
WIRED
MAY 2018
THE YOUNG AND THE RECKLESS
GAME OVER
MICROSOFT
FBI
A gang of teen hackers snatched the keys to Microsoft's videogame empire. Then they went TOO FAR.
By Brendan Koerner
CREATE. CONNECT. CONDÉ NAST


TOMMY HILFIGER
LEWISHAMILTON


TOMMY.COM
Official Team Partner
AMG
PETRONAS
MOTORSPORT

AI needs human-centered design

THE INTELLIGENCE IS NOT IN THE COMPUTER

By Jim Guszcza

Artificial intelligence—software that appears to mimic or exceed human reasoning, rather than simply automating repetitive tasks—is already reshaping business and society. But many large AI projects fail to deliver, and AI algorithms have even been blamed for disrupting society through social media.[1]

The ability of AI applications to automate tasks associated with human intuition is rapidly progressing: facial recognition, driving cars, interpreting speech, writing reports. In many cases, newer forms of AI can perform more accurately than humans. This makes it tempting to conclude that computers "understand" what they are doing. That's an illusion.

AI technology is a tool for human minds, not a mind itself. Human-centered design of AI is crucial, based on realistic conceptions of user needs and human psychological, organizational, and societal factors.

Aspects of Human-Centered AI Design

How does human-centered design make AI effective? There are several ways:

GOAL-RELEVANCE.
Ask Bing, "How big is Poland?" and its answer includes, "About the size of Nevada," an approximation that most people understand, rather than a number they don't.[2]

HANDOFF.
Many AI systems can run on "autopilot" much of the time, but require human intervention in exceptional or ambiguous situations. "The paradox of automation" is that users need to keep on top of their skills, despite delegating them to a machine most of the time.

FEEDBACK LOOPS.
Left alone, AI will do as it is trained, without a sense that it has gone off the rails by misinterpreting user behavior, or being unaware of social boundaries which humans instinctively work within.[3]

PSYCHOLOGICAL IMPACT.
Algorithms designed without a focus on their users' human nature can impair user behavior. Social media, designed to be addictive, is now being looked at as possibly harmful to obsessive users.

Keeping Humans at the Center of AI Design

Visionary researcher John Seely Brown once said, "The technology is the easy part. The hard part is figuring out the social and institutional structures around the technology."

Human-centric AI algorithms should reflect the information, goals, and constraints that a human decision-maker tends to weigh when arriving at a decision. The data should be analyzed from a position of domain and institutional knowledge, and an understanding of the process that generated it. An algorithm's design should anticipate the realities of the environment in which it is to be used. It should be peer-reviewed or audited. It should explain its conclusions: Why does the AI think you have heart disease?

The overall decision *environment* must be similarly well-designed. An algorithm's end users should have a sufficiently detailed understanding of their tool. Guidelines and business rules should be established to convert predictions into prescriptions, and to suggest when and how the end user might either override the algorithm or seek other information.

