, and ensure "that there is procurement money to buy those for the marginal cost." He'd been "calling everyone" to urge Congress to include, in its Covid bill, $4 billion for the international vaccine alliance GAVI and $4 billion for a global fund for therapeutics. "That's less than 1 percent to the bill," he said. "But in terms of saving lives and getting us back to normal, that under 1 percent is by far the most important thing, if we can get it in there."

When the pandemic hit, it might have seemed implausible that we'd be able to distribute a viable vaccine to the whole world by the end of 2022. But, Gates added, "that is only because of the scale of the innovation that's taking place. Now, whenever we get this done, we will have lost many years in malaria and polio and HIV and the indebtedness of countries of all sizes and instability." But, he continued, "it's because of innovation that you don't have to contemplate an even sadder statement."

You can read our full conversation on WIRED.com.

—Steven Levy is WIRED*'s editor at large*

CDC / Cynthia S. Goldsmith and A. Tamin (virus); Getty Images (all others)

ILLUSTRATION / SAM WHITNEY

Banking in the palm of your hands.

Capital One® checking and savings accounts have no fees or minimums and a top-rated banking app that lets you manage your money anytime, anywhere.

This is Banking Reimagined.®

Capital One®
What's in your wallet?®

P.40 A MORE PERFECT ELECTION

Dana DeBeauvoir
photographed in Austin, Texas

PHOTOGRAPH / SARAH LIM

ELECTRIC WORD

ON THE COVER

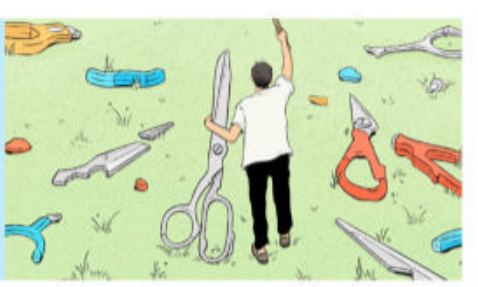
Illustration
by Adrià Fruitós

Behind the Scenes
To perfectly illustrate the complicated issues surrounding the security of US elections, our art team ended up reaching out to ... Europe. Cover illustrator Adrià Fruitós, who is from Spain but is based in Strasbourg, France, also created the art for the opener and two features in the election package. To see it all, head to page 40.

MIND GRENADES

GADGET LAB: SECURITY

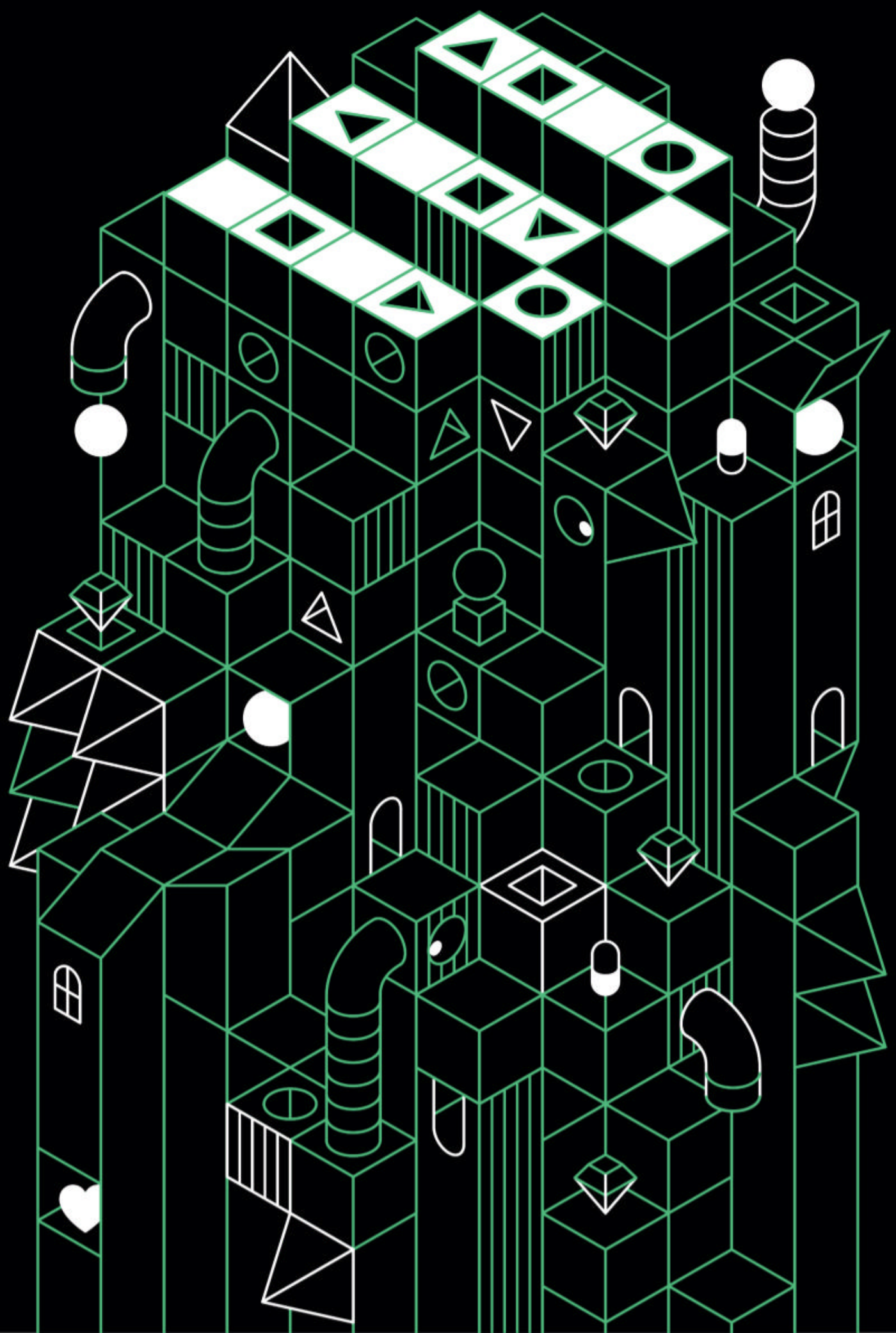
SIX-WORD SCI-FI



Images, from top: Hust Wilson, Suzanne Saroff, Violet Reed

COMING OCTOBER

WIREDGAMES



WHAT THE WORLD NEEDS NOW

The power, and paradox, of bad software.

BY PAUL FORD

When I go to the doctor, they ask what I do, and when I tell them, they start complaining to me about the software at the hospital. I love this, because I hate going to the doctor, and it gives us something to talk about besides my blood pressure. ■ This is a pattern in my life: When I'm asking at the library reference desk, chatting with the construction contractor with her iPad, or applying for a loan at the bank, I just peer over their shoulder a bit while they're answering a question—not so much to be intrusive—and give a low little whistle at the mess on their screens. And out pours a litany of wasted hours and bug reports. Now I've made a friend. ■ Good software makes work easier, but bad software brings us together into a family. I love bad software, which is most of it. Friends text me screenshots of terrible procurement

systems, knowing that I will immediately text back, "BANANACAKES." I'll even watch videos of bad software. There are tons on YouTube, where people demo enterprise resource-planning systems and the like. These videos fill me with a sort of yearning, like when you step inside some old frigate they've turned into a museum.

Best I can tell, the bad software sweepstakes has been won (or lost) by climate change folks. One night I decided to go see what climate models actually are. Turns out they're often massive batch jobs that run on supercomputers and spit out numbers. No buttons to click, no spinny globes or toggle switches. They're artifacts from the deep, mainframe world of computing. When you hear about a climate model predicting awful Earth stuff, they're talking about hundreds of Fortran files, with comments at the top like "The subroutines in this file determine the potential temperature at which seawater freezes." They're not meant to be run by any random nerd on a home computer.

This doesn't mean they're inaccurate. They're very accurate. As code goes, the models are amazing, because they're attempts to understand the entire, actual Earth via programming. All the ocean currents, all the ice and rain, all the soil and light. And if you feel smart, reading a few pages of climate model code will fix you up *tout suite*. If you, too, would like to know exactly how little you know about the machinery of the natural world, go on GitHub and look through the Modular Ocean Model 6, released by the National Oceanic and Atmospheric Administration, which is part of the Department of Commerce. Only America would make the weather report to money.

Every industry or discipline has its signature software. Climate has big batch climate models. Sales has the CRM, hence Salesforce. Doctors have those awful health care records systems; social scientists use SPSS or SAS or R; financial types plug everything into Excel. There are big platforms that help people do all kinds of work. But you know what blows them away? Software for making software. The software industry's software is so, so good (not that people don't complain). Just take a look at the modern IDE (integrated development environment), the programs programmers use to program more programs. The biggest are made by tech giants: Xcode (Apple) and Visual Studio (Microsoft) and Android Studio (Google), for example. I love to mock software, and yeah, these programs are huge and sprawling, but when I open these tools I feel like a medieval stonemason dragged into midtown Manhattan and left to stare at the skyscrapers. My mouth hangs open and my chisel falls from my sandstone-roughened hands.

In an IDE you drag buttons around to make the scaffolding for your apps. You type a few letters and the software guides your hand and finishes your thoughts, showing you functions inside of functions and letting you pick the right one for the task. Ultimately you click a little triangle (like Play on a music player) and it builds the app. I never get over it. And they give it away for free, so that people use it to make more software, which is why all the real estate in New York City is worth around a trillion and a half bucks, and Apple, which takes its famous 30 percent cut in the App Store, is worth $2 trillion. Of course, that's a down payment when you consider what we're going to pay to mitigate climate change.

So the software people get amazing tools that let them build amazing apps, and the climate people get lots of Fortran. This is one of the weirdest puzzles of this industry. We have these tools for making new, wonderful tools, and yet the people who need help the most are using these old tools and methods. A lot of it is due to a very ancient and serious split—between academic programming, which is frequently optimized for doing something novel and publishing a paper about it, and the tech industry, which is, to put it simply, optimized for making lots of money by giving people things they use all the time.

That whole Xerox PARC thing in the 1970s—the thing that supposedly gave us the Mac, etc.—was actually not about having a mouse and windows; the big core idea was that we'd build models of our world in software and adapt them as we explored. Doctors could simulate new treatments; children could simulate rocket ships. We'd all have highly visual pocket climate models we could explore and manipulate, or the doctors would all be programmers themselves and make better patient-management systems. The idea was for software to become the humble servant of every other discipline; no one anticipated that the tech industry would become a global god-king among the industries, expecting every other field to transform itself in tech's image. There's a thing in programming: Code has a way of begetting more code. You start hacking on some problem, and six months later you're still hacking at it, adding features. You write code that helps you write more code. But what we don't do so much, what our tools don't help us do, is continually ask, who is this for, why are we doing it, and how will people build upon it?

The software people get amazing tools that let them build amazing apps, and the climate people get lots of Fortran. This is one of the weirdest puzzles of this industry.

Decisions were made for us, decades ago, and here we are. Best not to dwell on what might have been. Let's look around and learn. What I'm learning as I read that climate code in long pandemic evenings is that the rules of the world are to be discovered and accepted, not changed. It's a hard lesson to learn, when I work in a field with such wonderful, fluid, flexible tools. It feels as if we should be able to hack our way out of this. The next phase of growth for our industry, finally, should be to learn about the world before we try to change it.

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

ILLUSTRATION / ELENA LACEY

I'VE HEARD THIS BEFORE

A YouTube radio archivist blasts me to the past.

BY JASON PARHAM

Then as now, the days heave with smoke and apocalypse, the howl of sirens. ■ I am a child of rebellion. Which is to say, I know something of history's violent fires and how they spread. I came of age in the 1990s, the era of Black prosperity, raised on the belief that if I worked twice as hard, stuck to the rules, I'd survive. ■ But what I saw on TV said otherwise: Rodney King drew breath and was →

Downtown Los Angeles at night

Davey Adesida / Trunk Archive

beaten into blood and pulp; the police who did it walked free.

So this summer, as our present spiraled into our past, I went searching on YouTube for recordings of LA radio programs taped in the spring of '92. I needed a reminder: We were here before, we would make it through again.

I didn't find the riot broadcasts on my mind, tapings from the SoCal radio trinity of my youth: Power 106, 92.3 The Beat, and 102.3 KJLH. What I discovered instead was the channel of Jean-Gabriel Prats, who, since 2015, has been assembling an impressive archive of radio ephemera—a pomade of nostalgia I didn't know I was missing.

Under the moniker Majestik Magic RKO, Prats uploads hard-to-find, mostly forgotten broadcasts from all over the world, typically programs that aired during the 1980s and '90s. He is a hoarder of sounds and places, an Arturo Schomburg for our digital cosmos. There's a bit of everything to chew on. I'm treated to a buffet of crunchy hip hop classics on a November 1, 1996, taping of *The Tim Westwood Rap Show* (BBC Radio One). A succulent two-hour loop of *New York After Dark* with Yvonne Mobley (98.7 Kiss FM) from March 31, 1988, blends brass harmonies and silky R&B hits, including Tower of Power's lover-boy anthem "You're Still a Young Man." Not to be outdone, a 1997 taping of K-Love's afternoon hour (LA's 107.5) is a gushy whirlpool of Spanish romance ballads, from José José to Enrique Iglesias.

As I was listening my way through Prats' archive, I wondered: How do we hold onto the pieces that define us if progress demands an abandonment of what came before? What bits, if any, should we preserve? The only requirement for bona fide, bone-deep change, the kind our world so desperately craves, is that we adapt, that we grow, that we architect new styles of being. At the same time, surely not everything needs to be discarded.

Prats, who is 55, finds "satisfaction in sharing memories," he tells me by email from his home in Soissons, France. For him, restoring snippets of old radio is an act of remembrance, of ushering what *was* into what *is*. Doing so, he says, arises from a need to safeguard those small but precious histories. "It would be a shame if that was lost forever."

Prats grew up surrounded by music; his father collected vinyl, and his mother loved watching variety shows on TV. The sounds were everywhere and eclectic. He counts Jean-Michel Jarre, Run-DMC, and Kate Bush among his favorite artists, along with the film composers Akira Ifukube and Lalo Schifrin. These days, he's a regular on vintage-radio web forums. "This is part of cultural history, just like cinema or television," Prats says. "Companies spend a fortune to protect film or professional videos from time, make restorations, but there's nothing in the world of contemporary radio stations. It's a shame."

For Prats, restoring snippets of old radio is an act of remembrance, of ushering what *was* into what *is*. Doing so, he says, arises from a need to safeguard those small but precious histories.

Getting Prats' broadcasts onto YouTube is a team effort. Some he pulls from Archive.org recordings or scans sent to him by followers. Others he digitizes from old cassettes and tapes, which he saved from a stint working as a disc jockey for a French radio station during the early 1980s. Prats uploads to Mixcloud, too, and a handful of other music-centric platforms.

In 1986, Prats left the radio gig to, he says, "devote myself to a 'real job.'" He hopped from graphic design to network administration to managing an air-charter company. Still, he cherished his time in radio. He was one of the first DJs to introduce Parisians to the American concept of mastermixes, long sets that blend loosely connected genres across one unbroken tract of musical bliss.

With the rise of streaming, radio likewise had to adapt—transitioning fully to internet stations via the likes of Pandora and later SiriusXM. Over time, of course, it was delocalized. Once music streamers took hold by the 2010s, and the grip of Spotify and Apple Music became inescapable, there was no turning back. "Algorithm-driven internet radio," wrote Eric Harvey, a communications professor at Grand Valley State University in Michigan, in 2017, "posits a different route to self-discovery: a cybernetic system that reflects the self back to you through a combination of play and machine learning."

But the self doesn't only exist in the present. In *Uproot: Travels in 21st-Century Music and Digital Culture,* the DJ Jace Clayton writes about an effort in Beirut to digitize early-20th-century Middle Eastern music. The Arab Music Archiving and Research Foundation is a reminder, Clayton suggests, of "how fleeting greatness can be, and how handmade." It must be defended against impermanence, against the compulsion to forget.

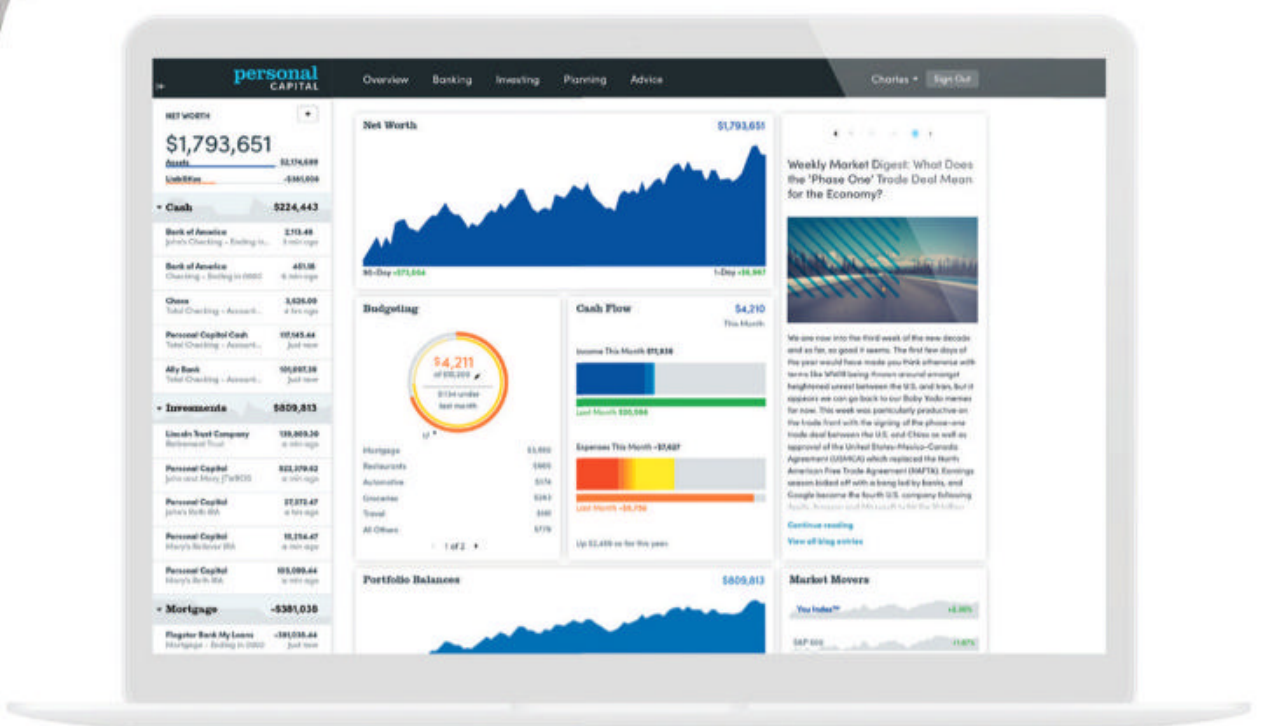
Prats would agree. "What gives me the most pleasure is to know that for a moment, even a very short one, there are listeners who have rediscovered their childhood or adolescent souls," he says. His work functions as a kind of rewind—back, back, back to our earlier selves.

Like most of the world, I'm confined to my immediate surroundings. But with Prats' recordings, I can travel, move across time. The smoke of the past clears a little, and I reach for my younger self. I get lost in a 1996 taping of the "Micky Ficky Mix," and when Tha Dogg Pound's perennial rap cut "Let's Play House" comes on, I crank the volume, louder and louder. It's there, in the muscular bass and rattling production: the sound of home, candy-sweet to the ear. I'm finding delight in the rewind.

JASON PARHAM *(@nonlinearnotes) is a senior writer at* WIRED. *He wrote about TikTok and digital blackface in issue 28.09.*

personal CAPITAL®

Wealth Management
Free Financial Tools



Want a clear view of your finances? Get these free tools.

Personal Capital puts free, professional-grade financial tools at your fingertips. See if you're on track for retirement, saving for your kid's college, or other big life events. Worried about the market? Check to see if you're risk-diversified with our Investment Checkup™ tool.

It's time to take control of your finances.
It's time for Personal Capital.

Get started with your free financial tools or talk to an advisor today at:

personalcapital.com/wired

Download on the App Store | GET IT ON Google Play

FREE FINANCIAL TOOLS AVAILABLE ON WEB & MOBILE

QANON'S GENIUS

The conspiracy theory has the best attributes of a multiplatform game—except it's dangerous and in real life.

BY CLIVE THOMPSON

When QAnon emerged in 2017, the game designer Adrian Hon felt a shock of recognition. ■ QAnon, as you very likely know, is the right-wing conspiracy theory that revolves around a figure named Q. This supposedly high-ranking insider claims that the deep state—an alleged cabal led by Barack Obama, Hillary Clinton, and George Soros and abetted by decadent celebrities—is running a global child-sex-trafficking ring and plotting a left-wing coup. Only Donald Trump heroically stands in the way. ■ It's nonsense, of course. But what intrigued Hon was the style of nonsense. ■ It is addictively participatory. Whenever Q posts about the conspiracy, he (or she or they) leaves clues—"Q drops"—on image boards like 8kun that are cryptic and open-ended. One in 2019, for example, read: "[C] BEFORE [D]. [C]oats BEFORE [D]. The month of AUGUST is traditionally very HOT. You have more than you know." Since the clues are oblique, it's up to the followers of QAnon to interpret them. They instantly begin Googling the phrases, then energetically share their own exegeses online about What It All Means. (August is when Trump will finally imprison Clinton!) To belong to the QAnon pack is to be part of a massive crowdsourcing project that sees itself cracking a mystery. ■ Which is what gave Hon the shock of recognition: QAnon was behaving precisely like an alternate-reality game, or ARG.

ARGs are designed to be clue-cracking, multiplatform scavenger hunts. They're often used as a promotion, like for a movie. A studio plants a cryptic clue in the world around us. If you notice it and Google it, it leads to hundreds more clues that the gamemaker has craftily embedded in various websites, online videos, maps, and even voice message boxes. The first big ARG—called *The Beast*—was created in 2001 to promote the Steven Spielberg movie *A.I. Artificial Intelligence* and began with a reference to a "sentient machine therapist" in the credits listed on the movie poster.

Hon was a student when *The Beast* was released, and he became obsessed. He even moderated a discussion forum where players shared clues. They solved the puzzle in about five months, and Hon was so inspired that he created his own firm to make ARGs, launching *Perplex City* (his most well-known game) in 2005. He's run several others since.

This is why he's convinced that game dynamics help explain why QAnon is such a seductive conspiracy. It plugs into the psychological lures that make ARGs so fun.

First off, QAnon poses a mystery that feels so big it can only be solved by crowdsourcing. It's thrilling to be involved with other people in something bigger than yourself. Plus, it turns one's armchair-warrior Googling into a heroic quest for truth.

"They're all saying, 'I've done my research,'" Hon told me of Q followers. "They're looking for signals in the noise."

There's also the thrill of creativity, of adding to a canon. QAnon followers "don't just passively receive Q drops. They create new videos and texts," notes Marc-André Argentino, a public scholar at Concordia University who researches QAnon. Q's followers behave like religious devotees who pore over their faith's central texts, crafting interpretations that become part of the official creed.

And, like an ARG, QAnon brings social rewards. If you're the first to post a new discovery, "other people can see it, and they instantly recognize it," notes Dan Hon, Adrian's brother, who helped create the *Perplex City* ARG.

In a way, ARGs and QAnon are the quintessence of internet culture. The web has always been about making willy-nilly connections: This links to that which links to this. And cyberspace facilitates the obsessive joint scrutiny of everything, from TV shows to knitting patterns to the belief that reptilians walk among us.

Once you chew on it that way, you start thinking, *jeez, maybe QAnon was almost inevitable*. As the scholar M. R. Sauter has pointed out, the internet is exquisitely suited to the conspiratorial style. "It's the joy of creating connections," Sauter says, noting that previous conspiracy theories have displayed ARG-like qualities too. One was Climategate, where global warming skeptics seized on the leaked emails of atmospheric scientists and produced reams of feverish, unglued analyses.

The web has always been about making willy-nilly connections: This links to that which links to this.

ARG makers have long worried about this culture and its relentless, wild-eyed nature. If players solve one puzzle, they crave the fun of tackling more, more, more. But they can wind up seeing puzzles that aren't puzzles. After the online group solved *The Beast*, one member suggested "solving 9/11." Hon and the other mods quashed that rearguard action. But it showed how easily ARG culture can be hijacked toward delusional ends.

And with QAnon, the appeal has pushed the conspiracy dangerously from the fringes into the mainstream. An internal Facebook review reportedly found millions of people on various QAnon sites, and QAnon believers recently won congressional primary races in Georgia and Florida. All of which suggests that QAnon is, alas, unlikely to fade away soon. Quite apart from its ideological roots, it's fueled by one of the oldest internet urges: It's fun.

CLIVE THOMPSON *(@pomeranian99) is a* WIRED *contributing editor. Write to him at clive@clivethompson.net.*

GHOST ME, FOR HEAVEN'S SAKE

Please don't complain to me about literally anything if you've touched human flesh since March. Being very single, I have not, and my Grubhub guy doesn't want a hug. So I am doomed, instead, to online dating in the context of a pandemic. Let me walk you through the torture. It starts typically enough, with endless scrolling through profiles of now-offensively-irrelevant travel photos. No one asks "How's it going?" anymore; the new opener is "Picked up any new hobbies?" I can't help but respond: "No, unless you count screaming into the void." If they find me cute-funny, we arrange a FaceTime or Zoom, the latter being preferable for its "Touch up my appearance" feature. We talk and misread glitching, pixel-blurred facial cues and, if all goes tolerably, make it to first base (a socially distanced park sit). Goodbyes, whether on a screen or IRL, are harder than ever. "All right ... well ... anyway," someone mumbles, straining to find an excuse, even though—amid mass boredom—there isn't one. Worse still is saying goodbye for good. A week after a third date that fizzled into mutual boredom, I got an "I'm not feeling the spark" text. Same, but, ouch? Another person sent me an unprompted "I'm not looking for a relationship" text four days after our last interaction, in which I did not ask for a relationship. Whatever happened to ghosting? Maybe it used to be "rude" and "detrimental to both parties' mental health" (actual quotes), but that was pre-Covid. I no longer need your attempts at nobility, reminders of a flesh-and-blood humanity made irrelevant by contactless existence. Ghosting is more suitable to the times. It's silent, it's safe, it conforms to the unbearable lightness of our disembodied beings. Besides, look around. It's 2020, and nobody expects a happy ending.

Illustration by Alyssa Walker

ILLUSTRATION / HUST WILSON

BEAUTIFUL AND BUTTERFREE

Players of the alternate-reality game *Pokémon Go* are still at it. They also seem, in these crazy days, to exhibit *well-being*.

BY VIRGINIA HEFFERNAN

In the second half of 2016, two roads diverged in an online wood. Each wound through a universe populated by fabulous creatures. One was delightful. The other was morbid. One knew it was fantasy. The other was deadly serious, and some who ventured there ended up spoiling for civil war, committing violent crimes, and brandishing knives, guns, and bullwhips against their phantoms. ■ The wise and good chose *Pokémon Go*, while the foolish and furious chose what came to be called QAnon. Or maybe it was just an accident. Maybe it didn't matter what kind of person you were before you entered. After you were in, you were in; your reality became significantly augmented, not to say distorted or even obliter-

➜

ILLUSTRATION / AUBREY WILLIAMS

THE ART OF WINE
THE TECHNOLOGY OF PRESERVATION

The LG SIGNATURE Wine Cellar marries form and function, bringing together
Optimal Preservation Technology™ with Multi-Temperature Control to keep Cabernet Sauvignon pleasantly
cool while Champagne is delightfully cold, all wrapped in a sleek Textured Steel™ cabinet.
Welcome to the bold new world of LG SIGNATURE.

THE ART OF ESSENCE
Find yours at **www.LGSIGNATURE.com**

LG SIGNATURE
WINE CELLAR

YOUR VOICE COUNTS

CONDÉ NAST

Scan to register to vote, or head to vote.gov
Please vote on November 3!

ated. And while QAnon is the subject now of much analysis—including in Clive Thompson's column in this issue—*Pokémon Go* deserves a closer look four years after its launch. The global phenomenon never went away. When contrasted with QAnon, *Pokémon Go* suggests that augmented reality games are not intrinsically corrosive. The players exhibit, of all things, a kind of online *well-being*—sociability and outdoorsiness, amusement and irony. While some in other quarters of the internet have gone gravely wrong in their hunt for enchantment online, millions more *Pokémon Go* "trainers," as they're called, have kept their imaginations fired in a world where the endearing virtual monsters are mischievous or mighty or loving but never sadistic—and bear no resemblance to humans in the news. Pokémon also can't die; instead, they cutely swoon.

"I've been a Pokémon fan since I was young, and when they first announced the game I was excited," Bryan Escobar, a Puerto Rican HVAC repairman and apartment porter, told me. When the *Go* version launched in July 2016, he jumped in, playing a handful of times every week. Now he plays for hours daily. "Adding legendary Pokémon to catch by battling them in raids gave the game so much hype. Another sweet addition was when they introduced adding friends and trading Pokémon." With the pandemic, Escobar continued, *PoGo* has introduced new features that improve indoor play, although on his days off he still walks between 6 and 12 miles chasing Pokémon.

Casey Greenfield, a Manhattan lawyer, came to the game later. "I blame or credit a friend who came to New York for a conference in 2018," she told me via email. "I asked if there was anything else she wanted to try to fit in. She said yes: Community Day"—an event that celebrates some of the game's most beloved Pokémon.

"So she took me on an items run and showed me the basics of gym defense. Sunday found me and my son running in frigid rain after floating steel creatures."

How much does she play now, two years later? "If you're playing, it's just there—maybe the way some people refresh their Twitter feeds," she said. "It's not like being in your gamer chair with a portable urinal. I'm not saying it's more glamorous; I'm just saying it's different."