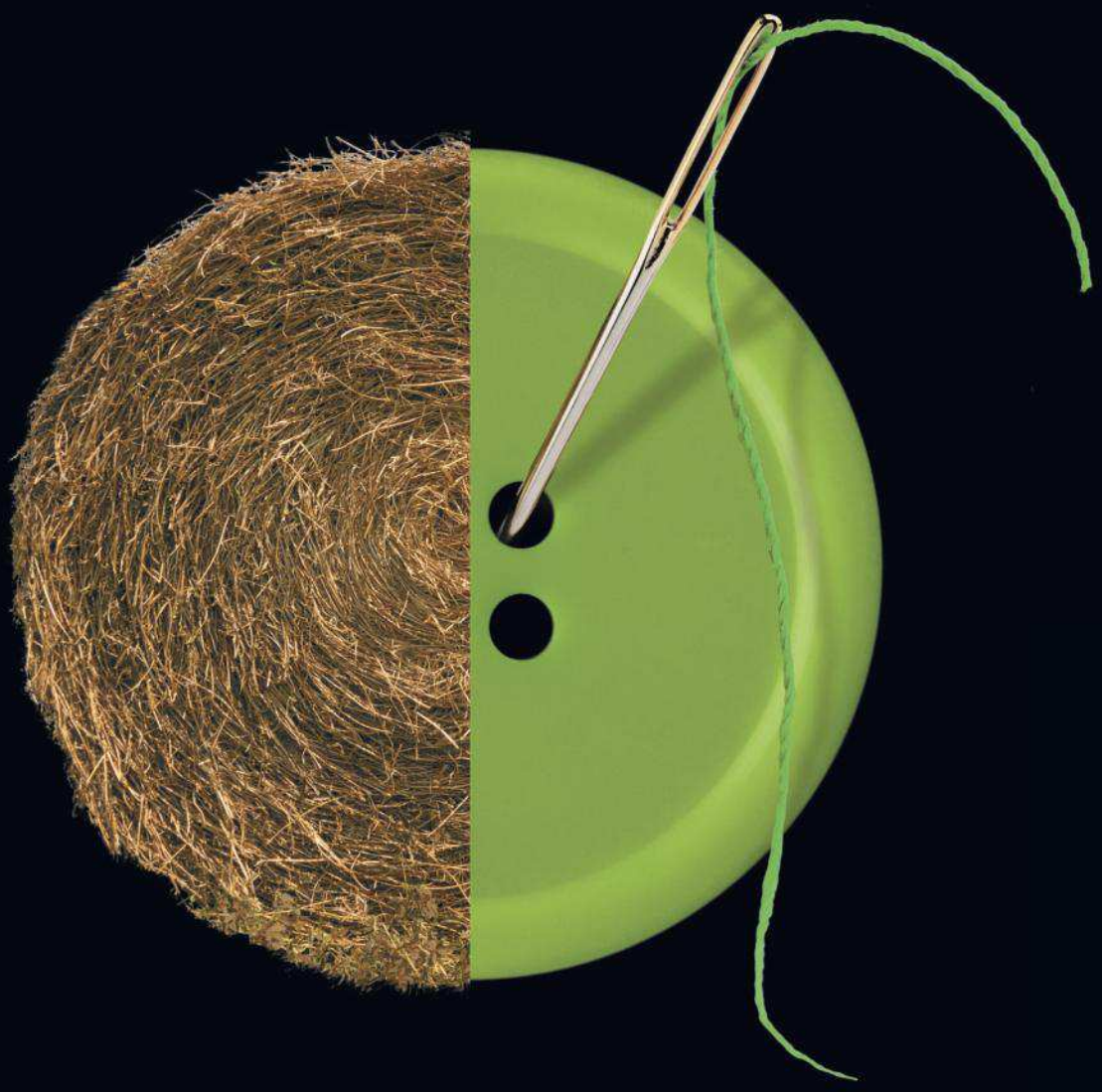
Whether intended for automation or human augmentation, AI systems are more likely to yield economic benefits and societal acceptability if user needs and psychological factors are taken into account. Design can help close the gap between AI algorithm *outputs* and improved human *outcomes* by keeping human needs, behaviors and goals at the center as we build our machines.

Jim Guszcza is the US chief data scientist of Deloitte Consulting LLP.

Read more about artificial intelligence and human design at deloitte.com/insights/ai-human-design

Deloitte.

[1]Matthew Hutson, "Even artificial intelligence can acquire biases against race and gender," *Science*, April 13, 2017; "Fake news: You ain't seen nothing yet," *Economist*, July 1, 2017; Paul Lewis, "'Our minds can be hijacked': The tech insiders who fear a smartphone dystopia," *Guardian*, October 6, 2017; Holly B. Shakya and Nicholas A. Christakis, "A new, more rigorous study confirms: The more you use Facebook, the worse you feel," *Harvard Business Review*, April 10, 2017. [2]This is the result of work led by cognitive scientists Dan Goldstein and Jake Hoffman on helping people better grasp large numbers (see Elizabeth Landau, "How to understand extreme numbers," *Nautilus*, February 17, 2017). [3]Many examples of algorithmic bias are discussed in April Glaser, "Who trained your AI?," *Slate*, October 24, 2017.



Cognitive tools see the needle you can't find

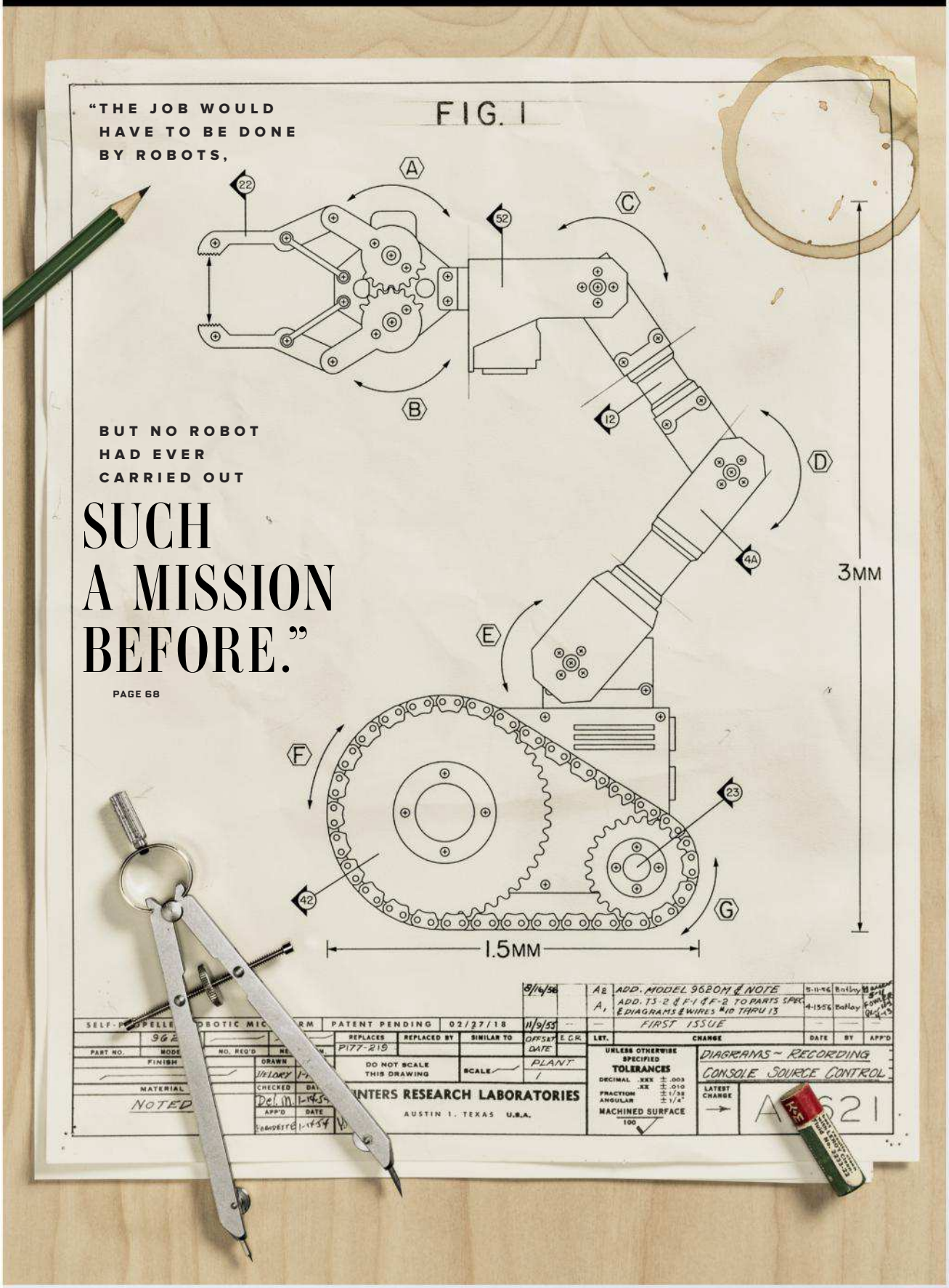
Finding what matters in big data can be daunting. But look again. Deloitte sees how new tools like robotic process automation and artificial intelligence can help clients sift through data fast and uncover insights that lead to stronger business outcomes.

Look again.™ See what insight can solve.

Copyright © 2018 Deloitte Development LLC. All rights reserved.

Deloitte.


R/EVOLUTION
AN ENTIRELY NEW CLASS OF YACHT
PRINCESS YACHTS PRESENT A CRAFT FILMS PRODUCTION R/EVOLUTION STARRING THE ALL-NEW R35
TECHNICAL PARTNER BAR TECHNOLOGIES MANUFACTURED BY PRINCESS YACHTS LIMITED
STYLING BY THE PRINCESS DESIGN STUDIO IN COLLABORATION WITH PININFARINA POWERED BY VOLVO PENTA
ART DIRECTION JAUME VILARDELL & BSUR SOUNDTRACK GANDO & DR K'S 'REFOOLUTION' ANIMATION BREAKFAST OF CHAMPIONS
10.09.2018
AFS
ACTIVE FOIL SYSTEM
#EXPERIENCETHEREVOLUTION
PRINCESSYACHTS.COM
PRINCESS
CRAFTED IN PLYMOUTH, ENGLAND



"THE JOB WOULD HAVE TO BE DONE BY ROBOTS,

BUT NO ROBOT HAD EVER CARRIED OUT

SUCH A MISSION BEFORE."

PAGE 68

REBEL, REBEL

Introducing the Uptown Maverick. Like a well-worn leather jacket, this street boot feels as good as it looks. With a light, springy sole for a cushioned ride, you're ready to zip up and step out.