The social internet sometimes seems to exist to slake our thirst for enchantment during our daily rounds. Greenfield's Twitter comparison was apt. There's a reason I tap the blue app a dozen or more times a day; a glance at quips by far-flung oddballs enlivens my routine. Likewise, during the short time I played *PoGo*, the gray sidewalks came to life with all kinds of weird stuff: sentient noses and pineapple lily pads. A walk to Key Food swept me through an invisible tollbooth into a kind of Narnia of *kawaii*. Better yet, no one could tell me from other tired moms.

QAnon devotees similarly relish being in on a secret and slipping around like spies; despite their singular insight into the true workings of the universe, no one can tell them from tired moms either. They, too, are intoxicated by their virtual creatures, including the dastardly ones they call "Tom Hanks" and "Hillary Clinton." Like Pikachu and Butterfree, these cartoons were designed online. Life's mundanity dissolves when you play an alternate-reality game, and everything from broken sidewalks to stifling quarantines can turn into high drama.

But I said two roads diverged. QAnon became a holy war, while *PoGo* remained a game, requiring a willing suspension of disbelief. *That funny little weirdo called Swablu is not really "there," but for now we'll pretend he is.* Most brains learn how to do this as children. We grasp that the world has room for both mice and Mickey Mouse, both the hanzi 鼠 and the brown-gray rodent it represents. Education is meant to cultivate nimbleness with signifier and signified. That facility is literacy itself.

Fortunately, there are more disciplined minds, like Escobar's and Greenfield's, than those who, quixotic about online fantasies, mistake their pocket monsters for reality. *Pokémon Go* has tens of millions, at times some 150 million, monthly players all over the world. By contrast, QAnon's numbers are usually given vaguely as "millions." And while QAnon adherents are notoriously solitary, angry, and furtive, *PoGo* trainers say the game has furnished them with bigger, warmer, more adventurous, more active, and more engaged lives.

"One of the things I like most is all the people I've met," said Nicole Rosen, a Winnipeg linguist who plays the French version of *Pokémon Go*, the better to relish the mind-spinning complexity of Pokémon names, which some in her field study for their "sound symbolism," or "Pokémonastics." (Don't skip that incongruously French *accent aigu* over the *e* in the word *Pokémon*—itself a *wasei-eigo*, or Japanese pseudo-Anglicist portmanteau word, for "pocket monsters.")

"The game started off somewhat solitary and has now become much more social," Rosen went on. On event days, "players all congregate in certain well-known areas and parks. They also added in-game friends and trading, which means people can interact even more. A lot of people seem to have taken it up again since being holed up at home, and the outdoors has been one of the safer places to be."

"It is an almost unendingly generous and considerate community in which people want to see others win," Greenfield said.

Elizabeth Carlen is a PhD candidate in biology who has appeared in the pages of WIRED for her research on pigeon evolution.

Fortunately, there are more disciplined minds, like Escobar's and Greenfield's, than those who, quixotic about online fantasies, mistake their pocket monsters for reality.

Carlen is drawn to *PoGo*—the way Pokémon can be made to "evolve." Some mornings, she sets research code in motion on her computer, then opens the app to catch a Pokémon or look through her Pokédex while the code is running.

"I'm a biologist; I like collecting and organizing things. My Pokédex is like my own little museum of animals I've collected."

Enchantment, taxonomies, off-road adventures, and forensic pleasures: A rough consensus seems to exist that these are the chief components of *Pokémon Go*'s allure. There are surprises to behold, classifications to make, tasks to complete, mysteries to solve. But these qualities also belong to other successful ARGs, including Q. Even if the attraction to magical worlds is not itself destructive, players evidently require discipline to keep their virtual experiences in bounds. What's more, not everyone can play a game, meaning realize they're *playing*, and realize that what they're playing is a game. This may be true, even when the game is as well built and flexible as *Pokémon Go*. Niantic, the game's developer, has several layers of safety reminders in the game, and the game stops if it detects that a player might be driving a car.

With hundreds of millions of players, *PoGo* has still yielded no stories of people shooting up pizza places in search of Snorlax, or launching congressional campaigns to promote Darkrai as the chosen one, or murdering people to end the depredations of Muk and Kabutops. By appealing to what Carlen calls "the problem-solving, hunting-gathering part of our brains" rather than the affronted, bloodthirsty part, *Pokémon Go* is a sophisticated and humane fantasia, and it's gotta be the best AR game that's ever hatched.

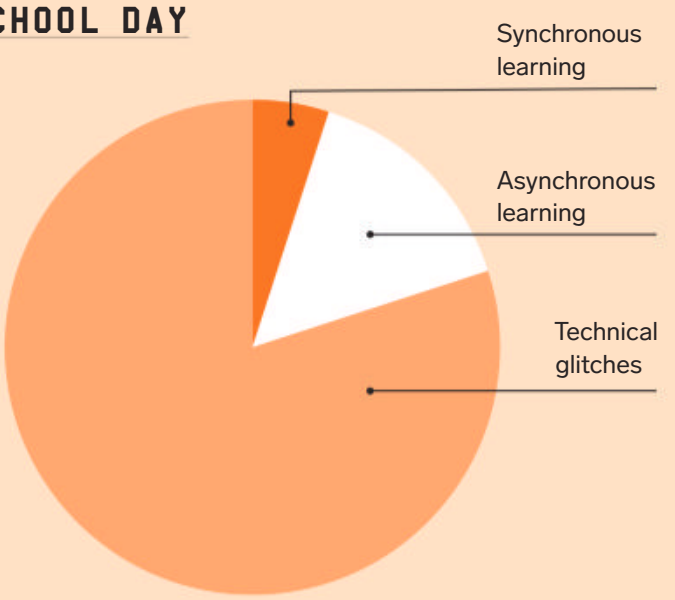
But superlatives, I learned, are for outsiders. When I raved to Greenfield about the perfection of the game, which I took up again while writing this piece, she corrected me. "Fans seem to operate the same way *Simpsons* fans do—it's the best thing ever created, and it's a constant disappointment. 'F*&^ing Niantic' is maybe among the top 50 phrases I hear, at times out of my own mouth. This is probably like other gaming and superfan cultures?"

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

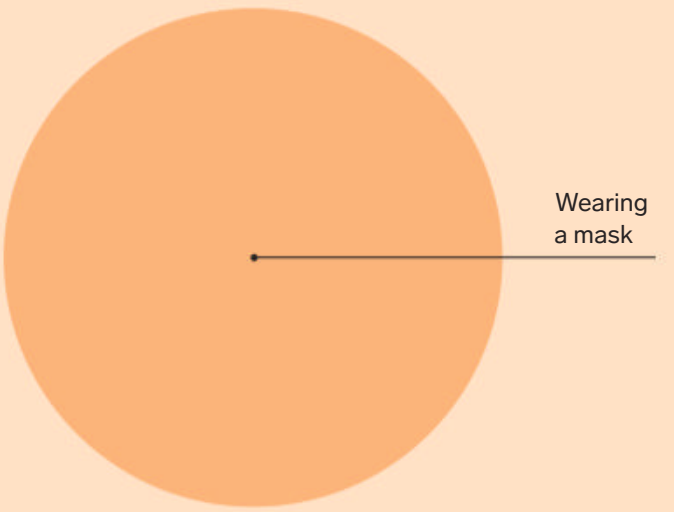
CHARTGEIST

BY JON J. EILENBERG

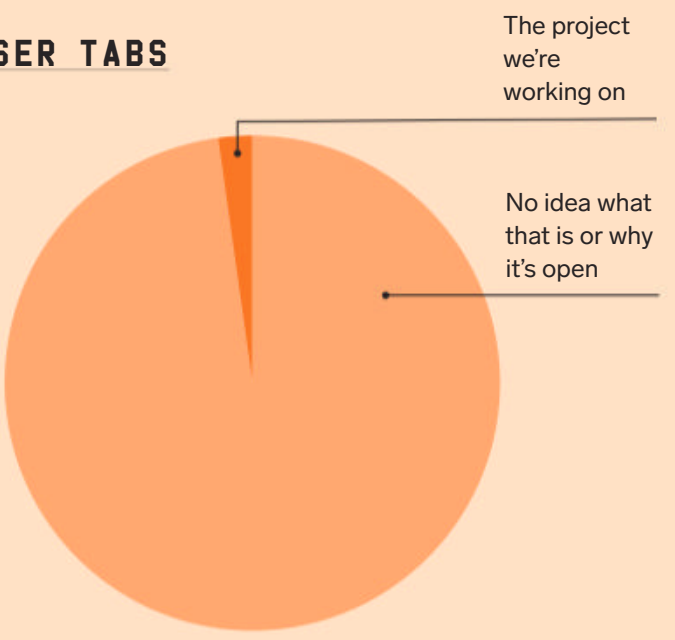
THE NEW SCHOOL DAY



ACCEPTABLE HALLOWEEN ACTIVITIES, 2020



OPEN BROWSER TABS



Use PROTECTION

The world is full of creeps, snoops, and interlopers. We're here with tips and tech to help you shield your home, devices, and digital life from prying eyes.

FETISH

Apple Security Research Device

Yup, it's an iPhone. But it's not just any iPhone. This fall, Apple is shipping a more hackable version of the iPhone to vetted security researchers worldwide. (Whitehats, apply now!) What can experts do with a more permeable iPhone? One of the iPhone operating system's security hallmarks is a design that keeps apps siloed and prevents them from accessing data and other resources they don't need. But these walls create their own security issues, making it more difficult for researchers to trace the path of an attack and find potential vulnerabilities for Apple to fix. Researchers have relied on DIY hacks to sidestep these restrictions for years, but the Security Research Device dissolves the barriers for real. It's a big step, but ever-cautious Apple will only distribute a set number of the phones (no, you can't buy one) and will likely place *some* limitations on how deeply researchers can probe. Why should you care? What the researchers report should make your own iPhone harder to hack. —Lily Hay Newman

FOR MORE EXPERT NEWS, REVIEWS, AND BUYING ADVICE, VISIT WIRED.COM/GEAR

PHOTOGRAPHS / SUZANNE SAROFF

Private EYES

With automated motion-tracking features and sensors that can see in the dark, these are our favorite cameras for monitoring the inside of your home from afar. —Medea Giordano

POWER USER

No Peeking!

How to keep safe from no-goodniks who want to hijack your new camera and peer into your home.

Avoid sketchy brands. Don't just buy some random camera you found on Amazon for cheap. Opt for cameras from well-known companies, or at least ones whose privacy policies are clearly outlined on their website. Going with a proven brand won't make you impervious to hacks, but it's more likely they'll know what to do if one occurs.

Set a strong password and enable two-factor authentication as soon as you create your user account.

Keep it updated. Check frequently for software updates, or set the camera to auto-update.

Turn the camera off whenever you're home. Hackers can't easily attack a device that isn't online.

TOP 3

Arlo Q

The Q is an older model, but this small, relatively affordable camera holds up well against Arlo's new, more complex, and more expensive cameras (many of which require a bulky $150 Smart Hub). The HD camera has night vision and a 130-degree field of view. Two-way audio lets you chirp back at the birds in your window feeder. Video of any motion- or audio-triggered "event" is stored for up to seven days for free—most cameras come with comparable free storage, and the manufacturers are happy to let you upgrade to a paid plan to store footage for longer.

$200

Wyze Cam Pan

Once you try a panning camera, you'll never want to go back to the stationary life. Wyze is my favorite smart-home company because it makes stellar products at a fraction of the cost of its competitors. The Pan camera, our top pick for the budget conscious, is no exception. It swivels horizontally 360 degrees, and the lens has a 93-degree vertical field of view. (Yep, it sees everything.) Program it to monitor four specific areas of a room, or let it detect and follow motion automatically. It's easy to set up and use, and with crisp HD video and two-way audio, you don't just see and hear Huxley meowing, you can speak softly to him and compliment him on his beautiful whiskers as well.

$30

Nest Cam IQ Indoor

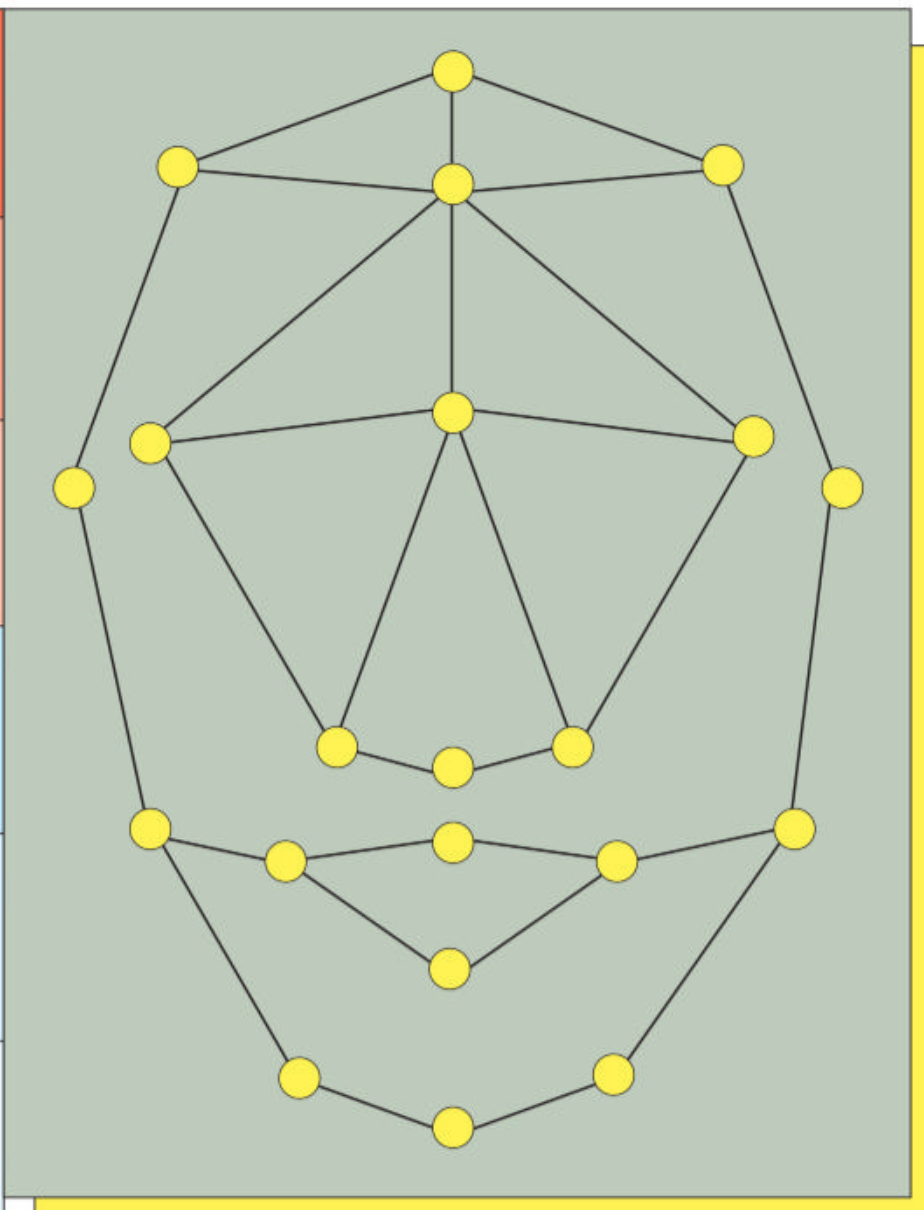
The Gadget Lab team prefers Google Assistant over other voicebots, so we appreciate that Nest's indoor cam fits painlessly into Google's voice ecosystem. The unobtrusive design with a built-in speaker and microphone blends in with your home's decor better than many other cameras. The imaging is top rate: Nest's Supersight feature recognizes humans and tracks them as they walk around the room, and the 4K sensor keeps the image clear when the camera automatically zooms in 12X for a closer look. At night, infrared LEDs give you a bright image of the darkest rooms. This peeper is pricey, so it's best for those who have already invested in other Google Nest hardware.

$299

Camera OBSCURA

Cops, corporations, and citizens alike are surveilling our public spaces with tools like facial recognition and infrared cameras. Whether you're protesting or just stepping out for a boba, you deserve some algorithm-free alone time. —Tom Simonite

HOW TO



MASK UP, BE SAFE

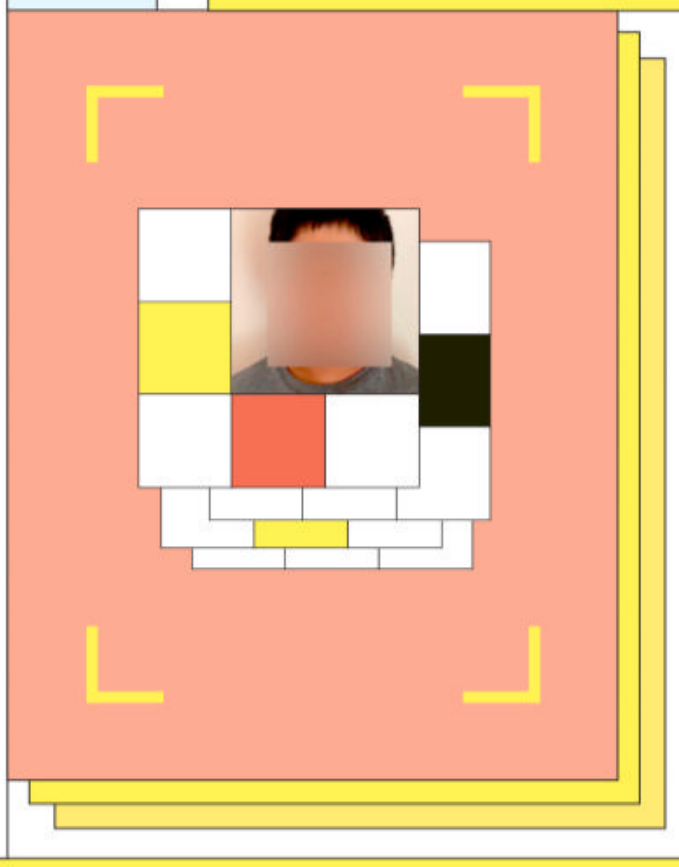
Facial-recognition tech can see around hoodies or big shades, so pair them with a face covering. Plus, you'll get protection against coronavirus particles and tear gas. There are makeup tutorials online for edgy face paint intended to trick face-recognizing algorithms, but these designs are unproven. Also, it's probably easier for humans to track you if you look like a member of Insane Clown Posse.

DRESS TO UNIMPRESS

Make yourself less memorable to both humans and machines by wearing clothing as dark and pattern-free as your commitment to privacy. Clothing search is a common feature of video surveillance software; it helps analysts track a person across different camera feeds. In other words, don't be the only search result for "chartreuse pants." Also, keep the rad tats and Manic Panicked hair hidden.

DELETE THE DEETS

Loose tweets compromise your peeps. Strip metadata like location tags from your phone pics by sharing screenshots of images, not the images themselves. Keep any identifying visual information obscured too. The encrypted messaging app Signal (which you should be using anyway) includes a feature that blurs faces in photos, helping you share in solidarity while foiling face-finding algorithms.



STAY COOL

To live is to radiate thermal energy, making you easily visible to an infrared camera even in a dark forest or urban jungle. Researchers at UC San Diego recently invented a way to potentially mask your heat signature like a thermal chameleon with a device that heats up or cools down to match the temperature of your surroundings. Unfortunately, the current prototype is only the size of a sweatband. Until there's a full-body version, be careful out there.

LOSE YOUR CAR

Logging license plates used to require specialized cameras, but now the software is so cheap that even small police departments and neighborhood associations can afford it. Today, many local and state agencies in the US share what they see via a nationwide database that can track vehicles over long distances. Cycling or walking cuts both your surveillance and ecological footprint.

RUN FACIAL INTERFERENCE

The cover of darkness can be quickly uncovered by flashguns and infrared cameras. Reflectacles' Ghost glasses ($164) shroud your face by bouncing back incoming light to dazzle conventional cameras. And the lenses are opaque to infrared sensors, so—bonus!—they also block facial-recognition systems that use 3D imaging, like the iPhone's Face ID.

WE GET HANDLING SECURITY ISSUES FROM THE SAFETY OF YOUR OWN DESK.

To easily manage devices from anywhere, you need Intel® and IT Orchestration by CDW®.

With the latest devices powered by 10th Gen Intel® Core™ vPro® processors, you get built-in security and remote manageability, all while boosting performance up to 40%. And when those devices are configured by the experts at CDW, you can handle more security issues in less time whether you're at the office or working from home.

CDW.com/BeGreatMakeTheShift

intel | CDW PEOPLE WHO GET IT®

Block PARTY

It's not hard for bad actors to track or hack your phone. But put it inside a Faraday pouch and you can drop off the digital map. —Matt Jancer

THREE LAYERS OF NICKEL- AND COPPER-COATED FABRIC—THE FARADAY CAGE—MEAN STRONGER PROTECTION THAN JUST ONE LAYER.

WEAR AND TEAR ON THE METAL FABRIC WOULD IMPEDE ITS SIGNAL-SQUELCHING ABILITIES; A SOFT LINER PROTECTS IT FROM ABRASION.

A LAYER OF THIN COTTON PADDING HELPS THE LEATHER OR NYLON OUTER SHELL PROTECT THE PHONE AGAINST BUMPS AND DROPS.

SILENT POCKET ALSO SELLS ITS FARADAY FABRIC SEPARATELY ($26 PER SQUARE METER), SO YOU CAN FASHION YOUR OWN DIY POUCH.

COMPONENT

Albert Einstein kept a portrait of the 19th-century scientist Michael Faraday on his wall, alongside a picture of Isaac Newton. Genius recognizes genius: Faraday's many discoveries led to electric motors, to electricity being put to practical use in technology, and to the concept of electromagnetic fields in physics. Faraday also figured out that an enclosure made of a mesh of conductive metal can absorb and redistribute electromagnetic interference. It is this work that's honored every time someone slips a cell phone into a pouch coated with metal, made for the specific purpose of preventing signals from getting in or out. The low-tech hack shields phones from digital buttinskies by blocking cellular signals, Wi-Fi, GPS, NFC, RFID, and Bluetooth. Privacy-craving citizens can put their phone into a Faraday pouch like this one from Silent Pocket ($60 and up), where a metal lining renders the device inside invisible to snoops. "The biggest threat is a law enforcement agency using the signals on your phone to prove you were at a protest or demonstration that they decide later is illegal, and using that information to arrest you," says Cooper Quintin, a security researcher with the Electronic Frontier Foundation, a nonprofit digital rights group. With a Faraday cage, your vanishing act is in the bag.

WEEKEND PROJECT

Inspector GADGET

Boost both your network security and your web browsing speed with this DIY content filter. —Scott Gilbertson

OBJECTIVE

Every device on your network is bombarded 24/7 with malware, banner ads, pop-ups, and activity-tracking scripts. All that extra cruft slows down your browsing. But with a bit of tinkering, you can program a tiny and cheap Raspberry Pi computer to block this noisome dross. Follow these instructions to install the free program Pi-hole, which checks all incoming data against blacklists of your choosing before deciding whether the packets should be passed on to your devices. It's more efficient than a standard ad blocker; the filtering works across every device on your network, banishing ads, trackers, and malicious code from phones, iPads, PCs, game consoles, Rokus, and even smart TVs.

STEP BY STEP

WHAT YOU'LL NEED

→ Raspberry Pi ($35) with the free Raspberry Pi OS software installed
→ Home network router (either the one from your ISP or your own—we like the TP-Link AX6000)
→ Mac or Windows PC for installing and controlling Pi-hole
→ Comfort typing into a command-line interface (nothing too hairy, we promise)

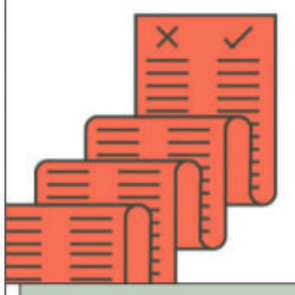
GET THE SOFTWARE

With the Pi and your computer on the same network, open a terminal window (use Terminal on Macs; Command Prompt on Windows) and connect to the Pi using SSH. The secure protocol sends commands from one computer to another; find instructions at Raspberrypi.org to help with this. Next, type the command below to install Pi-hole, selecting the default options and writing down any network info you see:

```
curl -sSL https://install.pi-hole.net | bash
```

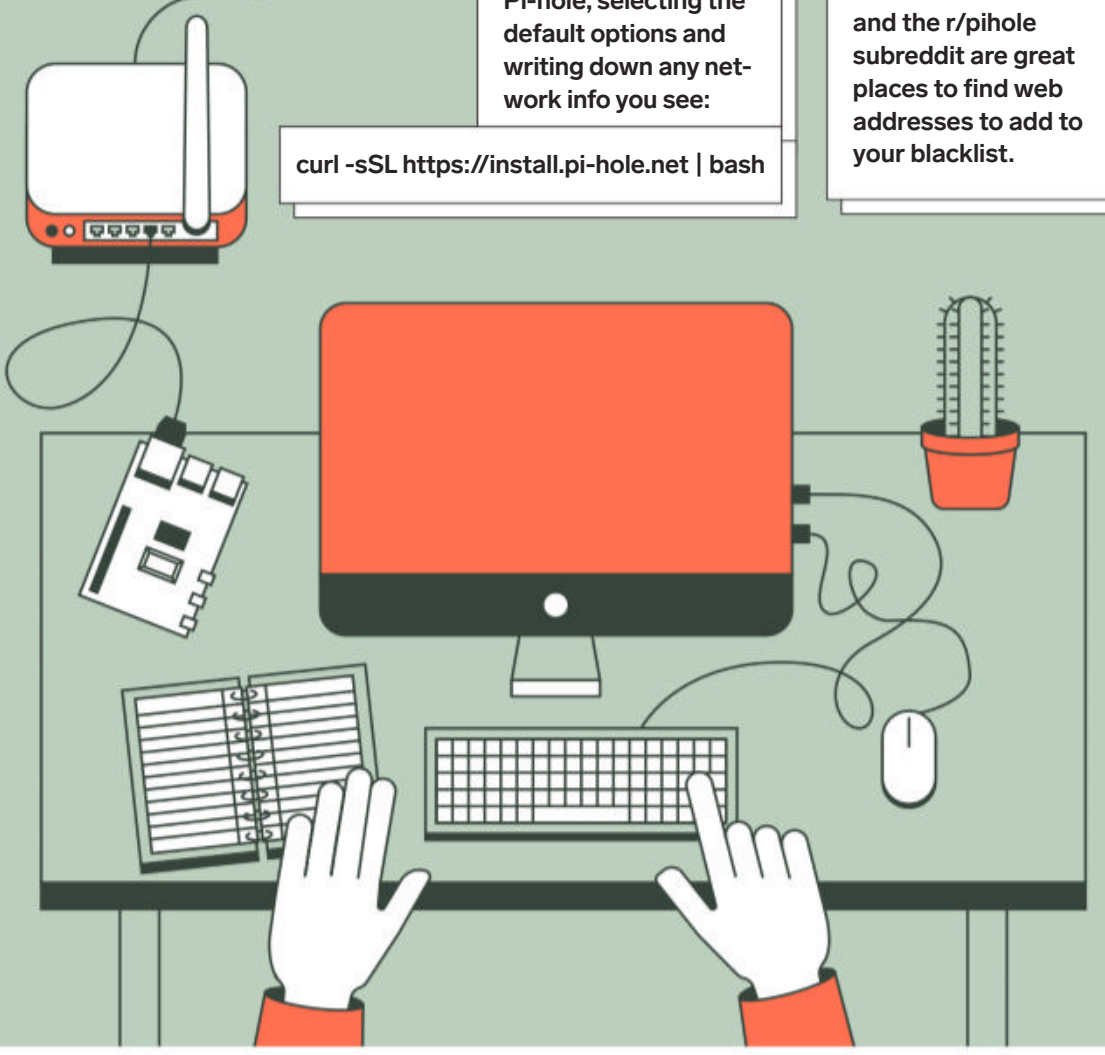
MAKE YOUR LIST

Close the terminal window; we're done with the command line. (See, that wasn't so bad.) Open a web browser and navigate to http://pi.hole. This is where you'll control Pi-hole and decide what to block and what to allow. You'll see some default options to block the most egregious trackers on the internet, but you can always fine-tune things to suit your needs by adding the web addresses where specific services live. Try nuking ads in Twitch or blocking Alexa requests so your kids can't summon pizzas or Ubers. Pi-hole.net and the r/pihole subreddit are great places to find web addresses to add to your blacklist.



REROUTE THE TRAFFIC

Keep your Pi-hole powered on and connected to your network; plug it directly to your router if you can. Now open your router's control panel in a web browser (consult your router's documentation for this part) and look for your network's DHCP/DNS settings for your LAN—not your WAN. In the DNS field, type in the IP address of your Raspberry Pi. (You wrote it down earlier, right?) This will force all inbound data to go through the Pi and get checked against your lists before going out to your devices. Now restart your networked devices one by one; this forces them to reconnect to the internet through the Pi-hole. Want to see how much gunk you're now blocking? Check out the dashboard at pi.hole/admin.



ILLUSTRATIONS / SAM WHITNEY

Here is a list of 25 things Business Communications should be:

1. Straightforward
2. Straightforward
3. Straightforward
4. Straightforward
5. Straightforward
6. Straightforward
7. Straightforward
8. Straightforward
9. Straightforward
10. Straightforward
11. Straightforward
12. Straightforward
13. Straightforward
14. Straightforward
15. Straightforward
16. Straightforward
17. Straightforward
18. Straightforward
19. Straightforward
20. Straightforward
21. Straightforward
22. Straightforward
23. Straightforward
24. Straightforward
25. Straightforward

Now we're talking.