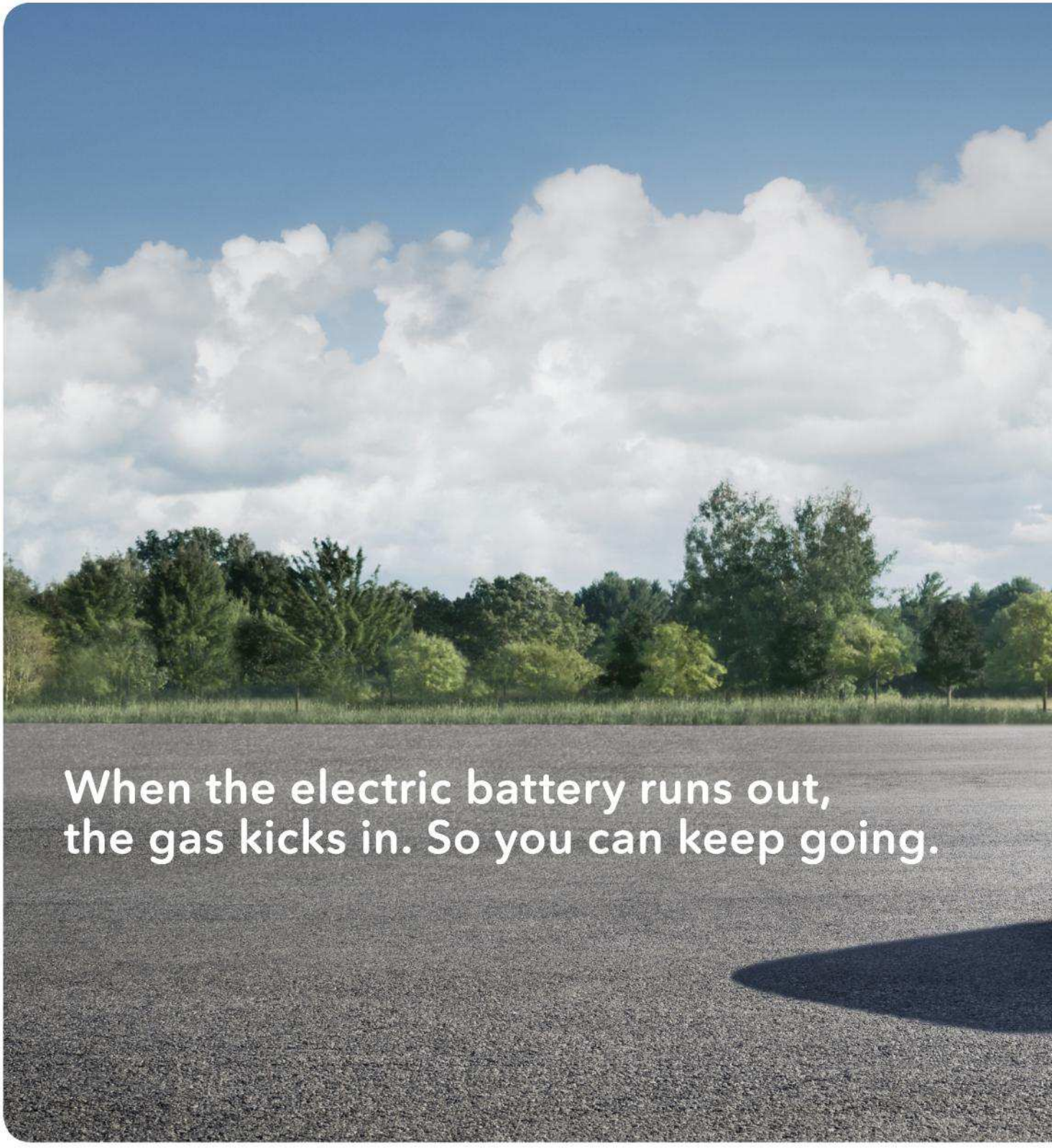
SAMUELHUBBARD.COM

SHOEMAKERS SINCE 1930

Free shipping and returns. Order online or call 844.482.4800.

A technician demonstrates a 3-D Holo Stage, a virtual space where engineers can plan routes for robots venturing into the ruined Fukushima nuclear plant.

SPENCER LOWELL


When the electric battery runs out,
the gas kicks in. So you can keep going.

Introducing the all-new Clarity Plug-In Hybrid.

The Plug-In Hybrid – the latest in the Clarity Electrification Series – has an all-electric range rating of 47 miles.* And it also has a gas-powered engine. For a combined range rating of 340 miles.*

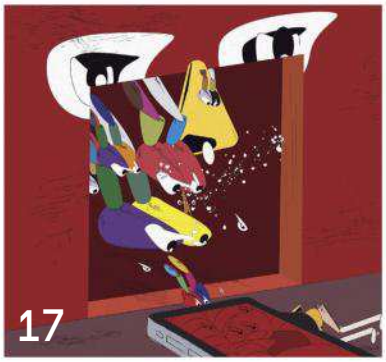
clarity.honda.com

*47-mile maximum EV mode driving-range rating. 340-mile combined gas-electric driving-range rating. Ratings determined by EPA. Use for comparison purposes only. Your driving range will vary depending on driving conditions, how you drive and maintain your vehicle, battery-pack age/condition and other factors. ©2018 American Honda Motor Co., Inc.

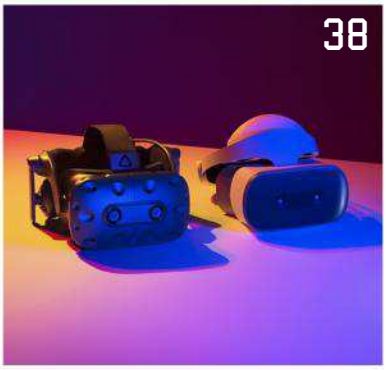
HONDA

26.05

ALPHA



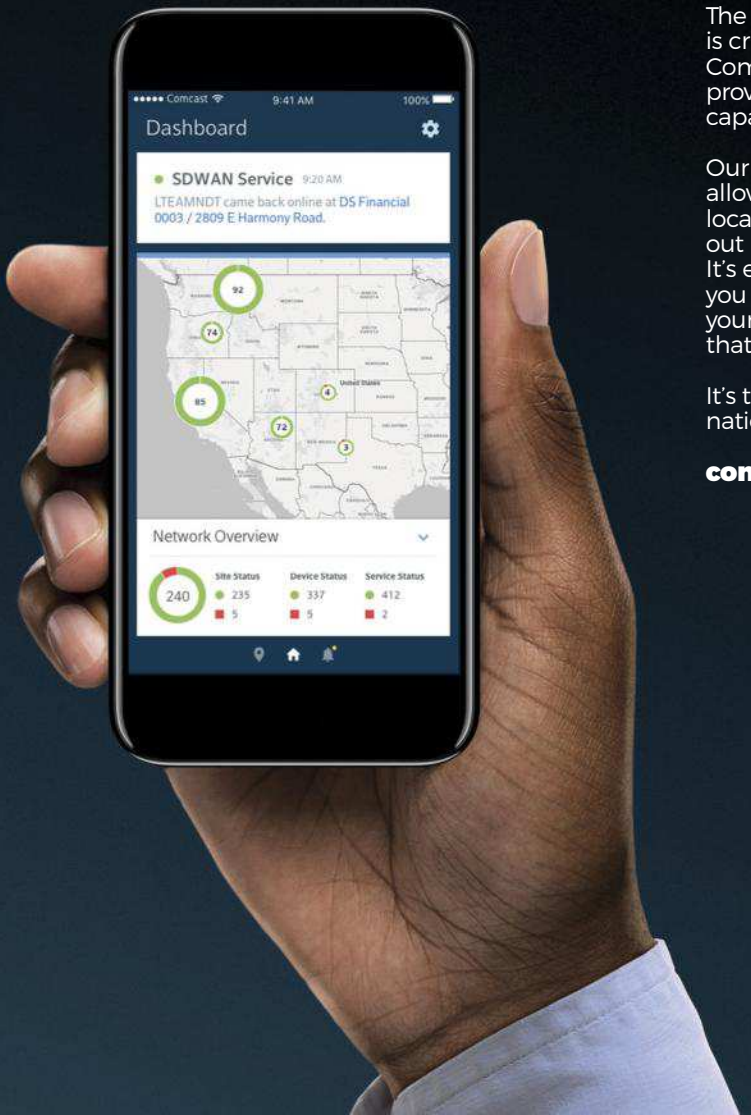
GADGET LAB



SIX BY SIX

ON THE COVER
Illustrated for WIRED by Zohar Lazar.

A BUSINESS IS ONLY AS STRONG AS ITS WEAKEST LOCATION.



The performance of every one of your remote locations is critical to the success of your business. That's why Comcast Business has built network solutions that provide your entire distributed enterprise with the same capabilities as HQ.

Our ActiveCore℠ Platform with its SD-WAN solution allows you to manage your network across all your locations effortlessly, reduce hardware costs, and roll out new capabilities everywhere in minutes vs. months. It's enabled by a leading-edge mobile app that lets you monitor your entire network from the palm of your hand. Also, our advanced Voice solutions mean that you and your employees never miss a call.

It's time to bring all your locations up to speed on the nation's largest Gig-speed network.

comcastbusiness.com/distributed-enterprise

COMCAST BUSINESS

OUTMANEUVER

Restrictions apply. May not be available in your area.
Actual speeds vary. ©2018 Comcast. All rights reserved.