VONAGE

RESEARCH AND REPORTING BY **GRAHAM HACIA**

—

ILLUSTRATIONS BY **MURUGIAH**

—

PORTRAITS BY **JAY RUBEN DAYRIT**

MAKE THINGS BETTER

When Sartre said hell is other people, he wasn't living through 2020. Right now, other people are the only thing between us and species collapse. Not just the people we occasionally encounter behind fugly masks—but the experts and innovators out in the world, leading the way. The 17-year-old hacker building his own coronavirus tracker. The Google AI wonk un-coding machine bias. A former IT guy helping his community thwart surveillance. There are people everywhere, in and out of the spotlight—in tech, science, food, culture, politics—who aren't deterred by disaster. Their wish: To make things better for all of us. Sounds like heaven. –THE EDITORS

TSAI ING-WEN

PRESIDENT, TAIWAN

CHEN CHIEN-JEN

VP (UNTIL MAY 2020), EPIDEMIOLOGIST

AUDREY TANG

DIGITAL MINISTER

A country's first female president, an epidemiologist as her veep, and a transgender digital minister with anarchist beliefs—together, this Taiwanese trio all but eradicated the coronavirus from their homeland. They did so through decisive actions, like early travel bans, strict social distancing measures, and real-time mask-availability apps. The country's true key to success, though, may be the hard lessons learned from the 2003 SARS outbreak (and the ensuing trust their people now have in the country's institutions).

LISA PICCIRILLO

ASSISTANT PROFESSOR, MIT; SOLVER OF THE CONWAY KNOT

Piccirillo untangled the 50-year-old Conway knot in a single week, working on the mathematical challenge in the evening as self-assigned homework. She's now been published in the prestigious *Annals of Mathematics* and has landed a tenure-track position at MIT.

"There's this idea that you have to be super-duper, magically smart to be a mathematician. That's a load of gibberish. Anybody who loves math can be a mathematician. You don't have to be a genius. You don't have to be nerdy."

HER HOBBIES:

- Woodworking
- '70s-era Japanese motorcycles

THEIR FELLOW COVID CONQUERORS:

Anne Hidalgo, mayor, Paris
Kathy Lofy, state health officer, Washington State Department of Health
Jacinda Ardern, prime minister, New Zealand
Sara Cody, public health director, Santa Clara County, California
London Breed, mayor, San Francisco

HER FAVORITE PODCAST:
99% Invisible

ANTHONY FAUCI

DIRECTOR, NATIONAL INSTITUTE OF ALLERGY AND INFECTIOUS DISEASES

Fauci fell for public service through the work of his father, a neighborhood pharmacist who often doubled as a doctor for low-income residents. As director of NIAID since 1984, he's advised six presidents on HIV, Ebola, Zika, and more. His integrity in the face of Covid-19 has made him an icon. In a divided nation, he's also a lightning rod.

"A lot of people think public health is the obstacle. That's incorrect. Public health measures should be a gateway to opening the country safely. The best way to do that is to get control of the outbreak, and the best way to get control of the outbreak is to abide by the guidelines. If everybody took that seriously, we could turn this around."

Fauci has been working 18 hours a day, seven days a week, since the beginning of February.

AL GORE

FOUNDER AND CHAIR, THE CLIMATE REALITY PROJECT

The truth is increasingly inconvenient: The globe is getting hotter, and we're to blame. In 2020, though, Gore is still working to fix it, by funding sustainable companies through the equity firm Generation Investment Management and educating the masses through his nonprofit Climate Reality Project. Among its campaigns: boosting voter registration to elect eco-friendly politicians.

THE NEXT GENERATION OF PUBLIC HEALTH: Kizzmekia Corbett, viral immunologist, NIAID Vaccine Research Center. "Corbett represents what's really good about America, in the sense that we have Black young people, who are in the very early stages of their career, who have been able to team up with experienced investigators and have made major contributions. She's going to be a real role model, as both a woman and as an African American." —Anthony Fauci

Houston Forward Times (Gore quote)

PATRICE PECK

CREATOR, CORONAVIRUS NEWS FOR BLACK FOLKS

In April, Peck launched a weekly newsletter to give the Black community the coronavirus coverage white journalists weren't delivering—quickly accruing nearly 1,000 subscribers in the first month.

MORE FABULOUS CORONA-COMMUNICATORS: **Shardé Davis** and **Joy Melody Woods,** #Blackinthelvory; **Corey Hardin,** lead doctor, Mass General FLARE newsletter; **Bob Wachter,** chair, UCSF Department of Medicine and San Francisco's unofficial Twitter town crier

HER RECOMMENDED TV SHOWS:
- *I May Destroy You*
- *Little America*
- *Ramy*

"We are at a political tipping point, thanks in large part to Greta Thunberg and millions of other young people speaking truth to power. They bring courage and moral clarity to the climate movement."

AVA DUVERNAY

FILMMAKER

DuVernay may be the most relevant director of 2020. Her body of work includes *Selma*, *When They See Us*—about the Central Park Five—and *13th*, her 2016 documentary about mass incarceration. (Viewership of the Netflix doc skyrocketed in the three weeks following George Floyd's murder.) This year she launched the online social justice course Array 101, as well as LEAP, a fund for artists whose work explores police violence.

MORE CULTURAL MASTERMINDS: Misha Green, Janet Mock, Michaela Coel, Nia DaCosta, Lena Waithe, Issa Rae, Beyoncé

TIMNIT GEBRU

TECHNICAL CO-LEAD, GOOGLE'S ETHICAL ARTIFICIAL INTELLIGENCE TEAM; COFOUNDER, BLACK IN AI

In 2016, Gebru was shocked to count only "about five Black people" out of an estimated 5,500 attendees at an AI conference. The following year, she helped organize Black in AI's first annual workshop to bring more diversity to the field. Her research has spotlighted racist algorithms and the ethical quandaries of data-mining projects and AI, arguing in a January 2020 paper that current methods of data collection and annotation for machine learning are rife with biases capable of causing real-world harm.

GEBRU'S HOBBIES:
- Piano
- Staring into space at cafés

"There's a lot of gatekeeping in the tech industry, but the industry needs people from all backgrounds. So don't let that gatekeeping make you feel like this is a thing you cannot do. It's important to find your support systems, find your advocates."

HER RECOMMENDED TV SHOWS:
- *Queen Sono*
- *Ramy*
- *The Wire*

AVI SCHIFFMANN

FOUNDER, NCOV2019.LIVE

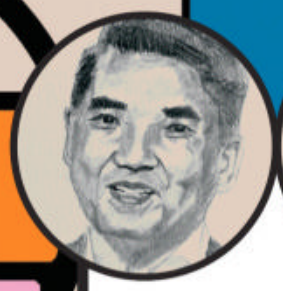
Just 17 years old, Schiffmann thought the government's coronavirus tracking sites "sucked." So he made his own. He has now attracted some 1.7 billion unique visitors and rejected millions of dollars in ads to keep his site bias- and distraction-free.

HE'D LIKE TO MEET:
- Bill Gates
- Tim Berners-Lee

"A lot of people say, 'You're going to be the next Mark Zuckerberg,' but I think that's kind of silly. The next Mark Zuckerberg is not going to make a social network. The next Larry Page is not going to make a search engine. I'm going to make my own unique, really big thing."

HIS OTHER PROJECT:
2020protests, a tracking site for BLM protests

SCHIFFMANN'S RECOMMENDED BOOK:
Factfulness: Ten Reasons We're Wrong About the World—and Why Things Are Better Than You Think, Hans Rosling, Anna Rosling Rönnlund, and Ola Rosling



ERIC YUAN

CEO, ZOOM

SARAH FRIAR

CEO, NEXTDOOR

By last April, well into the pandemic, Zoom's user base had climbed to more than 300 million daily users, and Yuan shifted his platform from servicing boardroom meetings to hosting quarantined book clubs, birthday parties, happy hours, weddings, graduations, and more. Then the "Zoombombing" began, pushing Yuan to mandate meeting passcodes and offer free end-to-end encryption for all users.

Friar, meanwhile, saw Nextdoor's daily users soar 80 percent from February to March, as the pandemic shrank people's daily lives to a few neighborhood blocks. She has now fine-tuned the site to combat misinformation, amplify local Samaritans, and promote small businesses and nonprofits.

FRIAR'S RECOMMENDED BOOKS:
- *Together*, Vivek H. Murthy
- *Biased*, Jennifer L. Eberhardt

VIJAYA GADDE

LEGAL, POLICY, AND TRUST AND SAFETY LEAD, TWITTER

Joining Twitter in 2011, Gadde quickly ascended to the top lawyer spot, where she now overlooks the site's 280-character id. Her latest challenge: counseling the Twitterverse through one of the most boundary-pushing presidential races in US history. This year, the platform started placing misinformation labels on high-profile tweets that it deemed capable of jeopardizing public safety or capsizing the democratic process. One such label was slapped onto President Trump's May 26 post that claimed mail-in voting would lead to widespread fraud.

"Our rules can never be stagnant. They have always had to evolve to new behaviors, new forms of online speech, and the changing world offline. In many ways, what we see on Twitter is a reflection of the challenges within society."

Gadde toyed with the idea of studying archaeology and anthropology in college, until her parents talked her out of it.

RECOMMENDED BOOK:
A Gentleman in Moscow, Amor Towles

HER FELLOW GUARDIAN:
Del Harvey, vice president of trust and safety, Twitter

BEN ADIDA

EXECUTIVE DIRECTOR, VOTINGWORKS

Adida started the nonpartisan, nonprofit VotingWorks in 2018 to ensure that US elections are trustworthy and accessible. It has done so by offering affordable paper-ballot-fed voting machines with voter-verifiable tracking codes and conducting risk-limiting audits. VotingWorks is developing print-at-home mail-in ballots. Plus, all of its software is written with open source code, making it more reliable and secure.

"We all have to believe our elections are working correctly. We all have to believe our judicial system is working correctly. We all have to believe the rules are being followed, and the moment we stop believing in that is the moment we lose democracy."

HIS HOBBIES:
- Baking
- Basketball
- Listening to Taylor Swift with his kids

SARAH COOPER

COMEDIAN

Without penning a single joke, Cooper has lit up TikTok and Twitter with her lip-sync parodies of President Trump. She has won bigly, with a guest-host spot on *Jimmy Kimmel Live* and an upcoming Netflix special called *Everything's Fine*.

JAMES MURDOCH

FOUNDER, LUPA SYSTEMS; EX-CEO, 21ST CENTURY FOX

On July 31, Murdoch resigned from the board of News Corp "due to disagreements over certain editorial content" and "other strategic decisions," severing his last tie to his family's media empire. Long considered the black sheep, he previously used part of his $2 billion stake in the majority sale of Fox to Disney to launch his investment firm, Lupa Systems. Among its goals: finance a more balanced media landscape, purge the internet of disinformation, and support eco-conscious businesses.

MURDOCH'S HOBBY:
Studying the history of Central Asia, "particularly the parts where great empires enter long periods of terminal decline."

ARLAN HAMILTON

FOUNDER, BACKSTAGE CAPITAL

KATIE RAE

CEO, THE ENGINE

Hamilton started the venture firm Backstage Capital while homeless, intent on investing in female, POC, and LGBTQ company founders long ignored by the Silicon Valley boys' club. Read about it in her new book, released in May, *It's About Damn Time*.

In 2016, MIT approached veteran venture capitalist Katie Rae after faculty bemoaned a paucity of funds for startups tackling hard problems that require years of research and development. She has now helped VC firm the Engine raise a $205 million fund for people who are focused on long-term challenges like climate change and world hunger.

"There's been so many times when I've walked into a room, and someone handed me their coat or keys and just assumed I was the help. The next time that happens, I'm taking the car."

–ARLAN HAMILTON

RAE'S HOBBY:
Paddleboarding with her dog, Lulu

HAMILTON'S GUILTY QUARANTINE PLEASURE:
The Titan Games with Dwayne "the Rock" Johnson

ADIDA'S ELECTION TECH COMRADE: **Josh Benaloh,** senior cryptographer, Microsoft Research (see "Lone Star," page 42)

MORE VCS ON A MISSION: **Carmichael Roberts,** cofounder, Material Impact; **Swati Mylavarapu,** cofounder, Incite

GWYNNE SHOTWELL

COO, SPACEX

Shotwell joined SpaceX as its seventh employee in 2002. Today she oversees the 8,000-person aerospace company, which this year scheduled 38 launches, including the *Crew Dragon* on May 30 with two NASA astronauts on board heading for the ISS. That liftoff marked the first time a commercially built spacecraft carried humans into orbit, turning Elon Musk's starry-eyed dreams into headlines. Up next: the moon and Mars.

ISLA MYERS-SMITH

FOUNDER, TEAM SHRUB

Over the past dozen years, Team Shrub has used satellites, drones, and boots on the ground to study the Arctic ice retreat—and flora advance—in the carbon-rich tundra. The group recently started putting AI to work, analyzing the terabytes of data they collected and giving us a glimpse into our precarious future.

HER RECOMMENDED BOOKS:

- *The Curve of Time,* M. Blanchet
- *A Woman in the Polar Night,* Christiane Ritter
- *The Invention of Nature,* Andrea Wulf

"These arctic ecosystems trap a lot of soil carbon, so they're basically like a giant freezer for the planet. And there are projections that, with warming, atmospheric CO_2 could double just from permafrost thaw."

Myers-Smith cofounded Coding Club to teach coding to ecology students. She also plays folk music in the pubs of Edinburgh, Scotland.

DEONIE & STEVE ALLEN

MICROPLASTIC RESEARCHERS, UNIVERSITY OF STRATHCLYDE, GLASGOW

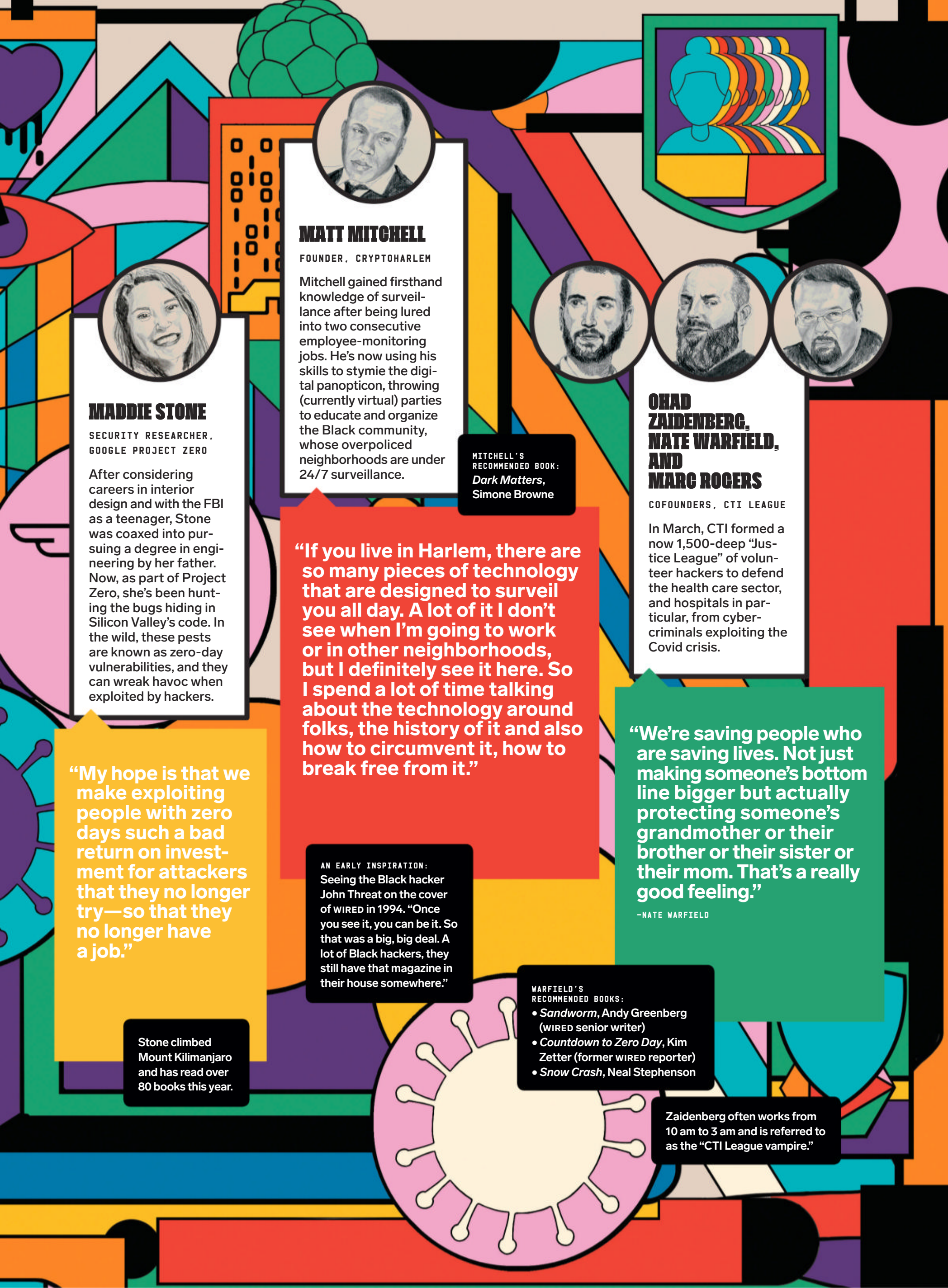
The two discovered microplastic in ocean breezes and over the French Pyrenees—in other words, it's everywhere. The Allens' 2020 mission is to pinpoint the sources and try to halt the spread.

THEIR RECOMMENDED TV SHOW:
BrainDead

"We were expecting to find 1 to 10 particles of plastic per square meter of air, not the 300 and something we found."

–DEONIE ALLEN, ON MICROPLASTICS IN THE PYRENEES

The Allens both paraglide and have lived on a boat for the past two decades, traveling halfway around the world.



MADDIE STONE

SECURITY RESEARCHER, GOOGLE PROJECT ZERO

After considering careers in interior design and with the FBI as a teenager, Stone was coaxed into pursuing a degree in engineering by her father. Now, as part of Project Zero, she's been hunting the bugs hiding in Silicon Valley's code. In the wild, these pests are known as zero-day vulnerabilities, and they can wreak havoc when exploited by hackers.

"My hope is that we make exploiting people with zero days such a bad return on investment for attackers that they no longer try—so that they no longer have a job."

Stone climbed Mount Kilimanjaro and has read over 80 books this year.

MATT MITCHELL

FOUNDER, CRYPTOHARLEM

Mitchell gained firsthand knowledge of surveillance after being lured into two consecutive employee-monitoring jobs. He's now using his skills to stymie the digital panopticon, throwing (currently virtual) parties to educate and organize the Black community, whose overpoliced neighborhoods are under 24/7 surveillance.

MITCHELL'S RECOMMENDED BOOK:
Dark Matters, Simone Browne

"If you live in Harlem, there are so many pieces of technology that are designed to surveil you all day. A lot of it I don't see when I'm going to work or in other neighborhoods, but I definitely see it here. So I spend a lot of time talking about the technology around folks, the history of it and also how to circumvent it, how to break free from it."

AN EARLY INSPIRATION:
Seeing the Black hacker John Threat on the cover of WIRED in 1994. "Once you see it, you can be it. So that was a big, big deal. A lot of Black hackers, they still have that magazine in their house somewhere."

OHAD ZAIDENBERG, NATE WARFIELD, AND MARC ROGERS

COFOUNDERS, CTI LEAGUE

In March, CTI formed a now 1,500-deep "Justice League" of volunteer hackers to defend the health care sector, and hospitals in particular, from cybercriminals exploiting the Covid crisis.

"We're saving people who are saving lives. Not just making someone's bottom line bigger but actually protecting someone's grandmother or their brother or their sister or their mom. That's a really good feeling."

–NATE WARFIELD

WARFIELD'S RECOMMENDED BOOKS:
- *Sandworm*, Andy Greenberg (WIRED senior writer)
- *Countdown to Zero Day*, Kim Zetter (former WIRED reporter)
- *Snow Crash*, Neal Stephenson

Zaidenberg often works from 10 am to 3 am and is referred to as the "CTI League vampire."

RYAN AND BRANDON TSENG

COFOUNDERS, SHIELD AI

After serving seven years as a Navy SEAL, Brandon Tseng approached his entrepreneurial brother Ryan about creating a company that would use AI to save the lives of service members and civilians. Their fully autonomous quadcopter drones are now scouting combat zones overseas—even inside buildings and tunnels—to identify threats for soldiers.

SWIZZ BEATZ AND TIMBALAND

CO-CREATORS, VERZUZ

On March 24, megaproducers Timbaland and Swizz Beatz got a concert-starved nation on its feet when they livestreamed Verzuz's inaugural hip hop and R&B battle to 20,000-plus fans on Instagram. They've now migrated their free face-offs to Apple TV and staged flowdowns like DMX vs. Snoop Dogg, Rick Ross vs. 2 Chainz, and Erykah Badu vs. Jill Scott. But it's about more than just lyrical sparring and beat-backed pugilism—the pair see the series as a sort of museum for Black musicians everywhere.

ARCA

ARTIST AND PRODUCER

Arca's new avant-pop album *KiCk i* (released in June) intercuts bubblegum beats with machine-gun clatter, cyberpunk reggaeton, and Björk crooning Spanish poetry in a bilingual duet. The kinetic stream of sonic shape-shifting mirrors the transgender Venezuelan artist's outspoken reinvention of the 21st-century diva. Or, as she raps on "Nonbinary," "What a treat / It is to be / Nonbinary / Ma chérie / Tee-hee-hee / Bitch."

RECOMMENDED VIDEO GAME:
Sky: Children of the Light

RECOMMENDED MUSICIAN:
Simón Díaz

"I think there should be a company the size of Microsoft or Google committed to the mission of protecting service members and civilians."

–RYAN TSENG

Brandon considered becoming a director when he was young; Ryan often starred in his short films.

"Food enables human connections. It's a powerful vehicle to inspire a change of mindset."

–MASSIMO BOTTURA

QUARANTINE PLEASURES:
RYAN: Growing tomatoes with his wife
BRANDON: pickleball and *Starcraft*

JON GRAY, LESTER WALKER, AND PIERRE SERRAO

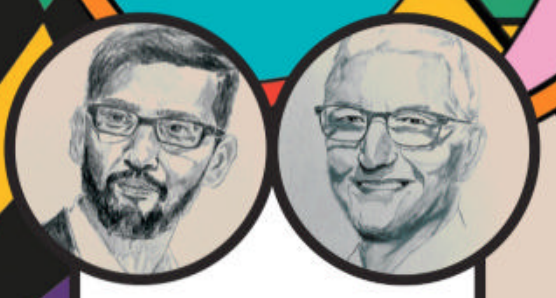
COFOUNDERS, GHETTO GASTRO

In the midst of a pandemic and BLM protests, this Bronx-based collective partnered with La Morada, a local Oaxacan restaurant, and Rethink, a nonprofit that redirects excess food to NYC families. Together, they've served 1,000 meals a day to those in need. Their goal is to keep growing the program, to feed, they say, millions.

Serrao originally considered becoming a pro soccer player or a Chippendales dancer.

"We use food as a weapon to sharpen up our thinking patterns and create a better atmosphere for ourselves and our children and our grandchildren."

–LESTER WALKER



SUNDAR PICHAI

CEO, GOOGLE

TIM COOK

CEO, APPLE

In the wake of the most cataclysmic viral outbreak in over 100 years, tech titans Sundar Pichai and Tim Cook overlooked their rivalry to unite the powers of Google and Apple for the greater good. Their Covid-19 contact tracing API has since been integrated into health care sector apps around the world. The next step: persuade 3 billion smartphone users to opt into the program and share anonymized Bluetooth pings with nearby Androids and iPhones. (Rest easy. Those encrypted pings will self-destruct in 14 days.)

OTHER PROPHETS OF FOOD:
Gabriela Cámara, Cala restaurant, San Francisco
Ron Finley ("The Gangsta Gardener"), Los Angeles
Massimo Bottura, Food for Soul, #kitchenquarantine on Instagram

"We're always struggling as an industry. The margins have been getting smaller and smaller. The only way to get larger margins is to cut costs, and the way society has been cutting costs is by industrializing food, and we know that has greater costs in the long run."

–GABRIELA CÁMARA

PHOTOGRAPH / FARAH AL QASIMI

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.

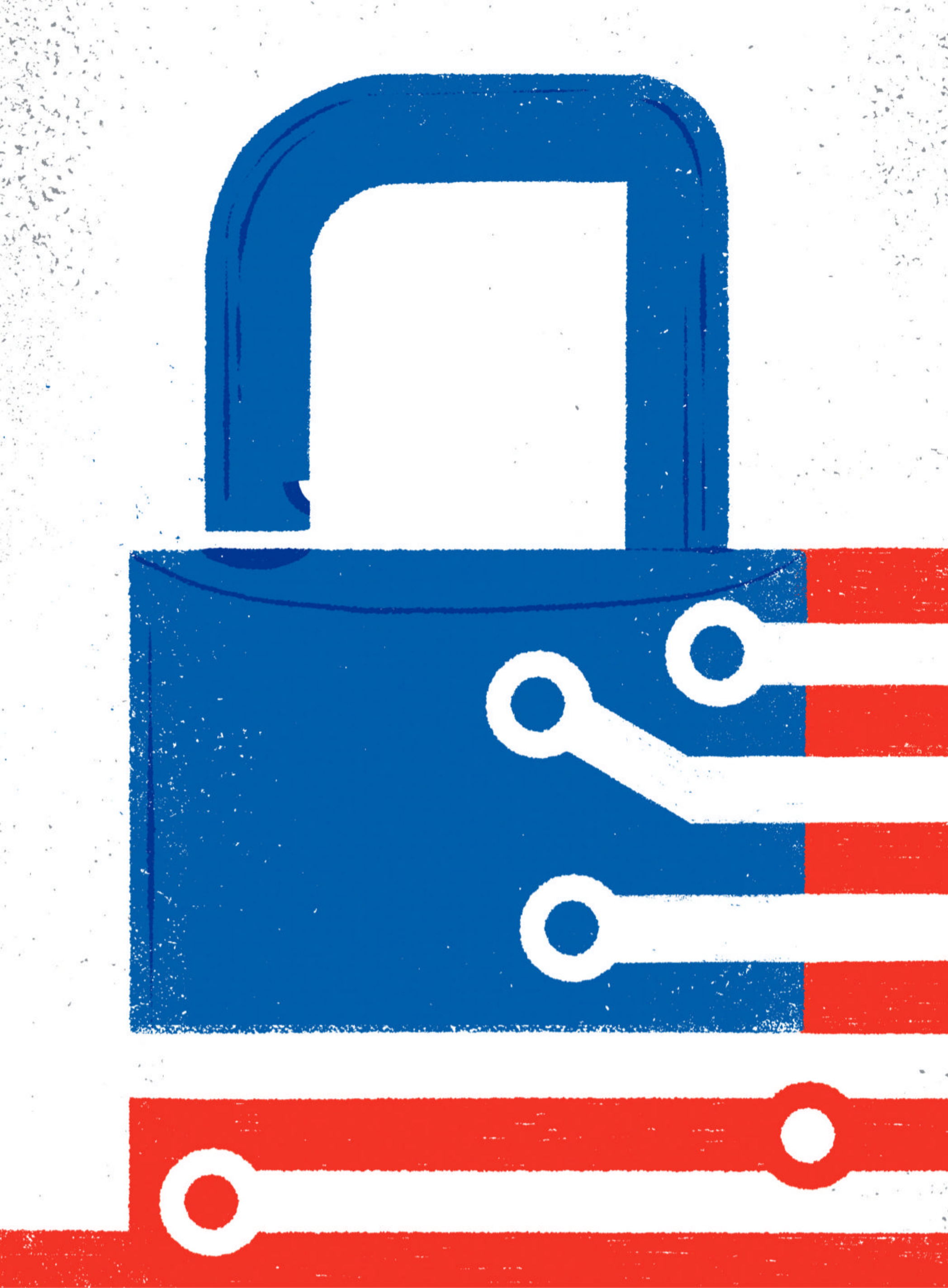
WIRED

Christie Hemm Klok

A MORE PERFECT ELECTION

Fraud-proof. Suppression-proof. Hacker-proof. Doubt-proof. Across the country, people are working hard to reboot the American voting system.

ILLUSTRATION BY ADRIÀ FRUITÓS



How one TEXAS county clerk set off the biggest, weirdest, and most promising REVOLUTION in American voting technology since the 1800s.

LONE STAR

BY BENJAMIN WOFFORD

PHOTOGRAPH BY SARAH LIM

It was not the first time Dana DeBeauvoir had moved a room full of men. At 9 o'clock in the morning on August 8, 2011, she adjusted a pair of half-frame reading glasses on the end of her nose, got up behind a tabletop podium in a downtown San Francisco hotel, and set out to enlist some of her most bitter adversaries in a dare. "I really appreciate the opportunity to visit with you today," she began in a warm tone of Southern geniality, flashing a wide, radiant smile.

DeBeauvoir (pronounced *day-buv-WAH*) introduced herself as the chief clerk and election administrator of Travis County, Texas, better known as the home of Austin. She was dressed in a dark tailored jacket and ruffled blouse, with nails polished in her favorite candy-apple red. Gazing back at her was an audience of academics, computer scientists, and hacktivists, whose collective occupation was warning the American people that the country's election technology was dangerously vulnerable. Most of them slouched around banquet tables in the programmer's uniform of mussed hair, rounded paunches, and untucked shirts. They were assembled for one of the nation's preeminent conferences on election technology, and DeBeauvoir—who had a fairly average grasp of computers—was the event's unlikely keynote speaker.

Trying to break the ice, she stammered through a yuk-yuk computer joke that strung together references to Python and CherryPy 3.2.0. It was greeted with scattered snickers. Then she cut the air by acknowledging what everyone already knew: "There's some unpleasantness here."