Spencer Lowell says photographing the inside of a nuclear reactor was "one of the highlights of my career."

NUCLEAR WITNESS

What's it like to be inside a nuclear reactor? LA-based photographer **Spencer Lowell** found out when he visited the site of the 2011 meltdown in Fukushima, Japan (page 68). In a full Tyvek suit, gloves, and mask, Lowell stood beneath a massive steel structure where fission reactions once took place. "It was surreal," he says. "It's generally something that you don't even get to go near, never mind go inside." The enormity of the reactor, and the eerie emptiness of the surrounding towns, left Lowell awed by the monumental catastrophe. "I've always been a proponent of nuclear energy," he says. "But you see something like this, and you question whether it's really worth it."

Get More WIRED

We launched a paywall on WIRED.com, but if you're already a print subscriber, don't worry: You can authenticate your subscription and read all of our stories, ad-free. Get the hookup here: **wired.com/register.**

When Brooklyn-based writer **Amanda Schaffer** first learned that a startup was conducting rogue clinical trials for a herpes vaccine on the Caribbean island of Saint Kitts, she was curious: "I wanted to understand people who would fly out of the country and take a chance on a treatment that the FDA had no part of." The scientist behind the trial was a tenured professor at Southern Illinois University, so why do research off the books? "How could someone with a conventional track record and seemingly good intentions reach a point where he was experimenting on people with no formal oversight?" she wondered. Find out in "Infectious" on page 86.

Contributing editor **Brendan I. Koerner** has covered the hacking of slot machines, the hacking of the US Office of Personnel Management, and the (figurative) hacking of young American minds by ISIS recruiters. When Koerner read about a foreigner convicted of hacking into US businesses to steal trade secrets (gaming companies, in this case), he tracked down David Pokora, the young Canadian behind the scheme. Pokora was being held in a New Jersey detention facility at the time, and it took two years to convince him to open up. "I was intrigued by the fact that he's incredibly gifted and talented and had gone down a rabbit hole of negativity that cost him a lot," Koerner says. Read his story on page 46.

Senior writer **Jessi Hempel** has spent the past 15 years covering Silicon Valley from an unorthodox location: New York. After moving there from San Francisco in 2003, Hempel got a job covering tech after the dotcom crash. "When you're watching from someplace else, you realize what's weird and what's normal about the Valley," she says. Hempel's reporting has run the gamut, from profiling a secretary of defense intent on wooing tech firms to exploring the new world of ride-hailing services. On page 60, she reports on the efforts of Uber's new CEO, Dara Khosrowshahi, to push past a year of scandal and atone for the company's recent failings. "I followed this story at every turn because it was basically the soap opera of 2017," she says.

PHOTOGRAPHS BY DENNIS POTAMI (SCHAFFER); FLORENCE PAK (HEMPEL); WILL STAR (KOERNER)

for the love of all things sparkling.

vapor-distilled for purity.
electrolytes for taste.

© 2018 glacéau. glacéau®, smartwater® and label are registered trademarks of glacéau.

ARE ALL EXPERTS WORTH BELIEVING?

MAGAZINE MEDIA

Better. Believe It.

When it comes to influencers, magazine editors are the originals. No one knows their stuff—or YOU—better. Their authentic, authoritative content makes magazine media more trusted than any other. No wonder its print, online, mobile and video audience has grown to 1.8 billion.

Experts you can trust. That's something to believe in.

#BelieveMagMedia | BelieveMagMedia.com

Sources: MPA, Total (Duplicated) Magazine Media 360° Audience, Jan-May YTD 2017, Brand Audience Report; Simmons Research, Multi-Media Engagement Study, Spring 2016.

ARGUMENT

TEAM OF RIVALS

WE ARE ALL SOLDIERS IN THE WAR AGAINST OURSELVES

BY VIRGINIA HEFFERNAN

OVER THE PAST three years, America's information ecosystem has proven easy pickings for anyone with a fistful of VPN connections and a sweatshop of kids playing World of Trollcraft. Whatever precise effects Russian interference had on the 2016 election, it finished off both social media's innocence and traditional media's authority.

But Americans, as of now, have nowhere else to turn. The habits of the library and the newsstand, to say nothing of pre-digital social life, are lost to us. Instead, we're stalled in the data smog that hangs over social media and search engines. Sometimes we confront trolls, bots, phish, spam, and malware head-on; sometimes we meet trollspeak in memes parroted by real people. But the sanctity of our reason

MAY ALPHA THEME: HYBRIDS

Car-subscription apps, tech-fortified food, AI-composed music, massive Marvel mashup, Crispr factory, and more.

is routinely violated online.