The room had been bracing for this. For the past 10 years, county election officials like DeBeauvoir and cybersecurity experts like those in the audience had been mired in opposing trenches. The "unpleasantness" began in 2002, when the lingering debacle of Florida's butterfly ballots prompted Congress to authorize billions of dollars for states to buy new digital voting machines. Among the most popular were devices known as DREs,


VOTE

direct-recording electronic voting machines. No sooner had they been taken out of the box, however, than a wave of computer scientists appeared over the hill like a guerrilla infantry. They assailed the machines' embarrassing security flaws and excoriated the technology vendors who built them.

But it was the nation's election administrators—the 10,000 or so secretaries of state, county clerks, and township presidents who actually ran the country's elections—who ended up taking all the heat. When local voters skimmed an incendiary op-ed that claimed the governor's race could be hacked, they didn't complain to the obscure manufacturers that virtually monopolize American voting; they called on their clerks, upset and confused. If for nothing but to quell mass panic, many election clerks had by the mid-2000s firmly locked arms with one another, pounding the same adamant message: They told voters to ignore the scientists, whom they portrayed as reckless doomsayers, and insisted that their machines were secure.

Many knew that wasn't true, but that was beside the point. From then on, the two sides eyed each other spitefully. The computer scientists took potshots from tech conferences and C-SPAN; the clerks hurled guff from local papers and town halls. The academics showed a hacker's flair for theatrics. They dug up voting machines whose encryption codes were "abcde," and they cooked up malware that forced DREs to run *Pac-Man* or swing elections for Benedict Arnold. One professor and his grad students hacked the real-life voting system of Washington, DC—forcing the machines' auxiliary speakers to blast a school fight song and changing the ballot choices to "Bender" and "Hal 9000."

One of the earliest stuntmen was a Texas professor named Dan Wallach. In 2001 he was called to testify about electronic voting machines before the city council in Houston, where he taught computer science at Rice University. During his testimony, Wallach stood up, crossed the hearing room, and opened a voting machine's hatch, pulling out its PCMCIA memory card. "This is where the votes are," he said, waving the card while cameras clicked. "This can be attacked."

Soon Wallach was accepting invitations to speak all across Texas, often leaving a trail of angry election officials fuming in his dust cloud. It was inevitable that he would eventually lock antlers with one of the most powerful clerks in Texas: Dana DeBeauvoir.

DeBeauvoir had been one of the first clerks in the country to adopt DREs, outfitting Travis County with a model called the Hart eSlate. Soon, she and Wallach were going to war in the pages of *The Austin Chronicle*. Wallach lambasted the voting machine manufacturers for keeping their code secret instead of going open source. "The bad guys can tear it apart," he told the paper. DeBeauvoir responded with measured reassurance but had sharp words for Wallach and his ilk. She told the paper that she was bending over backward to secure the machines—all for "appeasing a worry that is a little dubious." She torched Wallach's rhetoric as "awful" and "unfair" and later called him "a rock-thrower."

By 2011 this history was well known to everyone assembled in the conference room of the San Francisco Westin—where Wallach himself sat in the audience, watching DeBeauvoir from a distance.

Onstage, DeBeauvoir found her bearings and then turned up the heat. She wanted the computer scientists to know what the past decade had been like for *her*. She was tired of seeing clerks "vilified by electronic voting critics who made broad sweeping statements"—attacks that denigrated not just machines but "the people who administered them." Every year the broadsides continued, "without any advice to those of us who are in the field." She accused the academics of doing little to quell the conspiracy theories their research tended to spawn, meaning that "academic papers and internet rumors were often given equal weight in the public discourse." All this while she toiled endlessly just to convince citizens and politicians that elections were fair.

DeBeauvoir was practically seething, and the audience shifted nervously. Then, out of nowhere, she changed tack. Lately, DeBeauvoir confessed, she'd begun to see things from their perspective. Once upon a time, the specter of malware and advanced persistent threats felt "like science fiction." Now she'd come to understand that the scientists had felt ignored as much as she had. For the first time, a room of computer experts heard sounds of real sympathy from the mouth of an elections official. "For you, I imagine it felt—as we would say in Texas—*like hollerin' down a well,*" DeBeauvoir said. Today, she wanted the scientists to know "how much this country needs your wisdom, your knowledge of science"—and help.

She had come to the conference with one purpose: to invite the computer scientists to design a new voting system entirely from scratch. It would have a paper trail, an easy-to-use interface, and the greatest security conceivable. And, she declared, "The. Source. Code. Must. Be. Open."

By now, the attendees were frozen in stunned silence. One later recalled it was all he could do not to fall off his chair. It was as if someone from the IRA had breezed through the door and casually declared peace in Northern Ireland. But DeBeauvoir was in earnest. "The finding of a problem also comes with the obligation to help find a solution," she chided them. "May I suggest to you: Now is the time when you can put your mark on the future," she declared. "And you can use Travis County to make that mark."

DeBeauvoir had started her speech as a visitor from a hostile tribe. She ended it to fervent applause. When she opened the floor to questions, people rushed to the microphone. One was a computer scientist named Josh Benaloh, who was so excited he began brainstorming on the spot. "There are some other methods that might provide even greater assurance," he said cryptically. "I'd love to talk to you about it."

She pointed to another hand that shot up and realized it belonged to Dan Wallach. "I've been involved in Texas politics for long enough now to know that change in Austin doesn't happen easily," Wallach said dryly. "How are you gonna pull this off?"

"I might not!" DeBeauvoir shot back, to nervous laughter. But she felt obligated to try. Since *Bush v. Gore*, voting technology had barely improved in the richest country on earth. Over the previous decade, while civil servants and computer scientists had been at each other's throats, the vendors had been content to keep churning out the

PHOTOGRAPH / SARAH LIM

same mediocre and overpriced equipment. "Ten years!" she said. "And what's changed?"

She'd been raised in the Lone Star philosophy of asking forgiveness, not permission: "Ignore the obstacles, screw the rules, go get something better." The crowd of PhDs was studying her skeptically, and DeBeauvoir stared right back. "I'm an Austinite," she said flatly. "We're an odd mix of dreamers and realists. And if the establishment says it can't be done—well, you can bet that's the *one thing* we're gonna be hell bent to go do."

Dana DeBeauvoir was born in Fort Worth and grew up in nearby Arlington, the oldest of four siblings. In school, teachers lauded the plucky kid with good grades. They also noticed a precocious tendency to shout down bullies and shoo them away from prey. That was the only sign something might be wrong. As DeBeauvoir reflects, "I guess I was a good actress."

The truth was, DeBeauvoir was trapped in a nightmare. Since the age of 9, a dark cloud of sexual abuse at the hands of an adult had hung over her childhood. "There was no help." She understood nothing would be done, nothing could be done—"except to plan my escape," she says. "Which I did."

At 18, DeBeauvoir set out on her own. She worked in an orthodontist's office, ravenous to attend college. Later, her therapists would suggest that her intelligence was a key factor in her ability to survive the trauma of her upbringing. Another was that, even as a child, DeBeauvoir had little trouble recognizing that it was the adults in her life who were morally wrong, not her—a realization that placed her in a tiny minority of child victims. The experience "made for a lousy childhood," she says. It also made for an exceptionally clear-eyed adult. DeBeauvoir worked herself to the bone, attending the University of Texas at Arlington three years after leaving home. As she put it, "Education was my ticket out of abuse."

By then, her acute sense of injustice had pushed her toward public service. In 1979 she arrived at the LBJ School of Public Affairs, one of the premier policy schools in the country. For the first time, DeBeauvoir had found her people: puzzle solvers and brilliant pragmatists, students who'd otherwise fetch a killing in the private sector but who dreamed of a life in public service. Her professors included New Deal visionaries like Wilbur Cohen, "the man who built Medicare," as well as the little-recognized postmaster general who instituted the zip code system.

After graduating, she took a job in Austin, working for the local tax assessor. But soon her boss encouraged her to run for office. She won her first election, and in 1987 became the clerk of Travis County at age 32. "I was very green to politics," she says. "I didn't know anything, really." But she had faith in the power of competence. "That would be the inscription on my tombstone—'Be competent,'" DeBeauvoir laughs. "Either that or 'She ate life with a big spoon.'"

As the clerk of the state's fourth-largest city, DeBeauvoir had to manage a sprawling bureaucracy: property deeds, marriage licenses, and—this being Texas—steer branding. She also had to hold her own in the male-dominated world of Texas politics, "a boots and bellies convention," as she puts it dryly. What she lacked in managerial experience she far exceeded with heart-melting charm and a bottomless patience for details. In her private life, she was drawn to tinkerers and engineers. In Austin she fell deeply in love with a man named Ben Smithers, an Eagle Scout who raced sailboats, cycled competitively, played several instruments, and built airplanes by hand. They were married on her grandmother's birthday, to honor the only person DeBeauvoir could trust during years of abuse.

DAN WALLACH
Computer scientist, Rice University

But the part of DeBeauvoir's job she was least prepared for was the one she'd have to tackle first: running Austin's elections. She'd volunteered in one election before she took office to see how the "back of the house" worked. But the LBJ School had skipped over the subject entirely. And she would have to learn fast. The first election was less than six months away—just one in the parade of school board votes, township primaries, and Supreme Court contests that make running an elections office a year-round job. "Just thrown into the job!" she says. And her experience was far from unusual. "For a hundred and fifty years, the way we brought up our elections officials has always been trial by fire," she says. "We kind of fall into it."

During that same spring of 1987, while the new Travis County clerk was deciphering election law in Texas, a young mathematician 1,500 miles away at Yale University was submitting a doctoral dissertation that would eventually change the course of DeBeauvoir's life. The paper was called "Verifiable Secret-Ballot Elections," and its author was Josh Benaloh, then a 28-year-old grad student. Because of new techniques in cryptography, it began, mathematicians could now perform "tasks that seem to defy intuition." Those techniques, he wrote, made it theoretically possible to construct an election in which everyone's ballot could remain completely secret, while, at the same time, the record of everyone's vote could be "verifiable by all participants"—like a rabbit that's pulled out of a magician's hat and stays hidden inside it at the same time.

Back then, the field of modern cryptography was still young. Encryption had been around since forever—from the ancient Greeks of the Peloponnesian War to the rotor ciphers of World War I. But with the advent of public key cryptography in the 1970s, life as we knew it changed. It would allow ordinary people, not just governments, to cheaply encrypt and authenticate messages between parties; transactions as varied as bank transfers and exchanges between journalists and sources could all be shielded from prying eyes.

The most famous method of public key cryptography was called RSA—after its founders, Ron Rivest, Adi Shamir, and Leonard Adleman—which was first described by its authors to *Scientific American* in 1977. Benaloh was a freshman at MIT when he happened to read that first article at an optometry appointment. The child of activist parents, Benaloh had prodigious gifts in math that were matched by an abiding interest in politics. (As a kid, he spent time in a campaign office for the feminist Bella Abzug.) At MIT in 1981, he signed up for a class on cryptography taught by Rivest. And it was there that Benaloh first began toying with the idea of marrying encryption with electronic voting.

To grasp why this prospect is both so tantalizing and so devilishly challenging, it helps to remember that there are many different kinds of voting. One of them is the method that the House of Representatives has used to pass legislation since the early 1970s. Inside the Capitol, members of Congress cast their votes on a custom-designed machine by inserting a special ID card. When their name appears onscreen, they can choose Yea, Nay, or Present. Then they remove their ID card, *et voilà*—democracy.

As hardware and software go, the machines that tally Congress' votes are the opposite of secure; hacking them would be child's play. So why don't the North Koreans tamper with congressional votes? Because of what hangs above the balcony on the chamber's south wall: a giant electronic display board, the world's most boring jumbotron, where votes are displayed next to every member's name. A congressperson whose vote was hacked need only lift their eyes to catch the mistake, raise a hackle, and correct the problem.

Believe it or not, American public elections operated in much the same way until the late 1800s. They took place in mass public gatherings—not private deliberations of conscience, but large and boisterous affairs. Often, farmers or laborers chose between rival candidates' crowds as a poll clerk counted heads, and onlookers cheered and hissed. If voting still worked this way, running a trustworthy election would be a cakewalk. "It would be easy," says Ben Adida, another acolyte of Rivest who has worked on cryptographic voting. "You'd still use computers. But trusting them would be simple. You could just put up a big spreadsheet of how everyone voted."

The reason we can't is maddeningly simple: the secret ballot. By the late 1800s, vote selling and coercion had become so rampant in electoral politics that reformers stepped in. The secret ballot, appropriated from Australia, became their main weapon against corruption and graft. If Bob's ballot must be anonymous, then he can't be bullied or bribed into voting for Alice's candidate—because Alice can't check to make sure Bob followed through on the bargain.

The moment your vote is cast, it becomes dissociated from you, vanishing into a stream of ballots.

This system of secret ballots had a profound consequence, however: If a voter can never share their ballot, they can never verify it either. The moment your vote is cast, it becomes dissociated from you, indistinguishable from the others in a stream of paper. You can never know if your vote was counted, or counted accurately—whether your ballot sailed through, got jammed in the machine, or was abandoned in a lobby with a sack full of other votes (as happened in Connecticut in 2010).

In short, modern elections enshrine privacy at the cost of transparency, and try to compensate for the loss with a host of bureaucratic patches: voter-registration schemes to prevent people from voting twice, tally systems that ensure the number of voters matches the ballot total, and centralized polling places where rival election monitors can scrutinize the proceedings, all to impart legitimacy to a system of vanishing ballots. "If you want to understand why elections are hard, it's because of the secret ballot," says Adida—that's the single variable "that introduces all of the operational complexity and trust." Not for nothing did a leading technology conference recently declare voting the "hardest problem in IT security."

At MIT, Rivest tossed a paper onto Benaloh's desk that contained a clue to how that problem might be cracked. Mathematicians had noticed something funny about the structure of RSA encryption, which Rivest suspected might have beneficial uses. When a piece of text is digitized, it's rendered into a series of 1s and 0s; and when it's encrypted, those underlying 1s and 0s are transformed, through multiplication with a very large, randomly generated prime number, into what's called a ciphertext. What the mathematicians had understood was that when two ciphertexts are added or multiplied together, the result maintains a stable mathematical relationship with the original, unencrypted "plaintexts"—a relationship called a homomorphism. Say you wanted to add 2 + 4. This homomorphic principle allowed you to encrypt those two numbers, then add them together without decrypting them, and the sum would be an encryption of the number 6.

Benaloh's curiosity was set ablaze; he quickly understood that homomorphic cryptography, as it came to be called, had a perfect use case: voting in elections. On its face, traditional cryptography would seem pretty useless in an election, given that encrypting a vote is like sticking it inside a lockbox. How do you tally votes trapped inside a sea of lockboxes, which can't be opened and can't be seen? But an election, of course, is most fundamentally a process of counting votes—of *adding things together*. Homomorphic encryption made it possible to tally a set of votes even though they were encrypted. And at the same time, it unlocked a host of other benefits.

In 1987, Benaloh's thesis at Yale spelled out how a homomorphically encrypted voting scheme would come to life. First, voters would need access to a machine that could perform advanced cryptography. When they cast their ballot, each digital vote would start out as a simple binary—1 for Biden, 0 for Trump—but its ciphertext might be thousands of characters long. Rather than send voters home with a binder full of hexadecimal gibberish, the computer would print the ciphertext as something much smaller: a hash code, much like how a URL is shortened into a Bit.ly. That would serve as the voter's unique receipt, which they would keep and carry away with them.

At the end of the night, when the computers stopped whirring, all those encrypted votes would be added together. A small number of election officials—the county clerk, the secretary of state—would possess a key that allowed them to decrypt the sum. They'd compare the columns of votes for each candidate and reveal the winner.

Thanks to the nature of the math involved, those resulting sums would also be verifiable by independent outside observers. After the election, all the encrypted votes could be posted on a public, online bulletin board for all to inspect. Using a set of mathematical operations called Chaum-Pedersen protocols, auditors would be able to crunch all those ciphertexts to arrive at what cryptographers call a non-interactive zero-knowledge proof: "Proof that the vote is correctly captured," Benaloh explained, but without any way to know whose ballot said what.

But the thing that excited Benaloh most was what this scheme would mean for individual voters. When a voter left the polling place, clutching a receipt that bore their unique hash code, they could go home and perform a search for its twin among all the encrypted ballots on that massive public bulletin board. For the first time, elections would not only be verifiable, but people could be certain whether their specific vote had been counted, all without violating the secret ballot.

Crucially, Benaloh was not setting out to design an "unhackable" voting machine, an idea he regarded as a chimera. "We don't know how to build bug-free code," he says. Instead, what homomorphic cryptography offered was a beguiling twist on the congressional jumbotron. While the Russians or Chinese might wish to hack such a system, little would be achieved in the effort: In a network whose votes are rendered as gibberish, how could you know whose votes you stole? Moreover, should Fancy Bear attempt to delete 30,000 ballots in Milwaukee, the verifiability protocols meant they would be caught, probably minutes into the act—a downstream effect of giving voters a receipt to track their ballot from home. "The whole notion of end-to-end verifiability is not to say that a system can't be attacked," says Benaloh. "Rather than 'prevention,' it's all about *detection*."

His paper, he says, was "just a small step" in the broad scheme of cryptography. But that step contained the kernel of a radical notion. Since RSA, nearly every aspect of life had become verifiable, from the groceries we bought on our credit card to the suspicious-looking stereo we didn't. It seemed odd to Benaloh how few people had thought the same way about voting—what seemed to him like an act of public faith, when it should be a process of verifiable math. In 1994, Benaloh went to work for Microsoft, where he put his voting proposal on the shelf. But for the next 15 years, he never stopped evangelizing about homomorphic cryptography to any person who would listen.

One of them was Dan Wallach, whose crusade against unsafe voting machines was already underway. In 2007, Benaloh and Wallach discovered they were both at the same technology conference—convened in a sprawling castle near the Germany–Luxembourg border. On a forest hike, Benaloh relentlessly pressed his idea for more than an hour, just long enough for Wallach to get his head around the concept.

By then, Wallach had been involved in some of the most damning research on DREs, including a major investigation by the state of California. He was fixated on preventing malware from getting in. He had never considered a voting system that, by its nature, wasn't worth hacking in the first place. "That," Wallach says, "was the turning point." He became a convert. With his grad students, Wallach even built an experimental system called VoteBox, a bubble-gum-and-band-aid project that replicated the homomorphic approach.

DeBeauvoir knew none of this history when she turned up in San Francisco in 2011. When she extended her hand from

the podium, beseeching the room's technologists to build a new system, Wallach and Benaloh locked eyes from across the room. "*Are you punking me*?" Wallach recalls thinking. In the laggardly world of elections, he says, "this just never happens."

The truth was, DeBeauvoir had no interest in reinventing elections. She was simply tired of feeling trapped by bad technology. "I got angry," she says. "The election vendors pissed me off." So did the math professors, "wasting all that brainpower." She had no clue a system like Benaloh's was even conceivable. But she sensed that her predicament was unconscionable: Google was busy building self-driving cars. How was it that our voting technology was routinely hacked by grad students?

A week later, DeBeauvoir called Wallach. Would he lead the design for a new kind of voting system? Wallach agreed on one condition, which he put in the form of a question. "Can I bring some friends?"

While news about the project spread in the elections world, Wallach started to assemble a posse. Exactly what they would be building, no one was quite sure. But the goals of the design were laid out early—a voting machine that would be *secure*, *transparent*, *auditable*, and *reliable*. They called it STAR-Vote.

The team that Wallach put together was like a fantasy sports roster of election security luminaries. Benaloh, still at Microsoft, would be the lead cryptographer. A host of interdisciplinary players would join him. One was Philip Stark, a statistician from UC Berkeley who had invented a ballot auditing system, called risk-limiting audits. There were professors specializing in human factors, the psychology of how voters interacted with machines—the types who could have predicted the hanging-chads fiasco from a mile away. Then there was DeBeauvoir and her team of clerks, who could guide the group through the vagaries of election administration.

But it was when MIT's Rivest came on board that everyone understood the group had reached an ethereal level. When word of STAR-Vote reached an expert in homomorphic cryptography living in Brussels, Belgium, he was so excited that he copped for a plane ticket and, as Wallach tells it, "flew his ass to Austin."

The team assembled for its first meeting in Austin during the spring of 2012. They gathered in the county courthouse, a solemn art deco building on Guadalupe Street, and piled into a conference room. Things got off to a slow start. A chill still lingered between Wallach and DeBeauvoir. "We needed to break the ice. He'd been ugly to me," she recalls. But when Benaloh began scrawling diagrams on the whiteboard, they were off. The marathon weekend lasted four days, with little sleep and raucous debate, punctuated by beer-infused dinners at barbecue joints around town. "By the end of the weekend," says Wallach, "we had a design."

That design looked a lot like a typical voting machine. It included a screen interface from which voters could print a ballot for review. The software came with Stark's automatic audits baked in. There was a paper trail. And the code would be entirely open source.

The defining riddle, however, was how to convince voters to trust the encryption at all. It would be utterly alien to watch a can-

JOSH BENALOH
Cryptographer, Microsoft

PHOTOGRAPH / JOVELLE TAMAYO

didate's name snap into a series of numbers and letters—the hash code that would appear onscreen, and later on their printed receipt. Would voters believe it was *their* candidate underneath that ciphertext? Benaloh's answer to the problem was a "challenge" system. Once the voter had finished at the machine and printed out their encrypted paper ballot, they could either cast it in the ballot box to be counted or they could "challenge" it by taking it to a poll worker who would mark it as "spoiled." Then the citizen would vote again. After the election they could then look up their decrypted, spoiled ballot to see whether the machine had really recorded a vote for the right person.

Propagated across precincts on the scale of a national election, the cumulative challenges would add up: If 10,000 people out of 100 million spoiled their votes, the odds that an evil machine could swap your vote without being detected were 0.01 percent.

STAR-Vote also took the idea of verification further. Benaloh wanted to give voters the opportunity to help prove that the outcome of an entire election was correct. Since all the code was open source, a cryptographic verification program could be written by anyone. True, the odds that the average Joe would learn the requisite Chaum-Pedersen protocols were slim. But the odds were better that well-financed groups—like the League of Women Voters or the Republican National Committee—could build their own in-house verifiers. They might be apps or web programs, which could be distributed among the groups' members. Voters could run the program and see for themselves that the tally was accurate.

The innovation struck its designers as well suited to the divisive currents of American politics. "What it allows you to do is choose who you're going to trust," says Benaloh. But no matter who you choose, everyone's verifying the same math.

That summer, the STAR-Vote team published their design in a journal. Their ambitions were steep: to develop the country's first publicly owned, open source voting system. Once it was developed, they would make the system available to other local governments—freeing thousands of clerks from the shackles of weak security and the retrograde manufacturers that enforced it.

For DeBeauvoir, this was no theoretical exercise: Her mission now was to build a machine that would pass certification under Texas law, and do it before her Hart eSlate machines were due to be decommissioned. She was gambling her constituents' future on an idea that no one had attempted before. What's more, she told voters that Travis County could build STAR-Vote for cheaper than the machines the manufacturers were trying to sell. "Little old me is going to take on the national manufacturing sector!" she recalls. "It wasn't so much chutzpah as it was—genuinely—we thought we could do it."

But that would require getting STAR-Vote built. To keep the technology publicly owned, DeBeauvoir's office looked for a partner outside the private market. Immediately, she ran into problems. First she pursued a West Coast nonprofit. Then she tried the state government, pitching the idea to a publicly funded tech incubator. But in an email, she was informed that Texas counties shouldn't be investing taxpayer dollars in an open source design simply to "put the product out for the world to copy and use."

By the end of 2014, DeBeauvoir still had no takers. Throughout the next year, she chased down a medley of financial suitors: the Ford Foundation, the Pew Charitable Trusts. She badgered Lloyd Dogget, Austin's US representative, to see whether Congress might chip in. She explored social impact bonds. She flew some officials in from Los Angeles who were also thinking about designing their own open source voting system, and proposed that they double up. They declined. She couldn't get other clerks interested either. Once, she and Wallach drove to a Texas Association of Counties conference to press their case. "Quite frankly," she says, "they were a little intimidated by the level of math."

As the 2016 election loomed, DeBeauvoir was becoming desperate. The STAR-Vote team continued to fly into Austin for strategy sessions, tweaking the design and searching for solutions. DeBeauvoir relied on Ben, her polymath husband, as a sounding board and a source of antic brainstorms. She also confided regularly in Wallach. In one email, she agonized that time was running out. "I'm frustrated with how long this process is taking," she wrote. What if the county's eSlate machines started to break down? "No funding and no available replacement voting system would be a terrible predicament." Later, she fretted that *she* might be the source of the trouble. "It will be obvious that I am such a newbie at this," she wrote. "I don't want my inexperience to hurt STAR-Vote."

Finally, it became clear there wouldn't be money for a publicly owned system. The STAR-Vote team decided to solicit bids from the private vendor market. DeBeauvoir was reluctant to cast the project's fortunes with the companies whose security weaknesses and lack of transparency had put her in this predicament to start with. But during 2016, just as Russian hackers had begun poking around DNC servers and state election websites, DeBeauvoir began work on a request-for-proposal announcement.

When the document finally went out to potential bidders, it was unlike anything that had come through the fax machine in the elections market. It spelled out the math for a random number generator and the specs for a 16- to 20-digit originating hash code. DeBeauvoir was optimistic. "It took us three years," she emailed one colleague. "I anticipate getting a variety of responses to build it. At least I hope to."

All that hope, however, was misplaced. In the winter of 2016, 12 dismal responses came back. One company, ES&S, flatly declined to build the machine and politely steered DeBeauvoir to its standard brochure of offerings. Another proposal, obtained by WIRED, came from Hart, the company that had previously sold DeBeauvoir the eSlate; the company simply offered up its existing model with a few perfunctory modifications, and with palpable uneasiness toward its open source requirements. Wallach called the proposal a "check-the-boxes" exercise. DeBeauvoir had hoped to cobble together a system from a hodgepodge of proposals. But, she says, "there wasn't amongst all of them a single proposal that could build it."

Or perhaps it was more accurate to say they *wouldn't* build it. As a report published by the Wharton School of Business would reveal that same year, the election technology business was a heavily consolidated industry—a cartel, essentially, of just three vendors, all owned by private equity firms—that was starved for profit and all but incapable of innovation.

Subsequent research suggested that the companies earned their most stable revenue through a maze of fees: maintenance, upkeep, software licenses. Their core business model seemed to involve locking clients into relationships of "ongoing annual payments." Small wonder, then, that the firms hadn't leapt to DeBeauvoir's idea of building a machine with open source code that aimed to liberate local governments with cheap, self-sustaining technology.

Now things had turned dire for DeBeauvoir. "I could hear the voices of the critics," she says. "*You're just a fool!*" In a last effort, she threw a Hail Mary: She formed her own company to house STAR-Vote as a nonprofit LLC. It was a measure of pure devotion, and also a reflection of the absurd dimensions her dilemma had taken. "What I didn't realize was, basically, I was becoming a startup," DeBeauvoir says. "I was setting up a whole company, a whole product line, a whole dual budget and development system."

By that time, however, Travis County's eSlate DREs—the machines Austin had been using since 2001—were about to hit their expiration date. Finally, in October 2017, she relented. "I had nothin'," she says. She contacted one of the big vendors and began negotiating for a new fleet of machines. They would last until 2030. STAR-Vote was effectively a dead letter.

DeBeauvoir had been trying to build STAR-Vote for six years. "We worked so hard, for so long. And then it was just—" She pauses. "I just couldn't push it anymore." DeBeauvoir laughs. "Even *stubborn* wasn't going to work."

During the middle of her negotiations for a new contract on voting machines, DeBeauvoir received a horrifying call. Her husband had suffered a massive heart attack. DeBeauvoir rushed out of the county courthouse. But by the time she reached the hospital, he had died.

Not long after her husband, DeBeauvoir lost her mother too. "It was the worst year of my life," she says. Ashen with grief, she experienced a sensation she had long forgotten: despair. "All I had ever done was fight back. And I couldn't reach up and grab this one by the throat," she says. For the first time since she was a little girl, she felt unable to cope.

Ben's death detonated like a bomb in DeBeauvoir's life. But when she searched her feelings, she was startled by how much grief also came from the death of what she saw as her life's work. "Ben, mother, and STAR-Vote," she says. "That losing STAR-Vote would be up there so high—that surprised me."

"Now I tell myself the truth," she says. "Maybe it was always doomed."

In the winter of 2017, shortly after STAR-Vote was declared a loss, Josh Benaloh was sitting in his office at Microsoft when he received an email from unusually high up in the chain of command. A team from the company's Legal and Policy Division wanted Benaloh's advice on a sensitive idea, which hadn't been made public yet.

Benaloh worked at Microsoft Research, the corporate Goliath's private Darpa. There he could quietly tend the flame of his interest in elections, but mostly he worked on other problems. Every once in a while, he'd pitch his superiors on cryptography and voting, but got little interest. Eventually, he understood why. "There's no way that it makes sense for Microsoft to make a business out of elections," Benaloh explains. "Elections are a tiny business. Microsoft is a mass-market software company." Nor had Benaloh's pathfinding work on STAR-Vote attracted anything more than a cursory thumbs-up as one of a million interesting things going on in a place like Microsoft.

Then, all at once, something happened that completely reoriented Microsoft's stance. "What happened," Benaloh says, "was 2016."

As the scope and fallout of Russia's meddling in the presidential election became clear, Microsoft had quietly initiated an elaborate fact-finding process, searching for anything it could do in elections that wouldn't clash with the company's business imperatives. And now the brass wanted to know: Could Benaloh replicate what he'd attempted in Austin, this time for Microsoft? Benaloh's feet were practically out the door before he could say yes.

In 2019, Microsoft launched its project under the name ElectionGuard. Once again, the technology would rely on Benaloh's dissertation about homomorphic cryptography. Voters could still challenge their ballot and walk away from the voting booth with a hash code. But in key ways, ElectionGuard was different from STAR-Vote, especially in how it proposed to solve the problem of private industry. ElectionGuard would be built as a software development kit—a highly sophisticated plug-in, essentially, that would augment existing machines. The plan was to laboriously tailor ElectionGuard to several kinds of election technology, and then give it away to the big vendors for free. Microsoft wasn't becoming a rival so much as it was housing the massive R&D division that voting companies couldn't.

For ElectionGuard, yet another dream team has assembled. Benaloh is leading the cryptography, while Wallach is designing a risk-limiting audit system that would use Benaloh's encryption. The secure systems firm Galois, STAR-Vote's only bidder for its cryptography software, won a contract to assist ElectionGuard. And Microsoft has partnered with a nonprofit called VotingWorks—run by Ben Adida, the other student of Rivest's at MIT—to build the hardware on which ElectionGuard would be demonstrated.

Earlier this year, Microsoft went searching for a real-life election where they could introduce ElectionGuard as a pilot. They settled on the town of Fulton, Wisconsin, population 3,000, about an hour's drive west of Milwaukee. In February, the town would be voting in a tiny primary: a state Supreme Court seat and the local school board. For weeks leading up to the election, a squadron of Microsoft programmers parachuted into Wisconsin farmland, running test votes on dummy ballots with the names of Fulton's favorite sons. (Willem Dafoe was one.) The people of Fulton were only too happy to be guinea pigs. Lisa Tollefson, the county clerk there, has a degree in industrial technology; she was fascinated, not intimidated, by ElectionGuard's math. "You can actually add while it's still encrypted, which is a-mazing," she beamed.

Not everyone is so thrilled about ElectionGuard. The election vendors have varied

in their degree of openness toward Microsoft's complimentary toy. In part, that may be because they know that what's free for them is also free for us—and for the next Dana DeBeauvoir who might come along to build a better voting machine. Indeed, VotingWorks, the nonprofit that built the Fulton demo, has its own ambitions to disrupt the voting industry. The vendors also say that, if they sign on, ElectionGuard will still need to run through a gauntlet of regulatory certifications—an expensive proposition. Innovation is simply harder under a mountain of regulation. "Like Silicon Valley, we'd like to 'move fast and break things,' but we do not have that luxury," said a spokesperson for the vendor Hart. (Microsoft says it is optimistic that all three vendors will eventually jump aboard.)

Remarkably, some other skeptics can be found on the teams that designed STAR-Vote and ElectionGuard itself. Philip Stark told me he wishes he'd pushed for a radically different design on DeBeauvoir's project. Sure, Benaloh's system allowed for easy detection of fraud; but what would happen when you *did* detect fraud? You could rerun the election or conduct a massive audit, unleashing chaos in either case. The perfect knowledge afforded to voters by ElectionGuard might draw an even bigger target on elections, Stark speculated, especially for hackers who simply wanted to cause confusion and undermine trust. Another conscientious objector was Adida, the guy who was literally building the hardware for Microsoft's demo in Fulton. With some heartache, he had concluded the field was moving too fast for its own good. What voters really needed was an affordable machine that worked. Would they even show up to vote on a system they couldn't really understand?

At 8 am on an arctic-cold morning, voters in Fulton began shuffling into their squat town hall. Benaloh was on hand, along with several others from Microsoft. Wallach beamed in over Zoom. One by one, voters stooped over the machine, printing two sheets—a ballot and a hash code—before they fed their vote into the tabulator and left with a strange new receipt in their hand. In all, 398 came and went. Fulton would keep track of the paper ballots, then match them against ElectionGuard's encrypted tally.

When the polls closed at 8 pm, Benaloh and his programmers hunched around a computer, running the Chaum-Pedersen protocols and poring through the data. By 9, they had a verdict: The paper ballots and the program were in perfect unison. ElectionGuard tallied the vote flawlessly. "It was 398 votes. I sweated *bullets* over those 398 votes," one of the programmers, R. C. Carter, told me. Convinced he had just seen the future of American voting, Carter—who has worked in tech for years—describes the night he spent shivering in Wisconsin as "one of the peaks of my career."

Among the team, everyone knew whose shoulders they stood on. "The Fulton demonstration was the modern interpretation of STAR-Vote," Wallach says. Benaloh saw things the same way. "STAR-Vote was not a failure," he says, and DeBeauvoir's efforts hadn't been wasted. "She deserves tremendous credit for this."

No one will be voting with ElectionGuard in November 2020. "This is long-term for us," says Benaloh. "If we get a significant use in 2022, 2024, and beyond—we're happy." But this election makes it particularly easy to see the appeal of a voting system built for verification and trust.

Of course, a complicated new homomorphically cryptographic reinvention of the franchise is not going to assuage this crisis of trust overnight. One person who knows all too well that trust is more than an encryption protocol is DeBeauvoir—who has spent the summer and fall managing an election for which she knows no precedent. "It's not a good situation in Texas right now," she sighs. "They are fighting tooth and nail down to the last sick voter, trying to prevent people from voting by mail." Requests for mail ballots have skyrocketed, and DeBeauvoir has been busy concocting ways to outmaneuver the obstacles to those votes. "It's really going to hurt voters if I don't do something," she says. But just as quickly, her ardor returns: "I'm working on it."

As for STAR-Vote, DeBeauvoir seems content simply to know that her efforts were of use. "It's not my baby anymore," she says, laughing. But she's revised her sense that the project was always doomed. "We were a little ahead of our time," she says slyly. "That was the only mistake we made."

BENJAMIN WOFFORD *(@BenWoffordDC) is a staff writer at* Washingtonian *magazine.*

HOW TO FEND OFF RUSSIAN INTER-FERENCE

An international playbook

By now, the Kremlin has meddled in so many elections around the world that the immune system of global democracy has gotten at least a little wise to its threats. Here are some lessons that other countries can teach us in the age of Russian mayhem. —Andy Greenberg

When in Doubt, Go Analog

In 2017, spooked by stories about Russian hacking in the US election, Dutch TV broadcaster RTL investigated the Netherlands' software system for counting paper ballots and found it riddled with security flaws. "The average iPad is more secure than the Dutch electoral system," said one security researcher. So in a dramatic move just six weeks before a big election, the country decided to count all the votes manually—a slower but far more secure option.

Get Physical Authentication

In 2007, Estonia was an early victim of Russian cyberattacks; yet today nearly half of the country's citizens vote online. Estonia has kept the Kremlin from corrupting that digital democracy in part by giving every citizen a smart ID card that physically authenticates their identity for online banking, paying taxes, and voting. Online elections remain science fiction in the US. But issuing Estonia-style authentication tokens—think YubiKeys—to American election officials and political campaigns could do a lot to protect them from targeted hacking.

Muddy the Waters

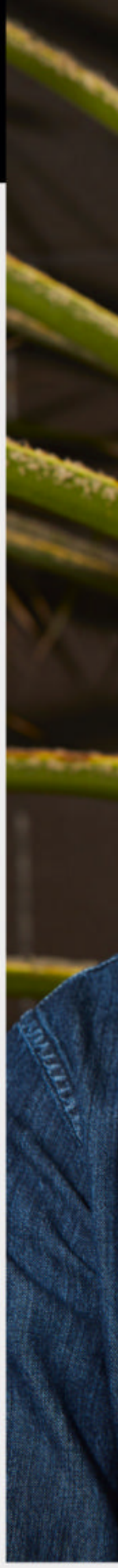
In 2017, Russian spies hacked the campaign of French presidential candidate Emmanuel Macron and leaked a trove of its emails. The campaign immediately posted a statement saying there were fabricated documents among the real ones. As Macron staffers later told *The New York Times*, the campaign itself had created entire fake email accounts to confuse the hackers. Not knowing what to believe, the media didn't take the bait.

BY
ARIELLE
PARDES

THE MASTER'S TOOLS

Donald Trump's BRILLIANT use of Facebook was key to his victory in 2016. Now a group of former staffers from the company is trying to turn his playbook AGAINST HIM.

ILLUSTRATION
BY
ADRIÀ
FRUITÓS



Three months before Election Day, James Barnes teleconferenced into a strategy meeting about how, exactly, to persuade people not to vote for Donald Trump. The 32-year-old wore his hair loosely gathered in a man bun and had the sober expression of someone who, as a hazard of his occupation, thinks about the president nearly all the time. Other faces popped up on his monitor, offering glimpses into millennial apartments, until someone started a screen share. They were here to review a series of video testimonials by conservatives who had decided to oppose Trump. Barnes and his colleagues wanted to know which ones resonated most with prospective voters on Facebook. Were testimonials from men or women more effective? Midwesterners or Southerners? How many viewers made it past the first 15 seconds?

Barnes, who works at the political nonprofit Acronym, attends these meetings every week. His team has two goals—to nudge voters away from Trump and to close what he politely calls the "enthusiasm gap" for Joe Biden. Using a custom-built tool dubbed Barometer, they microtarget "movable" voters on Facebook, run randomized tests to see what kind of ads work best, and then adjust them to taste.

Barnes, who spent the early part of his career at Facebook, leads his colleagues in two-week-long "sprints," following Mark Zuckerberg's adage about moving fast. In the past year, they've completed hundreds of tests, refining their own strategy and sharing insights with other Democratic groups. "We've got a larger corpus of data than anyone else about what's moving people," he says. (One takeaway: Voters love the Midwestern men.)

In 2016, Barnes was the Facebook staffer assigned to get Trump's digital team comfortable on the platform. Raised in Tennessee, he had been a conservative all his life. As a student at George Washington University, he had chaired the DC Federation of College Republicans, then spent several years as a GOP political consultant. But "working with Trump specifically was not something that I wanted to do," he says. "There is nothing to like about that man."

Barnes loved Facebook, though, and he believed in the vision of building a new space for political engagement. He also saw the campaign as a chance to move up in the company's intensely competitive ranks. And so he pushed through what he describes as "an enormous amount of internal conflict," reassuring himself that the work was interesting and that he was doing a good job. He showed the campaign, led by an operative named Brad Parscale, how to measure the impact of its ads and fine-tune its messaging strategy, how to expand its reach with the Lookalike Audiences tool, how to use engagement data to hook first-time donors. The result, Facebook executive Andrew Bosworth would later say, was "the single best digital ad campaign I've ever seen."

> "I've done a lot of work coming to terms with the last four years of my life."

On the night of the election, before the returns came in, Barnes recalls "thinking that part of my life would be over, because the mission would be accomplished"—his mission as an engineer, that is, not the mission of claiming the White House. Nobody on the team, least of all him, believed Trump would win. Barnes, in fact, had voted for Clinton. The outcome left him rattled. "Now, here it is four years later, and I'm still at it," he says. "A different chapter of the same book."

Barnes didn't leave Facebook until 2019, by which point he'd registered as a Democrat, moved from DC to San Francisco, and cycled through several teams at the company. Then, during his "recharge"—a 30-day vacation perk that Facebook employees receive every five years—he traveled to Peru, drank ayahuasca with a shaman, and found himself on the road to Damascus. When he returned to the States, he quit Facebook and started intermittent fasting. He set to work on a project that would repurpose the strategies he'd learned in 2016 to oppose Trump in 2020.

Last fall, Barnes met Tara McGowan, Acronym's founder and CEO, who loved his idea so much that she hired him. He began recruiting former colleagues to help. Since then, according to Damon McCoy, a researcher at New York University's Online Political Ads Transparency Project, Acronym has developed "the most sophisticated digital advertising campaign on the Democratic side."

Still, mainstream liberals have been slow to welcome the organization into the fold. Over the past year, Acronym has developed a problematic reputation. It is perhaps best known for its association with Shadow, the smartphone app that spectacularly failed to tally caucus results in Iowa, triggering rounds of recriminations and conspiracy theories. (Pete Buttigieg, who initially won the most delegates, had previously engaged Shadow's services, and McGowan's husband worked for his campaign.) Acronym is also the majority owner of a digital news ecosystem called Courier.

JAMES BARNES

In 2016, Barnes was a Facebook employee embedded with the Trump campaign. Now he's using his skills to promote Joe Biden.

PHOTOGRAPH / GABRIELA HASBUN

Modeled after the right-wing blogosphere, it promotes partisan ideology disguised as local news. NewsGuard, which rates news websites for their adherence to journalistic standards, gave Courier a 57 out of 100, placing it just above RedState and Blaze Media.

Acronym's cozy attitude toward Facebook is another major point of contention. Since the 2016 election, the platform has become something of a bogeyman in Democratic circles, owing to the role it played in Trump's upset victory. His campaign used Facebook's marketing tools not only to galvanize his supporters but also, as an unnamed senior campaign official told *Bloomberg* barely two weeks before Election Day, to engage in "major voter suppression operations" against Clinton. (Parscale has denied that the campaign's "memes and things" constituted suppression.) As a result, according to Neera Tanden, the president of the Center for American Progress, many progressives now see Facebook as "antithetical to a well-functioning democracy."

But McGowan rolls her eyes at the notion that Trump conjured some kind of digital black magic in 2016. She takes no issue with copying his playbook. In fact, she admires the way that conservative power brokers, including the Koch brothers, have used data to their advantage. She just wants to do it on the left. Some Democratic megadonors seem to buy her argument: Acronym and its affiliated political action committee have received millions in funding from LinkedIn cofounder Reid Hoffman, film director Steven Spielberg, and venture capitalist Michael Moritz.

Nearly three-quarters of adults in the US use Facebook, most of them every day. "This is where the game is played," Barnes says. "As long as the field is there, that's the field we're going to play on."

There are two types of voters: Those who know whom they're voting for and those who don't. Most fall into the first category, immutable long before Election Day, so candidates must fight not only to get their people to the polls but also to sway the very small pool of undecided, ambivalent, or otherwise out-of-touch voters that remains.

Since at least the George W. Bush era, they've done this with targeted messaging. Back then, the work took place offline. A campaign might identify conservative voters with religious leanings by, say, mining the public records of hunting licenses, purchasing membership lists from mega-churches, and looking at home ownership in specific zip codes. The winnowed-down group might then receive a glossy campaign pamphlet about the candidate's views on abortion. Barack Obama, in his 2008 presidential bid, used everything from demographic data to television pref-

erences to target voters. (One discovery: Those who watched TV Land, the basic cable channel best known for airing reruns, were less likely to have a presidential preference.)

Modern tech platforms have only sharpened that precision. Rather than guessing where the religious voters live, today's political advertisers can use geofencing technology to, for instance, locate Catholics who have been to mass at least three times in the past 90 days. On Google they can match their message to a specific search query, such as "impeachment." On Facebook, the level of control is even more granular. "It's very easy for these political advertisers to partition and very narrowly message and tell different people different things," says NYU's McCoy. "It definitely has an element of manipulation."

In 2016, with Barnes' help, the Trump campaign made particularly good use of a Facebook tool called Brand Lift. It was originally designed to help advertisers run randomized, controlled tests on their audiences: What proportion of people could recall seeing an ad for that $2,000 Gucci tote? How did they feel about Gucci generally? How likely were they to recommend it to their friends? In Trump's case, his staff would develop specialized ads for different slices of the electorate, push them out in huge numbers—reportedly as many as 60,000 a day—and gauge how people responded. Then, crucially, they would change the message as often as needed to keep voters' attention. Using Facebook, Parscale said in 2017, "I can find, you know, 15 people in the Florida Panhandle that I would never buy a TV commercial for." He added, "we took opportunities that I think the other side didn't."

Barnes coached Parscale through some of these strategies during meetings in San Antonio, Texas, where the operation was based. At the time, none of it seemed especially repugnant. Facebook wasn't the problem; the candidate was. But in the years afterward, as Barnes watched the company reckon with misinformation, foreign interference, and other abuses, his belief began to waver. In 2018 it emerged that Facebook's policies had allowed a Trump-affiliated consulting firm to harvest millions of users' personal data without their consent. Met with blowback from furious consumers and threats of government regulation from trustbusters in Congress, the platform changed its rules for political advertisers. It revoked access to some of the tools that had been crucial to Trump's efforts, including Brand Lift. At Acronym, Barnes essentially rebuilt them.

The work of the Barometer team is to constantly be in motion, to push "the messaging strategy for as long as it works," says McGowan. "And it won't work for very long." They begin by creating an audience of people whom they consider movable, based on official voter files and political preference data provided by Facebook. For most campaigns and PACs, the ideal target is someone who may not have strong partisan leanings but nevertheless casts a ballot year after year—who is likely, in other words, to provide a good return on investment.

McGowan believes that's a flawed strategy, one that cost Democrats in 2016. In the Trump-Clinton race, there was an unexpected surge in turnout among low-education voters with little political knowledge. McGowan predicts an even bigger one this year. To isolate that key demographic, Acronym blankets Facebook with surveys consisting of relatively simple multiple-choice questions, like "Who controls the House of Representatives?" Those who score lowest make up the target audience.

Much of the thinking behind Acronym's strategy comes from Solomon Messing, its chief scientist, whom Barnes poached from Facebook last fall. Academic literature supports Messing's views: Research from the Kaiser Family Foundation found that while swing voters come from many different demographics, a consistent similarity is their tendency not to pay attention to the news. Messing says he wasn't sure this would still hold true in 2020, "because everyone has an opinion about Trump," but, remarkably, it has.

Once the Barometer team has identified its low-information audience, it splits people into experimental groups and shows them different sets of messages. In July, Barnes and his colleagues tested ads criticizing Trump's response to the pandemic. One highlighted his "refusal to promote clear public-health guidelines." Another said that his administration "spent billions bailing out big corporations while Americans struggled." Most political groups survey the audience again immediately after they've seen an ad; Barnes and his colleagues wait a week, to assess how well the message stuck. For the set of pandemic ads, middle-aged voters were most responsive to economic arguments, while older voters responded best to ads that focused on Trump's threat to their health.

Some of the findings have been substantial. It turns out that posting a link to a story in *The New York Times* or other established media outlets has a much bigger effect than running straight ad copy. "For folks who don't watch the news, who don't see how badly Trump is handling things, we just show them the facts and they respond pretty well," Messing says. McCoy calls this a "trust shortcut." People are naturally wary of political ads, he says, but they're more receptive to a message when it comes from a news organization that doesn't seem to have an agenda—even if it's being promoted by an advertiser that does. (Facebook includes a label marking the post as a political ad and gives users the option to see why they were targeted.) Another genre that works quite well is critical testimony from conservative commentators. In January, Acronym pro-

moted a clip of Fox News host Tucker Carlson blasting the president for the killing of Iranian major general Qasem Soleimani. It dented Trump's approval rating by 4 percent among the low-information group.

At other times, though, Acronym's experiments have had exactly the wrong effect. After the group pushed out a series of ads attacking Trump on impeachment, Barnes and his team gathered for their standing meeting to review the data. It didn't look right. "We were like, is everything broken, or did we just move a bunch of people in the wrong direction?"

"The more partisan attacks and content there are, the more backlash we see."

he recalls. They found that all of the ads were received badly, and some of them actually made voters more sympathetic to Trump by reinforcing the idea of a Democratic witch hunt. "The more partisan attacks and content there are, the more backlash we see," says McGowan.

Later in the spring, Barnes proposed a way of getting a jump on that kind of backlash. Before he left Facebook, he had helped set up the elections integrity team, an internal effort to stop abuse and election interference on the platform. As part of its work, that group used various forms of user engagement (likes, comments, emoji reactions) as an indicator of outbreaks of misinformation.

Acronym had been treating the engagement data as an irrelevant byproduct, what Barnes calls "digital exhaust." But when he and his colleagues parsed it, they found "really strong correlations." Ads that flopped, for example, had a much higher number of "haha" emoji reactions; it seemed as though people were laughing at Acronym. When an ad had more comments than shares—a classic case of getting ratioed—that also foretold a backlash. Barnes' team incorporated these findings into a predictive machine-learning model. He calls it Dorothy, for Dorothy Thompson, a wartime journalist who got kicked out of Germany for calling attention to the rise of Nazism, and for the instrument used in the film *Twister* to spot a tornado before the funnel forms.

When I spoke with Barnes in August, he had just watched Joe Biden take the faux stage at the Democratic National Convention, cheered on by people Zooming in from all over the country. It stirred something inside of him—hope for a more presidential president, and maybe a morsel of relief.

Earlier that month, in a series of tweets about Stoicism and fasting, Barnes had quoted a few lines from Seneca, the Roman philosopher who served as an adviser to Nero, then was accused of conspiring to have the ruthless emperor assassinated. In his "Moral Epistles," Seneca had extolled the benefits of a monastic existence, of wearing coarse clothing and eating "hard and grimy" bread. Do this for long enough, he wrote, "and you will understand that a man's peace of mind does not depend upon Fortune."

Barnes thought of "Seneca's wisdom" every day. "I've done a lot of work coming to terms with the last four years of my life, so I'm not investing too much of my ego in a victory," he says. But if Donald Trump wins again? "It is an absolute nightmare scenario for the country."

As Election Day draws closer and the pool of movable voters dries up, the job of persuading them gets even harder. Fewer people pay attention to Acronym's ads now than they did in the spring; almost no one watches the video testimonials for more than 15 seconds. Back in March, when the "persuasion window" was wider, the Barometer team found that people who had seen its ads had a 3.6 percent lower approval rating of Trump, compared to a control group. By August, barely 1 percent of people would budge. Still, if these numbers seem trivial, consider a recent academic study of the persuasiveness of political ads on TV, which found "an average effect of zero."

Of course, none of that matters unless people vote. "The problem is, with all the money going into persuasion—and we've done the best work in the entire field—it's really fucking hard to connect the work you do to the actual votes converted at the end of the day," McGowan says. Barometer's second-round surveys now ask respondents to name the date of the general election, on the supposition that anyone who can likely plans to cast a ballot. But this is at best a proxy. Even for a team devoted to measurement, genuine enthusiasm is a hard thing to measure.

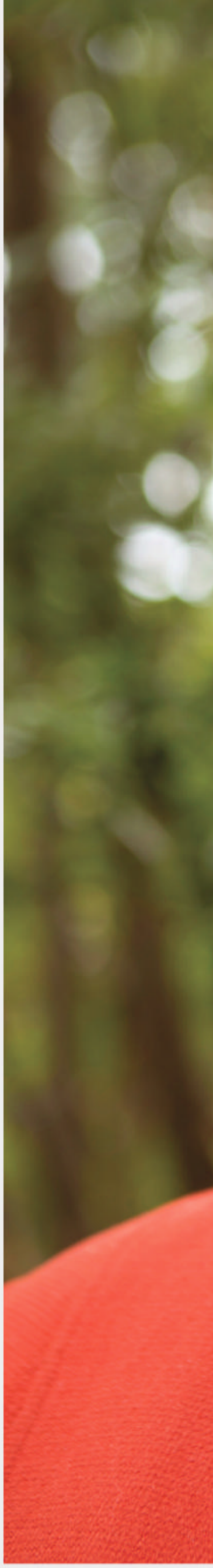
At Facebook, Barnes once led a group whose mission was to show that ads could make people do things, like visit a Macy's store after seeing the retailer's ads online. Although Barnes and his colleagues had pipelines of receipts from the Macy's data warehouse to track exactly who made a purchase, they couldn't prove much. Measuring the tangible impact of the political ads is even more complicated. "My basic perspective," he says, "is that we don't know anything." And as in 2016, they won't know what they don't know until the ballots are tallied.

ARIELLE PARDES *(@pardesoteric) is a senior writer at* WIRED*, where she works on stories about our relationship to technology. She profiled the actor Chris Evans in issue 28.02.*

The former Democratic candidate for GEORGIA GOVERNOR and founder of the advocacy organization FAIR FIGHT talks democracy, voter suppression, and why speaking Klingon doesn't always help. As told to GILAD EDELMAN.

An interview with

STACEY ABRAMS



Democracy is not partisan. That's where I begin this conversation. Who I choose once I'm inside the voting booth is my business. Ensuring my ability to *get* inside is the responsibility of government. I'm a progressive Democrat in part *because* I want the system to be fair. We should not be guaranteed victory, but we should be guaranteed access. Anyone who believes in our democracy should hold that to be a good.

We're becoming more aware of the challenges that millions of Americans have long faced when it comes to voter suppression. The pandemic has exposed even more cracks in the process. Right now, the overarching challenge is that we have this discordant set of rules that allow each state to determine how safe or how dangerous voting should be. We need uniformity in how these rules apply, and that should happen at the federal level.

Many places have taken measures to expand mail-in voting since 2016, especially since the start of the pandemic. Unfortunately, for almost every state, the beta test was done during the presidential primaries—the largest platform possible other than a general election. In Washington, DC, and New York and Pennsylvania, which have not regularly had more than 5 to 10 percent of their voters cast a ballot by mail, they simply haven't scaled the new systems appropriately. That's due to a combination of incompetence, inexperience, and a lack of resources. We are in a crisis, and all of these communities are cash-strapped.

There is both incompetence and malice at play in voter suppression. Texas, for example, is still refusing to allow voter registration online.

PHOTOGRAPH BY CHRISTIAN CODY

That is a failed policy. When technology, or the refusal to use technology, is designed to deny access, I believe it is wrong. That's my rubric. There is a narrow group of people, led by the president, who are afraid of increased voter participation. They are deeply worried that, as participation grows, their power will wane. And to them I say, I'm sorry, but that shouldn't undermine the legitimacy of access to the ballot.

If we can use technology to make the process easier, we want it. But as long as we do not have uniformity and safety and fairness in our process, we need to fall back on the analog. Paper and pen is the most easily audited form of voting. In Georgia we have these new machines that spit out your results. But the only way to audit them is to read a QR code. I'm not multilingual. I know a little bit of Klingon, but I can't read a QR code. So I have no way of verifying that what my ballot says on paper is what is being read into that computer. That lack of trust undermines my faith in the system, and unfortunately for millions of Georgians and millions of Americans, technology that does not come with trust is just as bad as someone outright stealing your election.

So often, people who have my personality type, my introversion, they shy away from this work. I tell a joke about the fact that—it's not a joke, it's true—when we used to have human contact and could knock on doors, I used to pray that no one would answer. I'm like, "God, please don't let them be at home, *please* don't let them be at home." And then they would open the door and I'd smile and I'd engage, but my heart would be beating fast. I don't like it. But I'm also very goal oriented, and my goal is to make certain that people in America have access to justice and opportunity. Just being in politics to be in politics is not my thing.

GILAD EDELMAN *(@GiladEdelman) is* WIRED*'s politics writer, based in Washington, DC.*

Why it would be nearly impossible to commit MASS VOTER FRAUD—and easy to detect if somebody tried.

THE CHECKS IN THE MAIL

BY
LILY HAY NEWMAN

ILLUSTRATION
BY
ADRIÀ
FRUITÓS

Late last October—before health officials in central China began racing to contain a mysterious outbreak of viral pneumonia, before DIY hand sanitizer tutorials flooded YouTube, before nearly 200,000 people in the US had died of Covid-19—legislators in Pennsylvania came together for a rare moment of bipartisan collaboration. For the first time since 1937, Republicans and Democrats passed a series of broad electoral reforms. Their constituents, long bound by some of the most restrictive voting rules in the nation, would now enjoy some of the most flexible. Like millions of other Americans, Pennsylvanians would be able to vote by mail without providing a reason for doing so.

"We were certainly preparing for a surge in mail-in ballots, just because people could do it now," says Kenneth Lawrence Jr., who oversees elections in Montgomery County, a suburban and rural area just northwest of Philadelphia. With the primary scheduled for April 28, he and his colleagues had about six months to launch the expanded system. They began scaling up their mail-in operations and sending out ballot applications, helped by a new state-run online portal. Then, on March 18, Pennsylvania recorded its first Covid-19 death. A week later, lawmakers voted to delay the primary to early June. Now it wasn't just the mail-in system that needed an overhaul; traditional polling places, ill-equipped for social distancing, would too.

Lawrence has lived in Montgomery County—Montco, as it's often known—for more than three decades. A lifelong Democrat, he spent most of his career running public affairs for nonpartisan clients, including Merck and Temple University. In 2017, at the age of 45, he became Montco's first Black county commissioner, initially appointed to fill a vacancy and then elected to a full term. Though he is undoubtedly losing sleep over what's coming in November, he remains affable and efficient. Like most of his counterparts across the country, he's focused on ensuring a fair and smooth voting process.

With a major public health crisis looming, that will be harder than ever. Montco has a population close to 831,000. In the 2016 presidential election, only 10,000 voters mailed in their ballots. In this year's delayed primary, that number catapulted to 126,000. Lawrence found himself in a bind. The new law required that all mail-in ballots be tabulated within eight days after the election, but an older law specified that the process couldn't begin until 7 am on Election Day. He didn't have enough staff or

equipment to make the deadline. "It took us over two weeks to count them, which is too long," he says.

As a profession, election administration is all about risk minimization, contingency planning, and thinking on your feet. A general election in a pandemic is the equivalent of the Iditarod. Across the country, officials have suddenly had to become procurement experts. Lawrence rattles off a list: hand sanitizer, face masks, face shields, sanitizing spray, disinfecting wipes, rolls of tape to mark out 6-foot increments on the floor, envelope sealers for provisional ballots. ("People don't want to lick the envelopes, and poll workers don't want to open them up," he explains.) He expects more than 200,000 applications for mail-in ballots, and he'll at least triple the size of his staff to handle the extra workload.

The United States has suffered through other difficult votes, of course, from the fraud-ridden election of 1876, in which 101 percent of South Carolina voters turned out, to the hanging chads of 2000. Covid-19 presents a historic challenge, and snafus are inevitable—but the goal, as always, is to win voters' trust. "There's a famous saying that the point of an election is to convince the loser that they lost," says Ben Adida, the executive director of VotingWorks, a nonprofit maker of open source voting equipment. "If you've convinced the loser, you've also convinced the public."