In rolling revelations all winter, Facebook and other tech companies admitted that potentially hundreds of millions of users had been tricked by data miners and harassed by trolls, including legions at the Internet Research Agency, the Russian outfit indicted by the Justice Department in February. That sounds like a cause for condolences. But trolled people troll people. Many victims turn around and enlist as foot soldiers, passing on their cognitive injuries to others. "Computational propaganda," as the human-machine hybrid campaigns are known, has been described as a way of "hacking people."

This damage to our brains is overdetermined. First, the crime is in the software. As WIRED's own Adam Rogers predicted in 2015, "Google's search algorithm"—with zero help from bad actors—"could steal the presidency." But digitization has also simply overwhelmed us. The journalist Craig Silverman put it this way: "Our human faculties for sense-making, and evaluating and validating information, are being challenged and in some ways destroyed." And the information war includes seasoned generals, including Yevgeny Prigozhin (a restaurateur, b. 1961 in Leningrad) and Mikhail Bystrov (a cop, said to be in his late fifties). These two men ran the IRA and deftly exploited America's mental vulnerabilities, flammable culture, and opportunistic software.

The weapons are hybrids too. According to reports in March, Cambridge Analytica, the data firm employed by the Trump campaign, launched disinformation scripts and bulk *provokatsiya*. IRA did the same, but it also conscripted real people. Some of these are partisans, or freestyling trolls. But a smaller group willingly subjugate themselves to specific infowar efforts. In January, a woman in South Carolina—a cheerful-looking phytocannabinoid seller in her mid-sixties—seems to have mobilized her #MAGA-festooned Twitter account to promote a Nunes-supporting meme: "Release the memo." "Make this trend," she implored. Trend it did.

Computational propaganda, which describes human-machine collaboration in influence ops, was coined at the Oxford Internet Institute at Balliol College, Oxford. (Balliol was founded in 1263, the year King James I of Aragon aimed to sabotage significant information channels by censoring Hebrew writing.) The phrase describes the mixing of algorithms, automation, and human curation to manipulate perceptions, affect cognition, and influence behavior.

That human curation is key. People can whitewash buggy botspeak by giving it a human sheen in a retweet. Curators can also identify the cultural flash points—the NFL, Colin Kaepernick, the memo—that fire people up, so botnets can ratchet up the velocity of the most incendiary memes. The writer Jamelle Bouie points out that, in the US, these "flash points" often entail racism. It takes an American idiom *and* id to properly troll the electorate.

Samantha Bradshaw, at the Oxford Internet Institute, recently documented the ways that 28 nations have used social media to shape opinion. In every case, the campaigns aimed to ape the style and habits of actual activists, and they caught on to the degree that seemed human. The content didn't need to be accurate or fair to be effective; it just needed to seem human, and humans with beating hearts are uniquely able to dispel the whiff of the uncanny from an automated script. Humans, of course, are indispensable when bodies are needed to show up in space or for photos.

BOTS HAVE EQUANIMITY WHEN IT COMES TO CONTESTED STORIES. HUMANS DECISIVELY PREFER TO SPREAD LIES.

As Bradshaw told the British parliament in testimony about hybrid information warfare, researchers lack the corporate datasets or government subpoena power to identify the exact humans involved in these campaigns. But the IRA indictments pointed the way to some Americans implicated in the Kremlin-sponsored infowar in 2016. When CNN approached two such people, they had contrasting responses.

"What would you think? A guy calls you and you talk to him and you build up a rapport over a period of time," said Harry Miller, who was reportedly and unwittingly paid by some of the Russian indictees to cage Hillary Clinton in effigy. "They had that beautiful website." By contrast, Florine Gruen Goldfarb, who mobilized Trumpites to demonstrate at an IRA-organized event, refused to accept that she'd been manipulated. "I don't go with the Russians. C'mon, give me a break," she said.