This past July, at the National Association of Secretaries of State virtual summer conference, some of the country's top election officials traded war stories from a rocky primary season. "We all knew that we were headed into what would be a contentious election year," Arizona's Katie Hobbs said in her remarks. But the pandemic had thrown everyone for a loop. Georgia had been plagued by interminably long lines as all 159 counties voted on new machines for the first time. "The transition would have been a challenge in the best set of circumstances," said Chris Harvey, the state's elections director. Throughout the US, officials were deep in negotiations to secure polling places for November, after established sites like schools, community centers, and churches had declined to open their doors. The secretaries also commiserated about the challenges of recruiting and training poll workers. Many of the usual volunteers had dropped out or simply no-showed at the primaries, owing to fears of contracting the coronavirus.

Farther down the ladder, the local officials who actually carry out the secretaries' policies and make do with the funding they receive from the state have struggled too. "It's absolutely very stressful," says Gina Kozlik, clerk-treasurer for the city of Waukesha, Wisconsin. "It's a lot of weight on our shoulders and a lot of responsibility trying to keep everyone safe."

> "We'll have shifts in place to count 24/7, as long as it takes."

Besides staffing and social-distancing concerns, the thing that worries many election officials most about November is the extra time it will take some precincts to tally votes and announce results. Americans expect to know who is president by the morning after Election Day. But that almost certainly won't be possible this year. In the 2016 race, 33 million people voted by mail; in 2020, the figure could reach 80 million or more. Depending on the state, some mail-in ballots won't be counted until a week or more after Election Day.

The longer the tabulating takes, the antsier voters are likely to get—particularly if in-person ballots tend to favor one candidate and mail-in ballots the other. "The primaries were a lesson in that," says Larry Norden, deputy director of the Brennan Center's Democracy Program at New York University School of Law. "You had election results that were very different after you counted the mail ballots." Norden fears that people will use the mismatch "to delegitimize legitimate election results." It's a concern Lawrence shares. "We don't want conspiracy theories about who got into the warehouse," he says.

That's an uphill battle, though, when one of the candidates on the ballot is the nation's conspiracist-in-chief. Donald Trump has repeatedly suggested—without evidence and over the objections of experts across the political spectrum—that the vote-by-mail system is rife with fraud, that it favors Democrats, and that efforts to expand it will make this "the most rigged election in history." Over the summer, he tried to engineer a slowdown at the US Postal Service, prompting a flurry of state lawsuits. For Trump, a delayed result seems to be synonymous with fraud. "I don't want to be waiting around for weeks and months," he said at a White House press conference in July. "I don't want to see a crooked election."

Lawrence is doing his best to take it all in stride, but some hurdles can

seem gratuitous. In June, the president's reelection campaign, along with the Republican Party, sued all 67 counties in Pennsylvania, including Montco, to prevent the use of secure drop boxes to collect ballots. They argued that the boxes "have increased the potential" for fraud, but were unable to muster any evidence of actual tampering. If the suit bothers Lawrence, he doesn't let on. "We had security guards at all of our drop boxes," he says, recalling the June primary. "They were all on county property, all on camera." And besides, he adds, "people liked them."

A mail-in ballot's journey to the voter and back is tightly choreographed and controlled. Most states use special US Postal Inspection Service barcodes to monitor ballots in transit. Once they're returned and opened—sometimes by hand, sometimes by machine—they're validated with personal information like Social Security numbers and signature checks. If a vote seems accidental (submitted in the wrong precinct, say) or suspicious (maybe the signature doesn't match the one on file), officials will pull it for detailed human review. Most states offer a digital portal that voters can use to check the status of their ballot and confirm that it has been received. If something goes wrong, or you're worried that it has, every state allows you to cast a provisional ballot in person.

In practice, then, the risk of anything truly nefarious happening in November is far lower than Trump has suggested. To actually steal a presidential election, "the size of the conspiracy would have to be enormous," says Marian Schneider, president of Verified Voting, a nonpartisan nonprofit that promotes election system integrity. Without a mole in the election precinct or the Postal Service, such a conspiracy would require a coordinated, mailbox-to-mailbox operation, one with access to a huge stolen database of voter signatures and Social Security numbers. "Every study we have had about that kind of election fraud shows that it's exceedingly rare," Schneider says.

Even smaller efforts are likely to raise alarm bells before they can affect the outcome of an election. This past May, the Postal Inspection Service reported that a mailbox in Paterson, New Jersey—a city voting entirely by mail for the first time—was stuffed with hundreds of ballots, a potential sign that they had been illegally collected from voters. The ballots were disqualified, as were more than 2,300 others whose signatures did not match those on record. In total, about one in five of all votes cast in the election had to be thrown out. Four men were charged with voter fraud, including one winning candidate who was barred from taking office. A state judge has ordered a redo of the election for November 3.

Election officials can also ferret out irregularities by spot-checking the results before they're officially certified. Sometimes this amounts to simply recounting a fixed percentage of ballots by hand to ensure the voting equipment didn't make any mistakes. But recently another, more sophisticated method has gained traction.

Devised in the late 2000s, so-called risk-limiting audits use statistics to minimize the chance of the loser being declared the winner. Officials pull a random, representative sample of ballots from across a county or state, checking only as many as are needed to satisfy the "risk limit," a kind of numerical comfort threshold. If the risk limit is set at, say, 8 percent, then the audit is designed to catch an incorrect result 92 percent of the time. This means that the scale of the audit is directly tied to the victory margin: If a candidate won in a landslide, a small sample is enough to confirm the results. If the election was a nail-biter, the sample is bigger and the audit takes longer.

Colorado was the first to implement mandatory risk-limiting audits statewide. This year, several states—including Michigan, which President Trump carried in 2016 by a margin of 0.23 percent—plan to use them. Many others have set up pilot programs or will allow individual counties to run their own. While these states are still in the minority, it's a huge leap from 2016, when exactly zero conducted risk-limiting audits.

Fraud protections will be an especially crucial backstop this year as election officials push to get votes in and tallied. In Waukesha, Kozlik has bought four extra optical scanners to relieve congestion at the busiest polling locations and speed the tabulation of mail-in ballots. Each polling place will receive and count the ballots of the people in its district. "We usually do a central count of absentee ballots in one location here at City Hall, but the increase in volume is definitely something that has caused me to look to make changes," Kozlik says.

Not all areas have the money for more equipment, though, or else they're so underfunded that any money they do get goes to making up existing deficits rather than expanding capacity. In states like Arizona, Alabama, and Louisiana, local election officials can't even afford to replace old voting machines or strengthen cybersecurity defenses for election-related systems.

But in Montco, at least, funding is less of an issue. County commissioners allocated $1.7 million for new equipment after the struggles and delays of the primary. "We purchased machines for opening up the ballots, sorting the ballots, and counting the ballots," Lawrence says. "We'll have shifts in place to count 24/7, as long as it takes." That's the mentality of officials around the US heading into this presidential election: Expect a challenge, come prepared, and don't stop until there's an accurate result—one that will convince the loser he lost.

LILY HAY NEWMAN *(@lilyhnewman) is a senior writer at* WIRED *focused on information security, digital privacy, and hacking.*

Data scientist SARA-JAYNE TERP is on a quest to quash MISINFORMATION online. Her approach: Treat it like malware and deploy the tools of CYBERSECURITY to trace the virus back to its source.

“BELIEFS CAN BE HACKED”

BY SONNER KEHRT

One day in early June 2018, Sara-Jayne Terp, a British data scientist, flew from her home in Oregon to Tampa, Florida, to take part in an exercise that the US military was hosting. On the anniversary of D-Day, the US Special Operations Command was gathering a bunch of experts and soldiers for a thought experiment: If the Normandy invasion were to happen today, what would it look like? The 1944 operation was successful in large part because the Allies had spent almost a year planting fake information, convincing the Germans they were building up troops in places they weren't, broadcasting sham radio transmissions, even staging dummy tanks at key locations. Now, given today's tools, how would you deceive the enemy?

Terp spent the day in Florida brainstorming how to fool a modern foe, though she has never seen the results. “I think they instantly classified the report,” she says. But she wound up at dinner with Pablo Breuer—the Navy commander who had invited her—and Marc Rogers, a cybersecurity expert. They started talking about

PHOTOGRAPH BY JOVELLE TAMAYO

modern deception and, in particular, a new danger: campaigns that use ordinary people to spread false information through social media. The 2016 election had shown that foreign countries had playbooks for this kind of operation. But in the US, there wasn't much of a response—or defense.

"We got tired of admiring the problem," Breuer says. "Everybody was looking at it. Nobody was doing anything."

They discussed creating their own playbook for tracking and stopping misinformation. If someone launched a campaign, they wanted to know how it worked. If people worldwide started reciting the same strange theory, they wanted a sense of who was behind it. As hackers, they were used to taking things apart to see how they worked—using artifacts lurking in code to trace malware back to a Russian crime syndicate, say, or reverse engineering a denial-of-service attack to find a way to defend against it. Misinformation, they realized, could be treated the same way: as a cybersecurity problem.

The trio left Tampa convinced there had to be a way of analyzing misinformation campaigns so researchers could understand how they worked and counter them. Not long after, Terp helped pull together an international group of security experts, academics, journalists, and government researchers to work on what she called "misinfosec."

Terp knew, of course, there's one key difference between malware and influence campaigns. A virus propagates through the vulnerable end points and nodes of a computer network. But with misinfo, those nodes aren't machines, they're humans. "Beliefs can be hacked," Terp says. If you want to guard against an attack, she thought, you have to identify the weaknesses in the network. In this case, that network was the people of the United States.

So when Breuer invited Terp back to Tampa to hash out their idea six months later, she decided not to fly. On the last day of 2018, she packed up her red Hyundai for a few weeks on the road. She stopped by a New Year's Eve party in Portland to say goodbye to friends. A storm was coming, so she left well before midnight to make it over the mountains east of the city, skidding through the pass as highway

workers closed the roads behind her.

Thus began an odyssey that started with a 3,000-mile drive to Tampa but didn't stop there. Terp spent almost nine months on the road—roving from Indianapolis to San Francisco to Atlanta to Seattle—developing a playbook for tackling misinformation and promoting it to colleagues in 47 states. Along the way, she also kept her eye out for vulnerabilities in America's human network.

Terp is a shy but warm middle-aged woman, with hair that she likes to change up—now gray and cropped short, now a blond bob, now an auburn-lavender hue. She once gave a presentation called "An Introvert's Guide to Presentations" at a hacker convention, where she recommended bringing a teddy bear. She likes finishing half-completed cross-stitches she buys at second-hand stores. She is also an expert at making the invisible visible and detecting submerged threats.

Terp began her career working in defense research for the British government. Her first gig was developing algorithms that could combine sonar readings with oceanographic data and human intelligence to locate submarines. "It was big data before big data was cool," she says. She soon became interested in how data shapes beliefs—and how it can be used to manipulate them. This was during the Cold War, and maintaining the upper hand meant knowing how the enemy would try to fool you.

After the Cold War ended, Terp shifted her focus to disaster response; she became a crisis mapper, collecting and synthesizing data from on-the-ground sources to create a coherent picture of what was really happening.

It was during disasters like the Haiti earthquake and the BP oil spill in 2010, when Terp's job included amassing real-time data from social media, that she started to notice what seemed to be intentionally false information engineered to sow confusion in an already chaotic situation. One article, citing Russian scientists, claimed the BP spill would collapse the ocean floor and cause a tsunami. Initially, Terp considered them isolated incidents, garbage clogging her data streams. But as the 2016 election drew near, it became clear to her—and many others—that misinformation campaigns were being run and coordinated by sophisticated adversaries.

As Terp crisscrossed the country in 2019, it was a little like she was crisis-mapping the US. She'd stop to people-watch in coffee shops. She struck up conversations over breakfast at Super 8. She wanted to get a feel for the communities people belonged to, how they saw themselves. What were they thinking? How were they talking to each other? She gathered her impressions slowly.

In Tampa, Terp and Breuer swiftly got down to plotting their defense against misinfo. They worked from the premise that small clues—like particular fonts or misspellings in viral posts, or the pattern of Twitter profiles shouting the loudest—can expose the origin, scope, and purpose of a campaign. These "artifacts," as Terp calls them, are bread crumbs left in the wake of an attack. The most effective approach, they figured, would be to organize a way for the security world to trace those bread-crumb trails.

Because cybercriminals tend to cobble together their exploits from a common inventory of techniques, many cybersecurity researchers use an online database called the ATT&CK Framework to analyze intrusions—it's like a living catalog of all the forms of mayhem in circulation among hackers. Terp and Breuer wanted to build the same kind of library, but for misinformation.

Terp stayed in Tampa for a week before hitting the road again, but she kept working as she traveled. To seed their database, the misinfosec team dissected earlier campaigns, from 2015's Jade Helm 15 military training exercise—which on social media was twisted into an attempt to impose martial law in Texas—to the Russia-linked Blacktivist accounts that stoked racial division before the 2016 election. They were trying to parse how each campaign worked, cataloging artifacts and identifying strategies that showed up again and again. Did a retweet from an influencer give a message legitimacy and reach? Was a hashtag borrowed from another campaign in hopes of poaching followers?

Once they could recognize patterns, they figured, they would also see choke points. In cyberwarfare, there's a concept called a kill chain, adapted from the military. Map the phases of an attack, Breuer says, and you can anticipate what they're going to do: "If I can somehow interrupt that chain, if I can break a link somewhere, the attack fails."

> Terp is cautiously optimistic about the strength of the human network that's under assault.

The misinfosec group eventually developed a structure for cataloging misinformation techniques, based on the ATT&CK Framework. In keeping with their field's tolerance for acronyms, they called it AMITT (Adversarial Misinformation and Influence Tactics and Techniques). They've identified more than 60 techniques so far, mapping them onto the phases of an attack. Technique 49 is flooding, using bots or trolls to overtake a conversation by posting so much material it drowns out other ideas. Technique 18 is paid targeted ads. Technique 54 is amplification by Twitter bots. But the database is just getting started.

Last October, the team integrated AMITT into an international, open source threat-sharing platform. That meant anyone, anywhere, could add a misinformation

campaign and, with a few clicks, specify which tactics, techniques, and procedures were at play. Terp and Breuer adopted the term "cognitive security" to describe the work of preventing malefactors from hacking people's beliefs—work they hope the world's cybersecurity teams and threat researchers will take on. They foresee burgeoning demand for this sort of effort, whether it's managing a brand's reputation, guarding against market manipulation, or protecting a platform from legal risk.

As Terp drove, she listened to a lot of talk radio. It told one long story of a nation in crisis—of a liberal plot to ruin America and of outsiders intent on destroying a way of life. Online, people on the left, too, were constantly agitated by existential threats.

This kind of fear and division, Terp thought, makes people perfect targets for misinformation. The irony is that the folks who hack into those fears and beliefs are typically hostile outsiders themselves. Purveyors of misinformation always have a goal, whether it's to destabilize a political system or just to make money. But the people on the receiving end usually don't see the big picture. They just see #5G trending or a friend's Pizzagate posts. Or, as 2020 got off the ground, links to sensational videos about a new virus coming out of China.

This February, Terp was attending a hacker convention in DC when she started feeling terrible. She limped back to an apartment she'd rented in Bellingham, north of Seattle. A doctor there told her she had an unusual pneumonia that had been moving through the area. Weeks later, Seattle became the first coronavirus hot spot in the US—and soon the Covid pandemic began to run in parallel with what people described as an "infodemic," a tidal wave of false information spreading along with the disease.

Around the same time Terp fell sick, Breuer's parents sent him a slick Facebook video claiming that the novel virus was a US-made bioweapon. His parents are from Argentina and had received the clip from worried friends back home. The video presented a chance to put AMITT through its paces, so Breuer began cataloging artifacts. The narration was in Castilian Spanish. At one point the camera pans over some patent numbers the narrator claims are for virus mutations. Breuer looked up the patents; they didn't exist. When he traced the video's path, he found it had been shared by sock-puppet accounts on Facebook. He called friends in South and Latin America to ask if they'd seen the video and realized it had been making its way through Mexico and Guatemala two weeks before showing up in Argentina. "It was kind of like tracking a virus," Breuer says.

As Breuer watched the video, he recognized several misinformation techniques from the AMITT database. "Create fake social media profiles" is technique 7. The video used fake experts to seem more legitimate (technique 9). He thought it might be planting narratives for other misinformation campaigns (technique 44: seeding distortion).

As with malware, tracing misinformation back to its source isn't an exact science. The Castilian Spanish seemed designed to give the video an air of authority in Latin America. Its high production value pointed to significant financial backing. The fact that the video first appeared in Mexico and Guatemala, and the timing of its release—February, right before migrant workers leave for spring planting in the US—suggested that its goal might be undermining American food security. "They targeted the US by targeting somebody else. It's somebody who really understood geopolitical consequences," Breuer says. This all led him to believe it was a professional job, likely Russian.

Of course, he might be wrong. But by analyzing a video like this, and putting it into the database, Breuer hopes the next time there's a polished video in Castilian Spanish making its way through South America and relying on sock puppets, law enforcement and researchers can see just how it spread the last time, recognize the pattern, and inoculate against it sooner.

A month or so into her recovery, Terp got a message from Marc Rogers, with whom she'd had dinner after the D-Day event. Rogers had helped organize an international group of volunteer researchers who were working to protect hospitals from cyberattacks and virus-related scams. They'd been seeing a flood of misinformation like the video Breuer analyzed, and Rogers wanted to know if Terp would run a team that would track campaigns exploiting Covid. She signed on.

On a Tuesday morning in August, Terp was at home trying to dissect the latest misinformation. A video posted the previous day claimed that Covid-19 was a hoax perpetrated by the World Health Organization. It had already racked up nearly 150,000 views. She also got word about a pair of Swiss websites claiming that Anthony Fauci doubted a virus vaccine would be successful and that doctors thought masks were useless. Her team was searching for other URLs linked to the same host domain, identifying ad tags used on the sites to trace funding and cataloging particular phrases and narratives—like one claiming German authorities wanted Covid-infected kids to be moved to internment camps—to pinpoint where else they appeared. All of this will be entered into the database, adding to the arsenal of information for battling misinformation. She's optimistic about the project's momentum: The more it's used, the more effective AMITT will be, Terp says, adding that her group is working with NATO, the EU, and the Department of Homeland Security to test-drive the system.

She's also cautiously optimistic about the strength of the network that's under assault. On her road trip, Terp says, the more she drove, the more hopeful she became. People were proud of their cities, loved their communities. She saw that when people have something concrete to fight for, they are less prone to end up in phantom battles against illusory enemies. "You have to involve people in their own solution," she says. By creating a world where misinformation makes more sense, Terp hopes more people will be able to reject it.

During the George Floyd protests, Terp's team was tracking another rumor: A meme kept resurfacing, in various forms, about "busloads of antifa" being driven to protests in small towns. One of the things she saw was people in small, conservative communities debunking that idea. "Somebody went, 'Hang on, this doesn't seem right,'" she says. Those people understood, on some level, that their communities were being hacked, and that they needed defending.

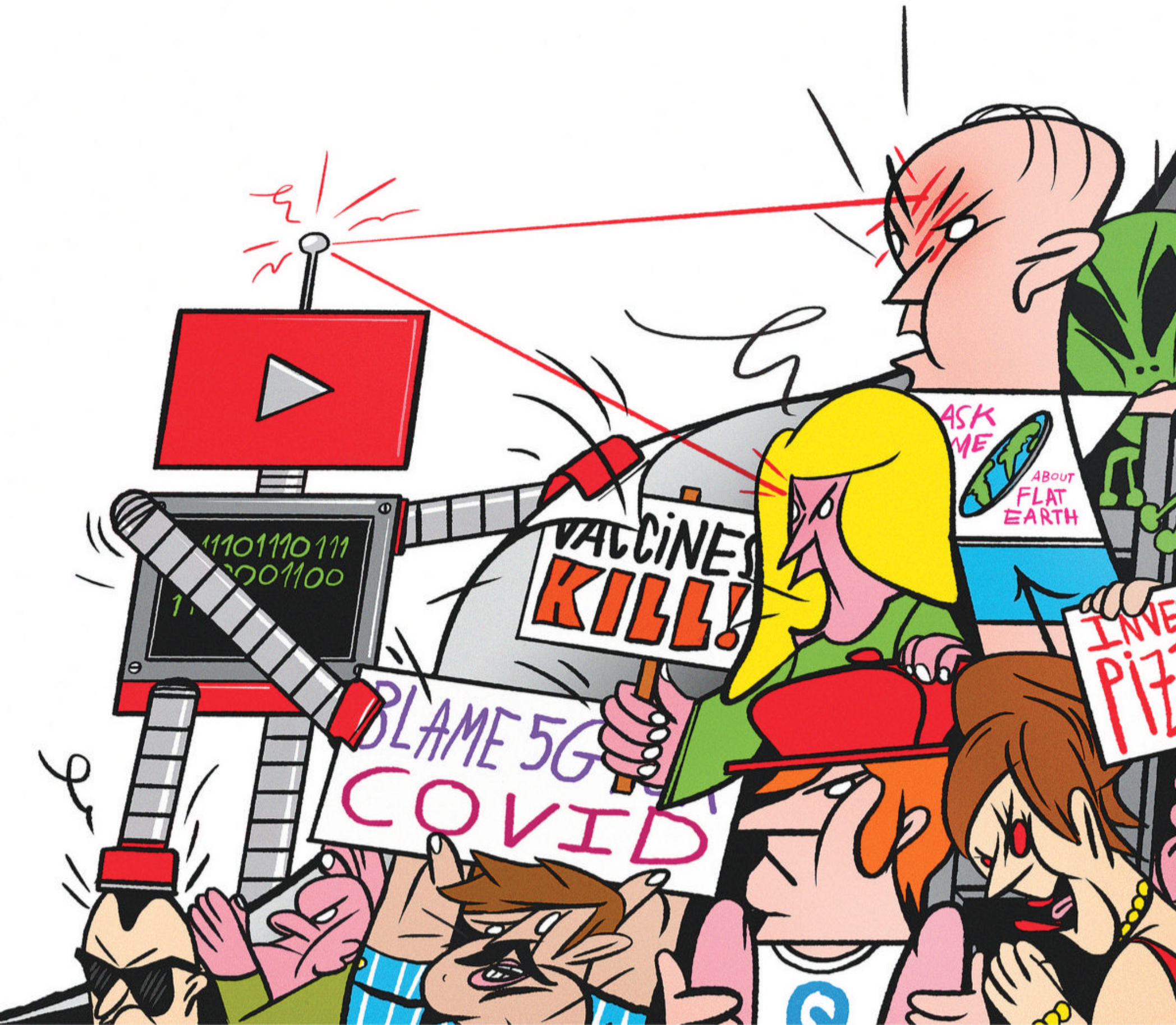
SONNER KEHRT *(@etskehrt) is a freelance writer in California. This is her first story for* WIRED.

Nothing to see here.

From flat-earthers to QAnon to Covid quackery, YouTube is awash in conspiracy theories and misinformation. But the video giant is deploying AI to try to keep the lunatic fringe from going viral.

by **CLIVE THOMPSON**

Illustration by **BRÁULIO AMADO**



Mark Sargent saw instantly that his situation had changed for the worse.

A voluble, white-haired 52-year-old, Sargent is a flat-earth evangelist who lives on Whidbey Island in Washington state and drives a Chrysler with the vanity plate "ITSFLAT." But he's well known around the globe, at least among those who don't believe they are living on one. That's thanks to YouTube, which was the on-ramp both to his flat-earth ideas and to his subsequent international stardom.

Formerly a tech-support guy and competitive virtual pinball player, Sargent had long been intrigued by conspiracy theories, ranging from UFOs to Bigfoot to Elvis' immortality. He believed some (Bigfoot) and doubted others ("Is Elvis still alive? Probably not. He died on the toilet with a whole bunch of drugs in his system"). Then, in 2014, he stumbled upon his first flat-earth video on YouTube.

He couldn't stop thinking about it. In February 2015 he began uploading his own musings, in a series called "Flat Earth Clues." As he has reiterated in a sprawling corpus of more than 1,600 videos, our planet is not a ball floating in space; it's a flat, *Truman Show*–like terrarium. Scientists who insist otherwise are wrong, NASA is outright lying, and the government dares not level with you, because then it would have to admit that a higher power (Aliens? God? Sargent's not sure about this part) built our terrarium world.

Sargent's videos are intentionally lo-fi affairs. There's often a slide show that might include images of Copernicus (deluded), astronauts in space (faked), or Antarctica (made off-limits by a cabal of governments to hide Earth's edge), which appear onscreen as he speaks in a chill, avuncular voice-over.

Sargent's top YouTube video received nearly 1.2 million views, and he has amassed 89,200 followers—hardly epic by modern influencer standards but solid enough to earn a living from the preroll ads, as well as paid speaking and conference gigs.

Crucial to his success, he says, was YouTube's recommendation system, the feature that promotes videos for you to watch on the homepage or on the "Up Next" column to the right of whatever you're watching. "We were recommended constantly," he tells me. YouTube's algorithms, he says, figured out that "people getting into flat earth apparently go down this rabbit hole, and so we're just gonna keep recommending."

Scholars who study conspiracy theories were realizing the same thing. YouTube was a gateway drug. One academic who interviewed attendees of a flat-earth convention found that, almost to a person, they'd discovered the subculture via YouTube recommendations. And while one might shrug at this as marginal weirdness—*They think the Earth is flat, who cares? Enjoy the crazy, folks*—the scholarly literature finds that conspiratorial thinking often colonizes the mind. Start with flat earth, and you may soon believe Sandy Hook was a false-flag operation or that vaccines cause autism or that Q's warnings about Democrat pedophiles are a serious matter. Once you convince yourself that well-documented facts about the solar system are a fraud, why believe well-documented facts about anything? Maybe the most trustworthy people are the outsiders, those who dare to challenge the conventions and who—as Sargent understood—would be far less powerful without YouTube's algorithms amplifying them.

For four years, Sargent's flat-earth videos got a steady stream of traffic from YouTube's algorithms. Then, in January 2019, the flow of new viewers suddenly slowed to a trickle. His videos weren't being recommended anywhere near as often. When he spoke to his flat-earth peers online, they all said the same thing. New folks weren't clicking. What's more, Sargent discovered, someone—or something—*was* watching his lectures and making new decisions: The YouTube algorithm that had previously recommended other conspiracies was now more often pushing mainstream videos posted by CBS, ABC, or *Jimmy Kimmel Live*, including ones that debunked or mocked conspiracist ideas. YouTube wasn't deleting Sargent's content, but it was no longer boosting it. And when attention is currency, that's nearly the same thing.

"You will never see flat-earth videos recommended to you, basically ever," he told me in dismay when we first spoke in April 2020. It was as if YouTube had flipped a switch.

In a way, it had. Scores of them, really—a small army of algorithmic tweaks, deployed beginning in 2019. Sargent's was among the first accounts to feel the effects of a grand YouTube project to teach its recommendation AI how to recognize the conspiratorial mindset and demote it. It was a complex feat of engineering, and it worked; the algorithm is

less likely now to promote misinformation. But in a country where conspiracies are recommended everywhere—including by the president himself—even the best AI can't fix what's broken.

When Google bought YouTube in 2006, it was a woolly startup with a DIY premise: "Broadcast Yourself." YouTube's staff back then wasn't thinking much about conspiracy theories or disinformation. The big concern, as an early employee told me, was what they referred to internally as "boobs and beheadings"—uploads of pornography and gruesome al Qaeda actions.

From the first, though, YouTube executives intuited that recommendations could fuel long binges of video surfing. By 2010, the site was suggesting videos using collaborative filtering: If you watched video A, and lots of people who watched A also watched B, then YouTube would recommend you watch B too. This simple system also up-ranked videos that got lots of views, under the assumption that it was a signal of value. That methodology tended to create winner-take-all dynamics that resulted in "Gangnam Style"–type virality; lesser-known uploads seldom got a chance.

In 2011, Google tapped Cristos Goodrow, who was then director of engineering, to oversee YouTube's search engine and recommendation system. Goodrow noticed another problem caused by YouTube's focus on views, which was that it encouraged creators to use misleading tactics—like racy thumbnails—to dupe people into clicking. Even if a viewer immediately bailed, the click would goose the view count higher, boosting the video's recommendations.

Goodrow and his team decided to stop ranking videos based on clicks. Instead, they focused on "watch time," or how long viewers stayed with a video; it seemed to them a far better metric of genuine interest. By 2015, they would also introduce neural-net models to craft recommendations. The model would take your actions (whether you'd finished a video, say, or hit Like) and blend that with other information it had gleaned (your search history, geographic region, gender, and age, for example; a user's "watch history" became increasingly significant too). Then the model would predict which videos you'd be most likely to actually watch, and presto: recommendations, more personalized than ever.

The recommendation system became increasingly crucial to YouTube's frenetic push for growth. In 2012, YouTube's vice president of product, Shishir Mehrotra, declared that by the end of 2016 the site would hit a billion hours of watch time per day. It was an audacious goal; at the time, people were watching YouTube for only 100 million hours a day, compared to more than 160 million on Facebook and 5 billion on TV. So Goodrow and the engineers began thirstily hunting for any tiny tweak that would bump watch time upward. By 2014, when Susan Wojcicki took over as CEO, the billion-hour goal "was a religion at YouTube, to the exclusion of nearly all else," as she later told the venture capitalist John Doerr. She kept the goal in place.

The algorithmic tweaks worked. People spent more and more time on the site, and the new code meant small creators and niche content were finding their audience. It was during this period that Sargent saw his first flat-earth video. And it wasn't just flat-earthers. All kinds of misinformation, some of it dangerous, rose to the top of watchers' feeds. Teenage boys followed recommendations to far-right white supremacists and Gamergate conspiracies; the elderly got stuck in loops about government mind control; anti-vaccine falsehoods found adherents. In Brazil, a marginal lawmaker named Jair Bolsonaro rose from obscurity to prominence in part by posting YouTube videos that falsely claimed left-wing scholars were using "gay kits" to convert kids to homosexuality.

In the hothouse of the 2016 US election season, observers argued that YouTube's recommendations were funneling voters into ever-more-extreme content. Conspiracy thinkers and right-wing agitators uploaded false rumors about Hillary Clinton's imminent mental collapse and involvement in a nonexistent pizzeria pedophile ring, then watched, delightedly, as their videos lifted off in YouTube's Up Next column. A former Google engineer named Guillaume Chaslot coded a web-scraper program to see, among other things, whether YouTube's algorithm had a political tilt. He found that recommendations heavily favored Trump as well as anti-Clinton material. The watch time system, in his view, was optimizing for whomever was most willing to tell fantastic lies.

As 2016 wore on and the billion-hour deadline loomed, the engineers went into overdrive. Recommendations had become the thrumming engine of YouTube, responsible for an astonishing 70 percent of all its watch time. In turn, YouTube became a key source of revenue in the Alphabet empire.

Goodrow hit the target: On October 22, 2016, a few weeks before the presidential election, users watched 1 billion hours of videos on YouTube.

After the 2016 election, the tech indus-try came in for a reckoning. Critics laced into Facebook's algorithm for boosting conspiratorial rants and hammered Twitter for letting in phalanxes of Russian bots. Scrutiny of YouTube emerged a bit later. In 2018 a UC Berkeley computer scientist named Hany Farid teamed up with Guillaume Chaslot to run his scraper again. This time, they ran the program daily for 15 months, looking specifically for how often YouTube recommended conspiracy videos. They found the frequency rose throughout the year; at the peak, nearly one in 10 videos recommended were conspiracist fare.

"It turns out that human nature is awful," Farid tells me, "and the algorithms have figured this out, and that's what drives engagement." As Micah Schaffer, who worked at YouTube from 2006 to 2009, told me, "It really is they are addicted to that traffic."

YouTube executives deny that the billion-hour push led to a banquet of conspiracies. "We don't see evidence that extreme content or misinformation is on average more engaging, or generates more viewership, than anything else," Goodrow said. (YouTube also challenged Farid and Chaslot's research, saying it "does not accurately reflect how YouTube's recommendations work or how people watch and interact with YouTube.") But, within YouTube, the principle of "Broadcast Yourself," without restriction, was colliding with concerns about safety and misinformation.

On October 1, 2017, when a man used an arsenal of weapons to fire into a crowd of people at a concert in Las Vegas, YouTube users immediately began uploading false-flag videos claiming the shooting was orchestrated to foment opposition to the Second Amendment.

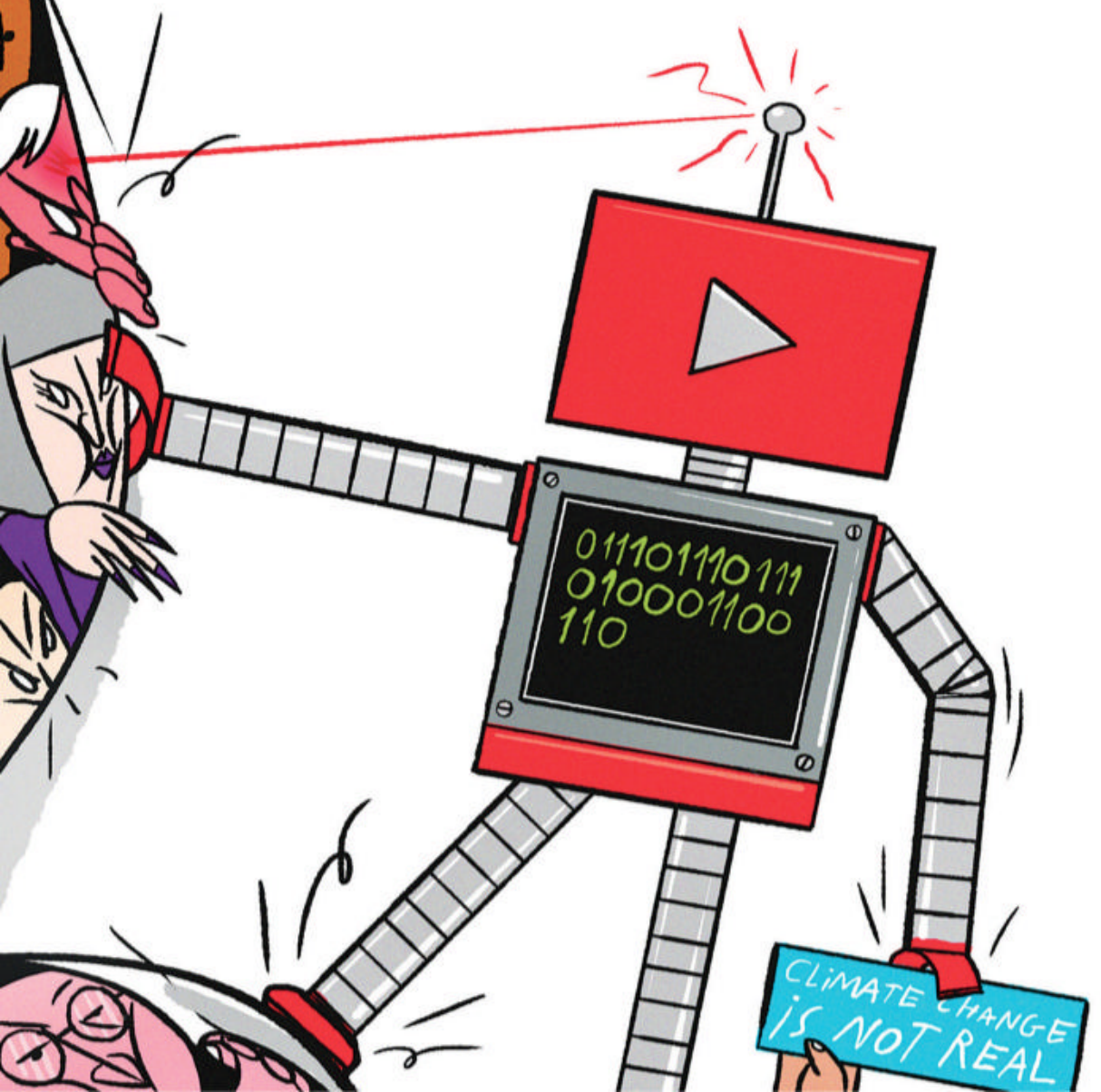
Just 12 hours after the shooting, Geoff Samek arrived for his first day as a product manager at YouTube. For several days he and his team were run ragged trying to identify fabulist videos and delete them. He was, he told me, "surprised" by how little was in place to manage a crisis like this. (When I asked him what the experience felt like, he sent me a clip of Tim Robbins being screamed at as a new mailroom hire in *The Hudsucker Proxy*.) The recommendation system was apparently making things worse; as BuzzFeed reporters found, even three days after the shooting the system was still promoting videos like "PROOF: MEDIA & LAW ENFORCEMENT ARE LYING."

"I can say it was a challenging first day," Samek told me dryly. "Frankly, I don't think our site was performing super well for misinformation ... I think that kicked off a lot of things for us, and it was a turning point."

YouTube already had policies forbidding certain types of content, like pornography or speech encouraging violence. To hunt down and delete these videos, the company used AI "classifiers"—code that automatically detects potentially policy-violating videos by analyzing, among other signals, the headlines or the words spoken in a video (which YouTube generates using its automatic speech-to-text software). They also had human moderators who reviewed videos the AI flagged for deletion.

After the Las Vegas shooting, executives began focusing more on the challenge. Google's content moderators grew to 10,000, and YouTube created an "intelligence desk" of people who hunt for new trends in disinformation and other "inappropriate content." YouTube's definition of hate speech was expanded to include Alex Jones' claim that the murders at Sandy Hook Elementary School never occurred. The site had already created a "breaking-news shelf" that would run on the homepage and showcase links to content from news sources that Google News had previously vetted. The goal, as Neal Mohan, YouTube's chief product officer, noted, was not just to delete the obviously bad stuff but to boost reliable, mainstream sources. Internally, they began to refer to this strategy as a set of R's: "remove" violating material and "raise up" quality stuff.

But what about content that wasn't *quite* bad enough to be deleted? Like alleged conspiracies or dubious information that doesn't advocate violence or promote "dangerous remedies or cures" or otherwise explicitly violate policies? Those videos wouldn't be removed by moderators or the content-blocking AI. And yet, some executives wondered if they were complicit by promoting them at all. "We noticed that some people were watching things that we weren't happy with them



watching," says Johanna Wright, one of YouTube's vice presidents of product management, "like flat-earth videos." This was what executives began calling "borderline" content. "It's near the policy but not against our policies," as Wright said.

By early 2018, YouTube executives decided they wanted to tackle the borderline material too. It would require adding a third R to their strategy—"reduce." They'd need to engineer a new AI system that would recognize conspiracy content and misinformation and down-rank it.

In February, I visited YouTube's headquarters in San Bruno, California. Goodrow had promised to show me the secret of that new AI.

It was the day after the Iowa caucuses, where a vote-counting app had failed miserably. The news cycle was spinning crazily, but inside YouTube the mood seemed calm. We filed into a conference room, and Goodrow plunked into a chair and opened his laptop. He has close-cropped hair and sported a normcore middle-aged-dad style, wearing a zip-up black sweater over beige khakis. A mathematician by training, Goodrow can be intense; he was a dogged advocate of the billion-hour project and neurotically checked view stats every single day. Last winter he mounted a brief and failed run in the Democratic primary for his San Mateo County congressional district. Goodrow and I were joined by Andre Rohe, a dry-witted German who came to YouTube in 2015 to be head of Discovery engineering after three years heading Google News.

Rohe beckoned me to his screen. He and Goodrow seemed slightly nervous. The inner workings of any system at Google are closely guarded secrets. Engineers worry that if they reveal too much about how any algorithm works—particularly one designed to down-rank content—outsiders could learn to outwit it. For the first time, Rohe and Goodrow were preparing to reveal some details of the recommendation revamp to a reporter.

To create an AI classifier that can recognize borderline video content, you need to train the AI with many thousands of examples. To get those training videos, YouTube would have to ask hundreds of ordinary humans to decide what looks dodgy and then feed their evaluations and those videos to the AI, so it could learn to recognize what dodgy looks like. That raised a fundamental question: What is "borderline" content? It's one thing to ask random people to identify an image of a cat or a crosswalk—something a Trump supporter, a Black Lives Matter activist, and even a QAnon adherent could all agree on. But if they wanted their human evaluators to recognize something subtler—like whether a video on Freemasons is a study of the group's history or a fantasy about how they secretly run government today—they would need to provide guidance.

YouTube assembled a team to figure this out. Many of its members came from the policy department, which creates and continually updates the rules about the content YouTube bans outright. They developed a set of about three dozen questions designed to help a human decide whether content moved significantly in the direction of those banned areas, but didn't quite get there.

These questions were, in essence, the wireframe of the human judgment that would become the AI's smarts. These hidden inner workings were listed on Rohe's screen. They allowed me to take notes but wouldn't give me a copy to take away.

One question asks whether a video appears to "encourage harmful or risky behavior to others" or to viewers themselves. To help narrow down what type of content constitutes "harmful or risky behavior," there is a set of check boxes pointing out various well-known self-harms YouTube has grappled with—like "pro ana" videos that encourage anorexic behaviors, or graphic images of self-harm.

"If you start by just asking, 'Is this harmful misinformation?' then everybody has a different definition of what's harmful," Goodrow said. "But then you say, 'OK, let's try to move it more into the concrete, specific realm by saying, is it about self-harm? What kinds of harm is it?' Then you tend to get higher agreement and better results." There's also an open-ended box that an evaluator can write in to explain their thinking.

Another question asks the evaluators to determine whether a video is "intolerant of a group" based on race, religion, sexual orientation, gender, national origin, or veteran status. But there's a supplementary question: "Is the video satire?" YouTube's policies prohibit hate speech and spreading lies about ethnic groups, for example, but they can permit content that mocks that behavior by mimicking it.

Rohe pointed to another category, one that asks whether a video is "inaccurate, misleading, or deceptive." It then goes on to ask the evaluator to check all the possible categories of factual nonsense that might apply, like "unsubstantiated conspiracy theories," "demonstratively inaccurate information," "deceptive content," "urban legend," "fictional story or myth," or "contradicts well-established expert consensus." The evaluators each spend about 5 minutes assessing each video, on top of the time it takes to watch it, and are encouraged to do research to help understand its context.

Rohe and Goodrow said they had tried to reduce potential bias among the human evaluators by choosing people who were diverse in terms of age, geography, gender, and race. They also made sure each video was rated by up to nine separate evaluators so that the results were subject to the "wisdom of a group," as Goodrow put it. Any videos with medical subjects were rated by a team of doctors, not laypeople.

This diversity among the evaluators' views can pose problems for training the AI, though. If evaluators are too divided over whether a video is deceptive or factually misleading, then their responses won't provide a clear signal. As Woojin Kim, a vice president of product management, pointed out, "If we're talking about a contentious political topic, where you do have multiple perspectives ... those would oftentimes end up being marked not as borderline content." When the AI classifier was

trained on those examples, it absorbed the same divided mentality. If it encountered a new video with the same characteristics, it would, metaphorically, shrug and not classify it as borderline either.

The evaluators processed tens of thousands of videos, enough for YouTube engineers to begin training the system. The AI would take data from the human evaluations—that a video called "Moon Landing Hoax—Wires Footage" is an "unsubstantiated conspiracy theory," for example—and learn to associate it with features of that video: the text under the title that the creator uses to describe the video ("We can see the wires, people!"); the comments ("It's 2017 and people still believe in moon landings ... help ... help"); the transcript ("the astronaut is getting up with the wire taking the weight"); and, especially, the title. The visual content of the video itself, interestingly, often wasn't a very useful signal. As with videos about virtually any topic, misinformation is often conveyed by someone simply speaking to the camera or (as with Sargent's flat-earth material) over a procession of static images.

Another useful training feature for the AI was "co-watches," or the fare users typically watch before or after the video in question. In a sense, it was a measure of the company a video keeps. If National Geographic posts a video titled "Round Earth vs. Flat Earth," an AI might recognize it as having words very similar to a flat-earth video. But the co-watches would likely be an interview with the astrophysicist Neil deGrasse Tyson or a scientist's TED talk, while a flat-earth conspiracy video might pair with a rant on the CIA's UFO cover-up.

The AI classifier does not produce a binary answer; it doesn't say whether a video is or isn't "borderline." Instead, it generates a score, a mathematical weight that represents how likely the video is to approach the borderline. That weight is incorporated into the overall recommendation AI and becomes one of the many signals used when recommending the video to a particular user.

In January 2019, YouTube began rolling out the system. That's when Mark Sargent noticed his flat-earth views take a nose dive. Other types of content were getting down-ranked, too, like moon-landing conspiracies or videos perseverating on chemtrails. Over the next few months, Goodrow and Rohe pushed out more than 30 refinements to the system that they say increased its accuracy. By the summer, YouTube was publicly declaring success: It had reduced by 50 percent the watch time of borderline content that came from recommendations. By December it reported a reduction of 70 percent.

The company won't release its internal data, so it's impossible to confirm the accuracy of its claims. But there are several outside indications that the system has had an effect. One is that consumers and creators of borderline stuff complain that their favorite material is rarely boosted any more. "Wow has anybody else noticed how hard it is to find 'Conspiracy Theory' stuff on YouTube lately? And that you easily find videos 'debunking' those instead?" one comment noted in February of this year. "Oh yes, youtubes algorithm is smashing it for them," another replied.

Then there's the academic research. Berkeley professor Hany Farid and his team found that the frequency with which YouTube recommended conspiracy videos began to fall significantly in early 2019, precisely when YouTube was beginning its updates. By early 2020, his analysis found, those recommendations had gone down from a 2018 peak by 40 percent. Farid noticed that some channels weren't merely reduced; they all but vanished from recommendations. Indeed, before YouTube made its switch, he'd found that 10 channels—including that of David Icke, the British writer who argues that reptilians walk among us—comprised 20 percent of all conspiracy recommendations (as Farid defines them); afterward, he found that recommendations for those sites "basically went to zero."

Another study that somewhat backs up YouTube's claims was conducted by the computer scientist Mark Ledwich and Anna Zaitsev, a postdoctoral scholar and lecturer at Berkeley. They analyzed YouTube recommendations, looking specifically at 816 political channels and categorizing them into different ideological groups such as "Partisan Left," "Libertarian," and "White Identitarian." They found that YouTube recommendations mostly now guide viewers of political content to the mainstream. The channels they grouped under "Social Justice," on the far left, lost a third of their traffic to mainstream sources like CNN; conspiracy channels and most on the reactionary right—like "White Identitarian" and "Religious Conservative"—saw the majority of their traffic slough off to commercial right-wing channels, with Fox News being the hugest beneficiary.

If Zaitsev and Ledwich's analysis of YouTube "mainstreaming" traffic holds up—and it's certainly a direction that YouTube itself endorses—it would fit into a historic pattern. As law professor Tim Wu noted in his book *The Master Switch*, new media tend to start out in a Wild West, then clean up, put on a suit, and consolidate in a cautious center. Radio, for example, began as a chaos of small operators proud to say anything, then gradually coagulated into a small number of mammoth networks aimed mostly at pleasing the mainstream.

For critics like Farid, though, YouTube has not gone far enough, quickly enough. "Shame on YouTube," he told me. "It was only after how many years

of this nonsense did they finally respond? After public pressure just got to be so much they couldn't deal with it."

Even the executives who set up the new "reduce" system told me it wasn't perfect. Which makes some critics wonder: Why not just shut down the recommendation system entirely? Micah Schaffer, the former YouTube employee, says, "At some point, if you can't do this responsibly, you need to not do it." As another former YouTube employee noted, determined creators are adept at gaming any system YouTube puts up, like "the velociraptor and the fence."

Still, the system appeared to be working, mostly. It was a real, if modest, improvement. But then the floodgates opened again. As the winter of 2020 turned into a spring of pandemic, a summer of activism, and another norm-shattering election season, it looked as if the recommendation engine might be the least of YouTube's problems.

A month after I visited YouTube, the new coronavirus pandemic was in full swing. It had itself become a fertile field for new conspiracy theories. Videos claimed that 5G towers caused Covid-19; Mark Sargent had interrupted his flat-earth musings to upload a few videos in which he said the pandemic lockdown was an ominous preparation for social control. He told me the government would use a vaccine to inject everyone with an invisible mark, and "then it goes to the whole Christian mark of the beast," the prophesy from the Book of Revelations.

On March 30, I talked to Mohan again, but this time on Google Hangouts. He was ensconced in a wood-paneled room at his home, clad in a blue polo shirt, while the faint sounds of his children echoed from elsewhere in the house.

YouTube, he told me, had been moving aggressively to clamp down on disinformation about the pandemic and to counteract it. The platform created an "info panel" to run under any video mentioning Covid-19, linking to the Centers for Disease Control and other global and local health officials. By late August, these panels had received more than 300 billion impressions. YouTube had been removing videos with dangerous "medical" information every day, including those promoting "harmful cures," as Mohan says, and videos telling people to flout stay-at-home rules. To raise up useful information, the company arranged for several popular YouTubers to interview Anthony Fauci, the director of the National Institute of Allergy and Infectious Diseases who had become a regular presence on TV and a voice of scientific reason.

Mohan had also been meeting with YouTube's "intel desk," whose researchers had been trying to root out the latest Covid conspiracies. Goodrow and Rohe would use those videos to help update their AI classifier at least once a week, so it could help down-rank new strains of borderline Covid content.

But even as we spoke, YouTube videos with wild-eyed claims were being uploaded and amassing views. An American chiropractor named John Bergman got more than a million views for videos suggesting that hand sanitizer didn't work and urging people to use essential oils and vitamin C to treat the contagion. On April 16, a conspiracy channel named the Next News Network uploaded a video claiming that Fauci was a "criminal," that coronavirus was a false-flag operation to impose "mandatory vaccines," and that if anyone refused to be vaccinated, they'd be "shot in the head." It racked up nearly 7 million views in two weeks, before YouTube finally took it down. Then came ever more unhinged uploads, including the infamous "Plandemic" video—alleging a conspiracy to push a vaccine—or the so-called "white coat summit" of July 27, in which a group of doctors assembled in front of the Supreme Court to falsely claim that hydroxychloroquine could cure Covid and that masks were unnecessary.

YouTube was playing a by-now familiar game of social media whack-a-mole. A video that violated YouTube's rules would emerge and rapidly gain views, then YouTube would take it down. But it wasn't clear that recommendations were key to these sudden viral spikes. On August 14, a 90-minute video by Millie Weaver, a contributor to the far-right conspiracist site Infowars, went online, filled with claims of a deep state arrayed against President Trump. It was linked and shared in a number of right-wing circles. Dozens of Reddit threads passed it on ("Watch it before it's gone," one redditor wrote), and it was shared more than 53,000 times on Facebook, as well as on scores of right-wing YouTube channels, including by many followers of QAnon, one of the fastest-growing—and most dangerous—conspiracy theories in the nation. YouTube took it down a day later, saying it violated its hate-speech rules. But within that 24 hours, it amassed over a million views.

This old-fashioned spread—a mix of organic link-sharing and astroturfed, bot-propelled promotion—is powerful and, say observers, may sideline any changes to YouTube's recommendation system. It also suggests that users are adapting and that the recommendation system may be less important, for good and ill, to the spread of misinformation today. In a study for the think tank Data & Society, the researcher Becca Lewis mapped out the galaxy of right-wing commentators on YouTube who routinely spread borderline material. Many of those creators, she says, have built their often massive audiences not only through YouTube recommendations but also via networking. In their videos they'll give shout-outs to one another and hype each other's work, much as YouTubers all enthusiastically promoted Millie Weaver's fabricated musings.

"If YouTube completely took away the recommendations algorithm tomorrow, I don't think the extremist problem would be solved. Because they're just entrenched," Lewis tells me. "These people have these intense fandoms at this point. I don't know what the answer is."

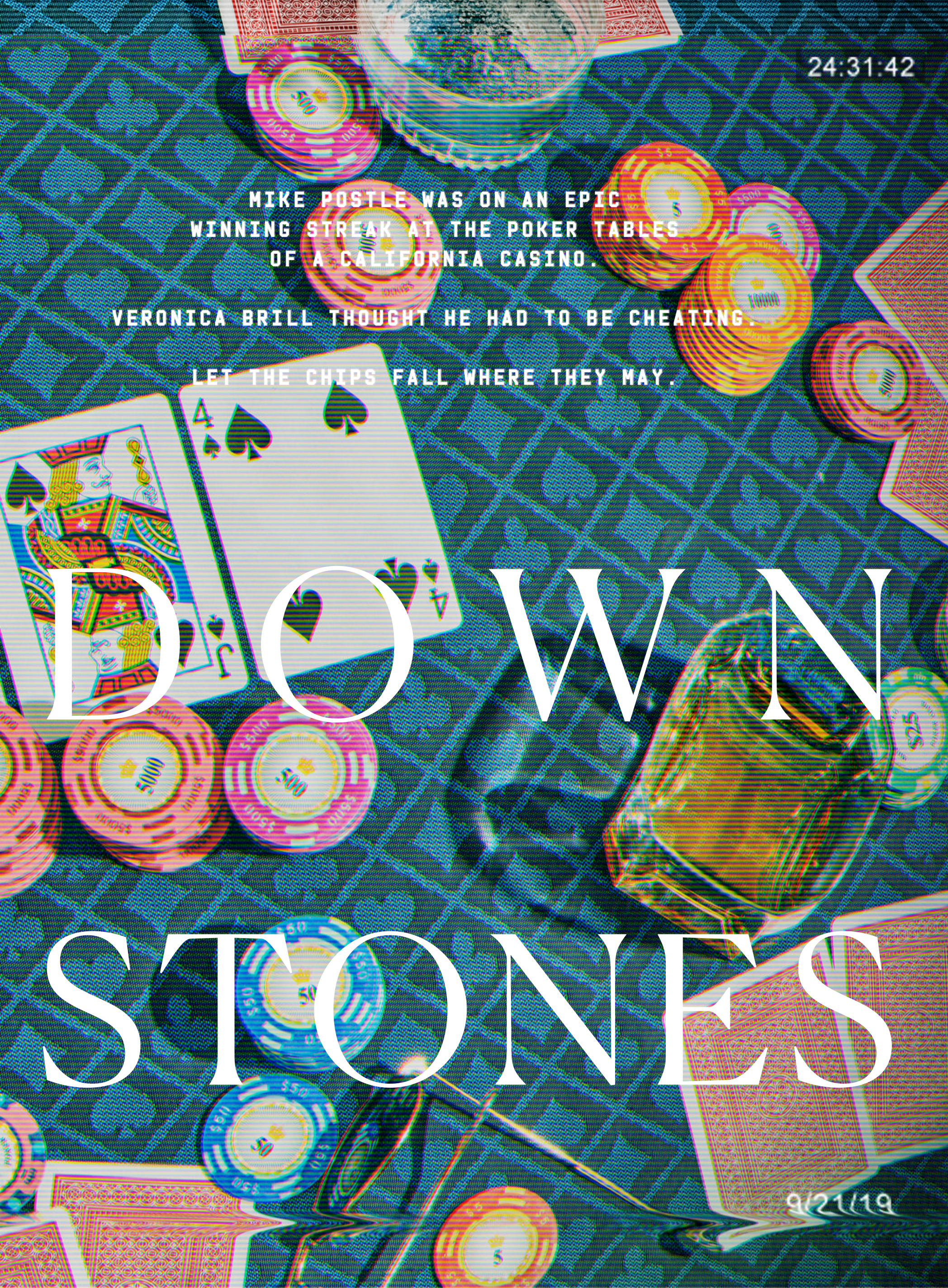
One of the former Google engineers I spoke to agreed: "Now that society is so polarized, I'm not sure YouTube alone can do much," as the engineer noted. "People who have been radicalized over the past few years aren't getting unradicalized. The time to do this was years ago."

CLIVE THOMPSON *(@pomeranian99) is a* WIRED *contributing editor and author of* Coders: The Making of a New Tribe and the Remaking of the World.

THE SHOW AT

By BRENDAN I. KOERNER

PHOTOGRAPHS BY
KEIRNAN MONAGHAN & THEO VAMVOUNAKIS


24:31:42
MIKE POSTLE WAS ON AN EPIC
WINNING STREAK AT THE POKER TABLES
OF A CALIFORNIA CASINO.
VERONICA BRILL THOUGHT HE HAD TO BE CHEATING.
LET THE CHIPS FALL WHERE THEY MAY.
DOWN
STONES
9/21/19

Mike Postle was on another tear. The moon-faced 42-year-old was deep into a marathon poker session at Stones Gambling Hall, a boxy glass-and-steel casino wedged between Interstate 80 and a Popeye's in suburban Sacramento. The September 21, 2019, game, which Stones was broadcasting to audiences via YouTube and Twitch, had attracted several top players to the casino's card room, a gaudily lit space done up like an Old West saloon. One pro from Las Vegas had flown in on a chartered jet with $50,000 in cash. Yet, as usual when he appeared on Stones' livestream, Postle was shredding the competition; he was the evening's chips leader by a comfortable margin.

Five hours into the show, a curious hand took shape. Like all games of Texas Hold 'Em, the most widely televised form of poker, the action began with each player receiving two face-down cards—the hole cards. Five community cards were then to be dealt face-up in three rounds, with opportunities for betting in between. The first face-up batch, called the flop, would consist of three cards. After that, the dealer would add a single card ("the turn") followed by one more ("the river"). Players would vie for the pot by assembling the best hands using their two hole cards plus any three from the shared array.

Even before the flop, though, seven of the nine players chose to fold. Postle, who'd been dealt the queen of diamonds and jack of hearts, pressed forward with the hand. His sole opponent would be Marle Cordeiro, a Las Vegas–based pro with a large social media following.

The flop contained the 8 of spades, 9 of diamonds, and jack of diamonds—a promising trio for Postle, who now had a pair (jacks) and was just a 10 away from a queen-high straight (8-9-10-jack-queen). There were two shared cards left to be dealt. The turn produced the relatively useless 4 of spades, after which Cordeiro placed a $600 bet.

Postle, his white baseball cap nearly concealing his eyes, clutched his right shoulder with his left hand as he mulled his options. Most seasoned players would call or raise in his situation: The statistical likelihood that his hand would yield a favorable monetary outcome was high enough to make proceeding to the river an easy choice. But Postle had an unorthodox style of play, and he often made decisions that his rivals deemed either wildly aggressive or inexplicably meek. Those instincts had served him well in recent months: He was in the midst of an epic winning streak—a "heater"—that had turned him into a local folk hero. He'd become such a force on Stones' livestream, in fact, that casino regulars had taken to calling him the Messiah and even God.

Postle spent half a minute in quiet contemplation, almost motionless in his black leather chair. Then, pursing his lips in resignation, he chucked his cards forward to fold.

Postle's surrender, though counterintuitive, turned out to be a canny move because Cordeiro was holding "the nuts"—poker slang for the most valuable hand. Her hidden hole cards were the 10 of diamonds and queen of spades, so she'd already secured a queen-high straight before the river; she had a 96 percent chance of maintaining her edge once all the cards were dealt.

Justin Kelly, one of the livestream's two commentators, gushed over the genius of Postle's eccentric play. "This is what I'm talking about people!" he exclaimed from his broadcast booth across the room. "Postle takes the weirdest lines and gets people to lay down huge hands all the time. But when he has top pair and a straight draw, he is able to just lay down against the nuts. Postle is just like a freak! He's just a freak of nature."

Kelly's co-commentator, 42-year-old Veronica Brill, did not share his sense of awe. She had been observing Postle up close for a while, both as an opponent at the table and a broadcaster, and she'd come to believe there was a nefarious reason for his success. For months she'd resisted mentioning her suspicions on the livestream, hoping that Stones would handle the matter behind the scenes. But the fold against Cordeiro struck her as so fishy that she could no longer keep quiet. Brill leaned back, gently shook her head, and took a half-step toward calling out God.

"It doesn't make sense," she said, her soft monotone tinged with mockery. "It's like he knows. It doesn't make sense. It's weird." Sounding caught off guard by his cohost's skeptical remarks, Kelly continued effusively—"Absolute insanity, guys!"—before managing to change the subject.

Late that night, as she drove in silence toward her Bay Area home, Brill turned the broadcast over and over in her mind. Her insinuation about Postle, though subtle, had the potential to cause a stir. Fellow players would gossip that jealousy had driven her to smear a more accomplished rival, a decent man who'd just come through a harrowing family drama. Gliding west on Interstate 80, Brill realized she had no choice but to commit one of poker's cardinal sins.

→ LIKE MANY OTHERS who spent huge chunks of time at Stones, Brill had long considered Postle a friend. A generous soul who exuded a puckish charm, Postle was the sort who'd pay for everyone's drinks while regaling the bar with bawdy tales. (He was particularly fond of a story about getting banned from Caesars Palace over a misunderstanding involving a sex worker.) But up until the summer of 2018, few of the pro players at Stones thought much of his poker prowess. "He was playing well enough to support himself, it seemed," says Jake Rosenstiel, a Sacramento pro. "But none of us thought Mike was this great poker player."

Everyone was thus surprised when Postle began to dominate the casino's livestreamed Texas Hold 'Em games starting in July 2018. The once middling Postle suddenly turned formidable, even taking thousands of dollars off some big-time players during their swings through Northern California. (Stones is not ordinarily a mecca for high rollers, but its popular livestreamed games occasionally

BRENDAN I. KOERNER *(@brendankoerner) is a contributing editor for* WIRED *and author, most recently, of* The Skies Belong to Us: Love and Terror in the Golden Age of Hijacking.

→VERONICA BRILL FELT OBLIGED TO GO PUBLIC WITH HER SUSPICIONS.

draw big names from Las Vegas and points south.) As Postle's heater stretched over months, Stones' broadcast team did its best to turn him into a poker celebrity. They created a series of graphics designed to hype his talents: One was a mock book cover that listed Postle as the author of a guide to "crushing souls and running pure"; another showed Postle's face superimposed over that of Jesus.

Brill, a self-described analytics geek whose day job is building medical software, was among those who got clobbered by Postle at the table, and she served as a livestream commentator during much of his streak too. By early 2019, she had seen enough to surmise that Postle's success didn't make mathematical sense. She thought he was winning far too often, particularly for a player whose strategy didn't jibe with game theory optimal, or GTO, the prevailing strategy in Texas Hold 'Em today.

The fundamental idea behind GTO is that there's a single best decision for every imaginable betting scenario—a decision that will maximize a player's winnings over time. In any given hand, a player who perfectly executes game theory optimal may still lose; there's only so much you can do if your opponent lucks into the nuts. But in the course of thousands of hours of poker, a player who adheres to GTO at every moment is virtually guaranteed to come out ahead.

Tremendous effort is required to develop the ability to know which single move to make in the millions of possible betting situations. There are 2,598,960 possible hands in five-card poker, a figure that vastly understates the game's intricacy. Players must also have a feel for how their opponents are likely to react to each gambit. To hone their GTO chops, top pros spend hours a day analyzing past hands with software that pinpoints the precise moments when they flubbed a probability calculation.

Brill could detect no trace of such a cerebral approach to poker in Postle's game. Time and again he made decisions that seemed to fly in the face of game theory optimal. The biggest oddity that stood out to Brill was the high rate at which Postle stayed in games prior to the flop, as measured by a statistic called "voluntarily put in pot," or VPIP. Postle often stuck around with hole cards that would lead most elite players to fold. But he rarely seemed to be punished for his audacity, and Brill thought this might be because he was operating with more complete information than anyone else at the table.

In March 2019, Brill approached Stones' tournament director, Justin Kuraitis, and shared her concerns about Postle. The table used for Stones' livestreamed games is embedded with RFID sensors that scan the hole cards and pipe that information into the livestream. Brill wondered whether there was any way Postle could be peeking at that data, even though the stream is broadcast on a 30-minute delay to prevent cheating.

Kuraitis dismissed Brill's inquiry as ridiculous. "Justin insists Stones is 100% secure and there is zero chance of cheating," Brill texted a friend who asked about the conversation. She added that Kuraitis said that most players simply failed to grasp Postle's brilliance.

Brill was not the only skeptic to confide in Kuraitis that month. On March 13, Kuraitis texted a pro named Kasey Mills to invite her to play in a livestreamed game. Mills asked whether Postle would be there, and then opened up about her misgivings. "I have concerns he may have found a way to cheat somehow," she wrote. "Or else he is a god which is very probable … I've just never

PHOTOGRAPH / CHRISTIE HEMM KLOK

seen anything close to what happens to him and it can't help but draw questions." Kuraitis assured Mills that he conducted quarterly security audits, and that "game fairness is one of my highest priorities." (Mills declined the invitation, but she continued to play against Postle in the months that followed.)

By the late summer, however, there were so many whispers about Postle that his rivals were no longer content to take Kuraitis at his word. Rosenstiel, the Sacramento pro, says he approached the casino's management and proposed they look for potential security flaws that Postle might be taking advantage of. But management refused, assuring him there was no truth to the cheating rumors.

By blurting out her suspicions on the September 21 livestream, Brill had ensured that the buzz about Postle would intensify. She now felt obliged to detail her allegations in public. She didn't anticipate that doing so would make her persona non grata at Stones.

POSTLE BECAME SUCH A POKER FORCE THAT PEOPLE TOOK TO CALLING HIM THE MESSIAH AND EVEN GOD.

→**ON SEPTEMBER 28,** Postle became aware of a story making the rounds on poker Twitter. Shortly before noon that day, Brill had posted an 18-minute video that contained clips of Postle's most unusual hands. "Am I sure that this player is cheating? No," Brill wrote in an accompanying series of tweets. "Do I think that there is a greater than zero % chance that he is? Yes ... I feel that with such a high VPIP and play style, if we run the SIM a hundred times with players of equal competency he's running in the 95th percentile of results." Brill added that even though cell phones were banned at some point, she thought Postle might still be receiving signals, perhaps through "a small device on his leg that lets him know when he's ahead."

By evening, Postle's phone was blowing up with messages and calls from worried friends. "I asked him directly, 'Mike, did you cheat in our game?'" says Joe Blackwell, a poker host who worked the September 21 game. "And he said, 'No, Joe, I respect you too much for anything like that. I would never cheat anybody in this or any other game.' And I believed him."

After a sleepless night, Postle sent a long and rambling text to Brill. He blasted her for going public instead of coming to him to discuss the matter privately, and he wrote several hundred words in defense of his poker skills. "I played against and consistently beat some of the best players in the world," he claimed. "I profited over 2 million online from summer of 2003 until the beginning of 2008." He could not believe that Brill, a person who'd never been anything but nice to him, "would betray me like this and throw me to the wolves of public opinion."

Postle was hardly the only person to criticize Brill after her video went viral. She was roundly scolded for presenting a purely circumstantial case against Postle. In poker, it's sacrilege to accuse a peer of cheating without airtight proof. And all Brill had done was offer a speculative hypothesis based solely on math. "I told her, 'You're not providing enough evidence,'" says Matthew Berkey, a well-known pro who has earned more than $4 million during his career. "In this game, trust and your word and your morality is currency ... So I kind of warned her that, hey, you're going to get a lot of backlash for this."

That backlash quickly turned vicious. On October 2, a player on Twitter launched a particularly cruel attack on Brill, one that made her curl up on the floor of her Santa Clara condo and cry. Brill, the author stated with poor punctuation, "couldn't wait for her own baby to die how sick is that."

→**GROWING UP IN** Edmonton in the 1980s, Brill was always slightly embarrassed by her parents' struggle to assimilate to Canadian culture. The family had fled communist Poland when Veronica was 6, and they'd lived in an Austrian refugee camp before moving to Canada. Though he possessed an advanced degree in engineering, Veronica's father had to work as a janitor in his new homeland. He and Veronica's mother both worked punishing hours and refused to treat themselves to even small luxuries.

When she was old enough to take charge of her own social life, Brill indulged her yen to perform: In her twenties she competed in beauty pageants and spun hip hop at Edmonton clubs as DJ Lady V. She took a meandering route through university and became a licensed practical nurse, an occupation that enabled her to buy her first home at 28. (She later became an RN.) The place came with a broken satellite dish that picked up three channels, one of which showed British poker nonstop. To her surprise, Brill found herself glued to these games into the wee hours each night. She was captivated not just by the mathematical intricacies of the action but also by the players' attitude toward money. "Growing up so poor, my parents pinched every single penny," Brill says. "I watched poker players take their money and turn it into a tool. They were able to separate themselves from that monetary value, and they were able to grow this chip stack and use it as a tool and then invest in themselves."

After seeing a boyfriend lose entire weekends to poker, Brill was inspired to teach herself the game through trial and error at a casino in a West Edmonton mall. Soon she was trouncing the well-paid roughnecks who traveled down from the Fort McMurray oil fields with thousands of dollars to burn. She'd then take her winnings to Las Vegas and lose it all to stronger players—the price a poker novice must pay to get better at their craft.

In 2008, Brill moved to Del Rio, Texas, to marry a US Air Force fighter pilot she'd met while he was taking part in a training exercise in Alberta. Four years later, the couple relocated to Sacramento when her husband was promoted to fly U-2 spy planes out of a nearby base. Though she had little professional experience outside nursing, Brill convinced a local hospital system to hire her for an IT job. She was put in charge of building software that streamlines how medical orders are processed. The new career sparked a deeper interest in advanced analytics, and in 2013 she began pursuing an online master's degree in predictive ana-


$5000
5000

lytics from Northwestern University. At the time she was several months pregnant with her first child, a boy due to be born that June.

Brill's life was transformed by the arrival of her son, David, whose genetic luck could scarcely have been worse. The infant boy had lissencephaly, a rare disorder that caused him to have frequent seizures. Brill devoted herself to caring for David, who doctors said was unlikely to survive until his first birthday. On the infrequent occasions she was able to leave the house, she headed for local casinos where she could lose herself in the rigid logic of Texas Hold 'Em. Stones Gambling Hall became her favorite haunt.

Brill noticed that Stones, which had opened in July 2014, was trying to boost its visibility by livestreaming its most competitive games. If Stones could build a digital audience, top pros would be more likely to play at the casino and sing its praises on social media. That publicity, in turn, would lure more amateur players—the so-called fish who are the lifeblood of poker rooms in California, which earn their money by taking a cut from every game.

The gregarious Brill cajoled Stones into letting her host a monthly livestreamed game. She proved to be such a magnetic presence at the table that Stones asked her to work as a regular commentator for other games. Brill was a natural, adept at alternating between ribald jokes and deft observations. Few at the casino knew how much she was struggling with her son's illness, or what an alarming amount of red wine she was consuming to cope. "Stones became my one place I could go to not feel any pain," she says, "or just to numb it for a little bit."

David made it to his third birthday and seemed to be thriving, but then a devastating complication arose: He was diagnosed with an aggressive form of cancer, leading to his death in December 2016. Brill's marriage soon failed, a casualty of the couple's overwhelming grief. Desperate for some form of solace, she retreated ever deeper into the booze-soaked poker scene at Stones.

→ **ON OCTOBER 1,** as Brill was about to be savaged as a monster who'd neglected her dying son, one of poker's biggest names was busy rallying to her cause. Joey Ingram, a well-known player and host of the *Poker Life* podcast, had taken a keen interest in the video Brill had assembled of Postle's questionable hands. He had experience doing quasi-journalistic investigations of poker scandals—in 2018 he accused a Costa Rican poker website of using bots to undermine its human users. But he'd never heard of shenanigans in a live game streamed from a brick-and-mortar casino where thousands of people watch the players' every move.

Ingram doubted there was anything to Brill's story, but he decided to check out a year-old game on Stones' YouTube channel. Before long he was deep down the Mike Postle rabbit hole, reviewing hours of Texas Hold 'Em footage in lieu of eating or sleeping. "I watched every hand he played. The guy's running and gunning and making these amazing plays, amazing bluffs," Ingram says. "I watched four sessions that first night, and it was the same thing in all four sessions. And I'm like, something's really messed up here."

Around 4 am on October 1, Ingram began to livestream himself evaluating Postle's old games at Stones. For five hours he narrated hands, noting each time Postle made moves that seemed bizarre but still led to wins or minimized losses. He also noted that Postle had a habit of staring down at his lap—the place where he happened to keep his cell phone during games. "I was like, all right, he's looking at his crotch and he seems to be playing like he's a god," Ingram says.

Ingram's livestream was such a hit that he followed it up with another extended session the next day. Tens of thousands of poker aficionados tuned in, captivated not just by the brazenness of the alleged offenses but also by the implications it held for the poker industry at large. According to many poker observers, Postle's supposed deceit had only come to light because he'd gotten greedy and neglected to cover his tracks by occasionally losing on purpose. That meant smarter cheaters might be flying under the radar by keeping their win percentages from getting suspiciously high. "It's like when Sammy Sosa got caught—he wasn't the only one with a corked bat," says Jonathan Sofen, a poker journalist and semipro player. "Or the Houston Astros—they aren't the only ones who cheated in baseball."

Ingram's fans soon began to inundate poker forums with their own investigative work. A thread on a site called Two Plus Two quickly grew to hundreds of pages long, and its contributors posted spreadsheets and graphs that purported to show that Postle had won money in upwards of 86 percent of the Stones livestreamed games he'd taken part in—an accomplishment that should be next to impossible given the mathematical strictures of Texas Hold 'Em.

The amateur detectives also highlighted several moments and visual details they claimed to be telltale signs of Postle's chicanery. They pointed to a clip from one game, for example, in which Postle appeared to resweep his hole cards over an RFID sensor because they hadn't registered. How, the sleuths asked, would Postle have known to do that unless he had access to the livestream? And was there a bulge beneath his omnipresent baseball cap that might be some sort of bone-conduction headphone, a receiver for inside information?

The crowdsourced investigation caught the attention of Scott Van Pelt, an anchor on ESPN's *SportsCenter*. On the night of October 3, Van Pelt spent three and a half minutes discussing the drama at Stones, and he made clear where his sympathies lay. "If you were this good, why would you be playing in games only with a videofeed at $1/$3 tables at Stones' poker room?" he asked as he wrapped the segment. "Why wouldn't you be in Vegas winning all the money in the world?"

With public opinion turning against him, Postle sought to seize back control of the narrative. He agreed to appear on an October 4 podcast hosted by Mike "The Mouth" Matusow. Sounding groggy and disjointed, Postle pleaded his innocence and argued that he'd been targeted by opponents who envied his minor fame: "There was a secret hatred for me for being made into, I guess, what you would compare to a reality TV star."

When Matusow invited his guest to refute the accusations, Postle replied in vague terms. "There aren't words to describe what I do," he said. "It's creative, diabolical, and predicated on having an MO of always trying to be the most unpredictable player at the table … There's no book or anything out there that can explain what I do."

The interview did little to quell the poker world's growing belief that Postle was guilty as charged. Strangers started showing up at his house, in a subdivision near Stones; they would bang on his door at odd hours and threaten him with violence. Postle began to worry not just about the future of the only career he'd ever known, but also about the safety of his 8-year-old daughter.

→ **EVEN AS A CHILD** in Wisconsin, gambling was central to Mike Postle's life. Games he played with his five siblings often involved a wager—when they played Monopoly, for example, real money changed hands. Postle also invented games of skill and chance, including a prize wheel that he installed at the roller rink his father owned. Kids would pay 50 cents a spin for a chance to hit the $5 jackpot. But as Andrew Postle, one of Mike's brothers, recounted on a Stones livestream in August 2019, the game was rigged. "My brother put some quarters behind the wheel so when you spun it, you'd always get so close to the $5 bill," he told one of the evening's commentators. "If there's an angle for my brother to do it, he'll do it."

When he turned 18, as Andrew recalled, Postle got a job at one of the Indian casinos near his home. He started out making change for customers before becoming a dealer, a gig that deepened his interest in poker. In the early 2000s he moved south to work in the casinos of Tunica, Mississippi, a poker hotbed. He soon found that, given his natural analytical gifts, he could make more money as a player than a dealer. By mid-decade, he was winning big tournaments. In one he claimed nearly $120,000 in prize money. "He was ahead of the curve back then," says Michael Weyer, who came in second to Postle in a 2005 tournament. "He didn't amass that amount of chips by being a dummy."

While riding high in Tunica, Postle joined the masthead of a poker magazine called *Rounder Life*. He wound up dating one of the models featured in the publication, the Las Vegas–born daughter of a professional bowler. When she became pregnant in 2010, the couple moved to Sacramento so Postle's parents, who had relocated there, could help take care of the child. A year after giving birth, Postle's girlfriend told him she'd been diagnosed with a brain tumor that required a risky operation, and that she wanted to get married before she died. Two days after the couple's hasty wedding in December 2011, Postle's now wife had her supposed surgery; for months afterward, she wore bandages on her head and spoke of undergoing follow-up radiation treatments that her husband was not allowed to attend.

But the brain tumor story was a lie: An MRI taken just over a week before her "surgery" showed that her brain was normal. Before Postle became aware of how thoroughly he'd been fooled, he also learned that his wife was struggling with serious mental health and substance abuse issues. The couple tried to work out their problems in therapy, but the marriage was doomed: Postle filed for an annulment in December 2015. (Postle's ex-wife, who has changed her name and is now engaged, told me she regrets some of the ways she acted while drinking to excess during the marriage. She describes her relationship with Postle as "toxic" and says that, toward the end, she was desperate to get "out of the gambling lifestyle.")

An ugly custody dispute ensued, filled with restraining orders and accusations of domestic violence on both sides. In 2016, Postle's soon-to-be ex-wife took their daughter to Idaho to live with her new boyfriend. Postle spent a small fortune to press for his daughter's return—a financial burden in the best of times, but one that he must have felt even more acutely because his career was on the downswing. In the years since his move to California, poker had been overtaken by studious practitioners of game theory optimal, some of whom hold science and engineering degrees. Less scholarly players like Postle found themselves eking out a living at low-stakes tables. "The past five or six years, you have to constantly be improving your game, otherwise you lose," says Jonathan Sofen, the poker journalist. "Everybody today, they're studying game theory optimal, they're watching training videos and reading books. The field of players who don't study? They've mostly gone broke."

> "STONES BECAME MY ONE PLACE I COULD GO TO NOT FEEL ANY PAIN, OR JUST TO NUMB IT."

Postle was still tangling with his ex-wife in family court when his heater at Stones began in July 2018. His winnings came in handy as he continued paying legal fees. Over the next several months, to Postle's relief, the courts agreed he could have sole physical custody of his daughter, and his ex-wife was granted unsupervised visits. After nearly a decade of heartache and hard luck, all seemed to be going right in Postle's world.

→ **AS THE STONES** scandal gained national attention in October 2019, the conventional wisdom held that Postle's results were so anomalous that something hinky must have occurred. But there was still a giant hole in the case against "God": How could he have gotten his opponents' hole-card information in real time?

The man best equipped to answer that question was an Australian named Andrew Milner, the inventor of the RFID-equipped table that makes livestreamed poker possible. A former IT worker who plays Texas Hold 'Em as a hobby, Milner cobbled together his first table in 2008 with an eye toward using it as a training tool. But he found there was a huge demand from casinos, which sought a low-cost way to reveal hole cards to spectators so they could broadcast games via the internet.

Justin Kuraitis, Stones' tournament director, called Milner in October and asked whether the RFID table had vulnerabilities that Postle could have exploited. Milner all but ruled out a theory that Postle might have tapped into the signal that's relayed from the table's sensors to the room that serves as the casino's broadcast center: That data is encrypted using the same technology employed by online banks, and it seemed unlikely that Postle had the technical skill to overcome such strong security. Milner did think it possible that Postle had installed a tiny webcam on the wall of the broadcast center, pointed at a PC screen that showed the livestream without delay. But the likeliest scenario, he suggested, involved an inside job. "I asked [Kuraitis], do you trust your people?" Milner recalls. "It doesn't matter how secure your environment is, if you can't trust the guys running it, all other measures are irrelevant." (When contacted for this story, Kuraitis' only response was to direct me to a *Rounder Life* story that sug-

gests Brill fabricated the cheating scandal "to become 'a name' in the poker world," a charge she vehemently denies.)

If Postle did have an accomplice at Stones, they would have had little trouble avoiding detection. According to multiple people familiar with how Stones operates, security in the broadcast room was lackadaisical at best. One former contractor told me that he was able to have a masseuse come into the supposedly secure room while he was working on the livestream, and that no one batted an eye. (In a text message exchange with Kasey Mills, Kuraitis says that his rules forbid technicians from even bringing their cell phones into the control room.)

On October 8, the accomplice theory made an appearance in a $30 million federal lawsuit filed by Veronica Brill and ultimately 87 other players—including Mills—who claimed either fraud or negligence by multiple defendants: Stones, Postle, Kuraitis, and an indeterminate number of unnamed collaborators. The plaintiffs' lawyer, Mac VerStandig, is an avid poker player who focuses on casino-related cases. The complaint contended that Postle had won at a clip "not known to have been achieved by any other poker player over such a significant period of time." The document spelled out what VerStandig and his clients believe went down:

> *The Plaintiffs have reason to believe the mechanisms through which these myriad acts of wire fraud were carried out by Mr. Postle, John Does 1-10 and Jane Does 1-10 involved Mr. Postle's cellular telephone being grasped by his left hand while concealed under the poker table and/or Mr. Postle's baseball cap being imbedded* [sic] *with a communications device creating an artificial bulge in its lining (that is notably absent in photographs of the same baseball cap on Mr. Postle when he is not playing on Stones Live Poker).*

VerStandig also wrote that the plaintiffs had "a good faith basis upon which to allege the identity of the person who is John Doe 1," but added that he would prefer to refrain from doing so until the discovery process had run its course.

Stones hired the elite law firm of Boies Schiller Flexner to fight the suit, while Kuraitis retained one of Sacramento's top specialists in white-collar crime. Postle, however, decided to represent himself; according to one of his close friends, this was in large part because he was now broke, despite having won an estimated $250,000 during his heater. (Postle has said he earned just $80,000 from the winning streak, and that his accusers have erroneously included chips he bought or loans repaid by fellow players.)

As the legal pressure mounted, the dwindling number of people from the Stones scene who'd stayed in touch with Postle worried that he was buckling under the stress.

→ I MADE NUMEROUS attempts to get in touch with Postle this past winter, including by visiting his home. I could tell right away the place was in rough shape. There was a downed tree in the overgrown front yard, the knob on the security door was loose, and the bent second-floor blinds were shut tight. I thought I heard a slight commotion when I rang the bell, but no one ever answered.

On March 7, Postle finally returned one of my many calls. He said he was at the airport on his way to Florida, where he planned to stay for an indeterminate amount of time. Though he declined to address the specific allegations against him, he did tell me that his appetite for poker had largely vanished, and that he'd instead been focusing on spending time with his daughter. He also railed against poker vloggers and social media figures for attacking him for their own cynical, money-grubbing motives. "I didn't really understand the whole fake-news manipulation that happens for the sake of a story until this happened," he said. "More or less all of the information that's out there? Honestly, none

of it's true. The exaggeration, the manipulation? It's just sickening."

In the weeks that followed, Postle promised to respond to a list of written questions about his past, and then apologized multiple times for blowing our agreed-upon deadline for his answers. After a while he stopped bothering to make excuses and fell silent.

Postle finally piped up again on June 4, a day after he'd received some welcome news: The federal court in California had granted Stones' motion to dismiss, largely on the grounds that California's gambling laws generally do not make poker losses recoverable through civil action. The judge left open an opportunity for VerStandig to refile if he could provide more information about how much money Stones had collected from the affected games, but Postle was in the clear. (At the time, Postle was still a defendant in a separate $250,000 lawsuit filed in Nevada by Marle Cordeiro, the player whom he folded against during Brill's last broadcast at Stones. The Nevada court dismissed that case on August 14, citing its lack of jurisdiction in California.)

Postle did not seem to be in a jubilant mood when he reached me by text after his June legal victory. "Veronica is a toxic pathological liar who has proven narcissistic and sociopathic traits and has really gone off the deep end recently," he wrote, citing no evidence. He seemed convinced that Brill had concocted the charges against him to build her following on YouTube, where she was still posting videos about the case. Postle later apologized for his invective but declined to speak any further, stating that he'd only be able to reveal all once he was no longer in legal jeopardy: "I'll be able to give not just the truth, but the shocking events of everything in detail ... with the corresponding truth to corroborate it."

I did not hear from Postle again until mid-August, when he called to request that I delay publication of this story. I said I might be amenable to doing so if he could finally share some evidence to back up his assertion that Brill had plotted against him. After talking in circles for a while, Postle said he'd check with a lawyer and get back to me. In the end he didn't send anything. He also declined repeated requests to answer detailed fact-checking questions for this article.

→ **VERONICA BRILL** was bewildered by the dismissal of the federal lawsuit in California. "You can cheat on live TV and get away with it," she told me just minutes after learning of the judge's ruling. "So frustrating. It's not the money, per se. It's the lack of accountability."

Several weeks later, Brill received another bit of disconcerting news: Rather than refile an amended complaint, VerStandig asked her and the other plaintiffs to accept a settlement from Stones. Brill refused when she learned that, in exchange for a paltry sum, she would have to sign a public statement conceding there was "no forensic evidence that there was cheating at Stones." (In a statement to WIRED, a Stones representative emphasized that plaintiffs who settled would have to acknowledge that both the casino and Kuraitis "were not involved if there was any cheating by Postle.")

In the wake of the dissolution of her legal case, Brill began receiving a torrent of abuse from anonymous Twitter accounts. "You're a FN idiot!" wrote one user who went by KarmaIsComing4U. "20 years ago we would of beat you ass for even accusing!!!!" (The account has since been deleted.) Brill fears that Postle plans to file a libel suit against her, which she assumes would take her years and her life savings to defend.

But Brill maintains she has no regrets about calling out Postle, an act she now views as part of a subconscious effort to move on from a dark period of her life. Stones was where she'd gone to mask her grief with an unhealthy amount of red wine and gambling; by blowing up her relationship with the casino, she liberated herself. "The game has gotten harder, I haven't been studying as much, and I'm very frustrated because I'm super-competitive," she says. "I'm actually better at analytics, at IT—y'know, everything else that I'm doing—and I'd rather put my time into that, where I can actually make some gains in lifelong terms."

Postle has an opportunity to put the Stones saga behind him, too. Though he says he's intent on marshaling evidence that will prove he's the victim of a grand conspiracy, there is a far simpler way to reclaim his reputation. "How do you prove you're not cheating at poker? You go play poker," Ingram says. "You would imagine that one of the best players you've ever seen in your life would have no issues saying, Let's play then. I can't really figure out an answer to why he won't do that." The livestream audience for God's return would surely be immense.

COLOPHON

Misinformation that helped get this issue out:

Promising to meet that deadline; *Lost Girls & Love Hotels* by Catherine Hanrahan; the magical thinking of expensive skin care products; no one will notice the dented fender, especially not the rental company; management training; that DIY swamp cooler will definitely work; watching Facebook friends thumbs-up the QAnon page (before it was banned); neck gaiters shoot coronavirus straight into other people's lungs; Donutgate; we fact-checkers will vanquish these falsehoods; low-calorie ice cream tastes just like the real thing; my cat and new kitten are totally getting along; dry lightning and hurricane-force wind gusts are very normal weather patterns; everything is going to be fine.

Volume 28, No. 10. WIRED (ISSN 1059–1028) is published monthly, except for the combined July/August issue, 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; Mike Goss, 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@WIRED.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 WIRED.condenet.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 SET IN A WORLD WITHOUT PAPER:

I KEEP LOSING AT ROCK SCISSORS.

Anna Jaruga
via Facebook

Honorable Mentions

THE DOG ATE MY MEMORY CARDS.
IRFAN DARIAN VIA FACEBOOK

HONEY, PASS ME THE NEWS TILE.
@RAINREIDER VIA TWITTER

THESE LEAVES WOULD HAVE TO DO.
@ELIPORTERALTIC VIA TWITTER

CHRISTMAS MORNING WAS NEVER A SURPRISE.
@TONY32938627 VIA TWITTER

I WROTE IT ON THE FRIDGE.
@APOCRYPHAL_X VIA TWITTER

MUSEUM REPORTS THEFT OF TOILET PAPER.
@JOOSTDOUMA VIA TWITTER

THE PEN IS NO LONGER MIGHTIER.
@MDEZIEL VIA TWITTER

POLICE SAY NO NOTE WAS UPLOADED.
@CWYANT VIA INSTAGRAM

Your next assignment:

IN SIX WORDS, WRITE A STORY ABOUT THE NEXT BIG SECURITY LEAK.

Each issue we publish a six-word story—and it could be written by you. Submit your story on Facebook, Twitter, or Instagram, along with **#WIREDBACKPAGE**. We'll pick one to illustrate here.

ILLUSTRATION / VIOLET REED

THE NEW YORKER FESTIVAL

OCTOBER 5–11

Join us this fall for the very first virtual New Yorker Festival, an eclectic mix of conversations, performances, and experiences, featuring some of the most influential and talented figures of our time.

For more information and to purchase tickets, go to newyorker.com/festival.

@NewYorkerFest