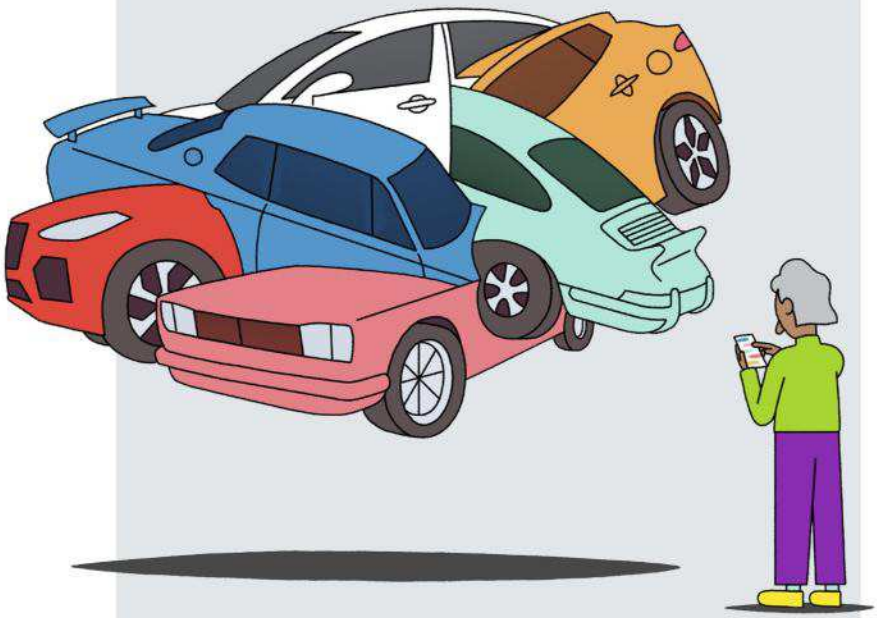
The fact that the campaigns involve masquerade, deception, and anthropomorphism—the disguising of robots as people—is part of why the IRA is charged

Virginia Heffernan *(@page88) is a contributor to* WIRED. *She wrote about how we see the world now in issue 26.04.*

with fraud and not acts of war. It's also why Americans are disinclined to see the internet and the nation as under siege. If we had swollen glands and bloody vomit, we'd accept a diagnosis of anthrax poisoning, but no one likes to see herself as cognitively vulnerable. Once, to my shame, I circulated some bot-amplified lies about antifa. (The meme was "Antifa is just as bad as neo-Nazism.") When caught out, I started to justify myself; fortunately, seeing disinfo as aerosolized anthrax—equally hard to detect—helped restore my confidence. I corrected my mistake. My immune system rallied. "No one likes to be told they've been duped," Bradshaw told me by email. But we must be "more aware of the ways in which bad actors try to infiltrate our networks to manipulate our thoughts and actions."

To determine how we got here, we might not need to perseverate on the exotic stuff: the Kremlin or troll farms and botnets. Perhaps the fault is in our ancient all-too-human bodies. In March, an MIT study of false news made it clear that bots have equanimity when it comes to contested stories, while humans decisively prefer to spread lies over truth. In particular, we appear to like and share the lies that shock and disgust, arousing our bodies in druglike ways.

If so, there's no way around this problem but through it. Of course, propaganda should be marked, regulated, and debunked. But at the same time, we need to understand our fragility as animals. Poor, mortal creatures of living-dying flesh that we are, we crave sensation. More even than robots, our most ancient proclivities may be our undoing.



WHAT'S THE DEAL

AUTO SUBSCRIBE
THE CAR OF THE MONTH

PEOPLE SEEKING a set of wheels traditionally had two options: buy or lease. But the advent of ride hailing turned the next generation of drivers into backseat riders. Now app-based subscriptions—think car sharing that's paid by the month, not the hour—are vying for consumers who fall between Uber addicts and car owners. ¶ Car sharing is projected to grow globally from 5.8 million users in 2015 to 35 million by 2021, according to Boston Consulting Group. "If we're right, nobody's going to borrow money to buy a car again," says Scott Painter, CEO of car-subscription startup Fair. He has reason to be bullish: His company has secured more than $1 billion in funding since 2016. The service connects drivers to used cars at dealerships nationwide, bundling warranty, maintenance, roadside assistance, and optional insurance into one month-to-month, pay-by-app fee (from $150). Pick up your car of choice at a participating dealer and return it at any time with five days' notice. ¶ A slew of other startups are also wooing commitment-phobic drivers. In 2015, Flexdrive launched subscriptions in Atlanta, Austin, and Philadelphia, with plans to expand to 24 other cities this year. Carma Car, which started in the Midwest, is now eyeing the East Coast. Even traditional automakers, from Ford to Porsche, are testing subscription models. "This takes a painful process—buying, financing, and maintaining a car—and turns it into a frictionless experience," says T. J. Rylander, a VC at Next47. It's the on-demand way: all the utility of ownership, none of the hassle. —CAITLIN HARRINGTON

EDIBLE DEVICES
FUSING FOOD AND TECH

FOOD DOESN'T ALWAYS pair so well with tech. The former is comforting and cultural, the latter cold and commercial. Lab-grown meat, transgenic crops, desserts extruded from the nozzles of 3-D printers: not exactly fodder for nostalgic childhood memories. ¶ But why not? asks Swedish designer Erika Marthins. "People often see technology as something alien," she says. "But if you're eating it, maybe that can help you understand it better." Working with engineers and scientists, Marthins uses tech to add motion, sound, and visuals to food. She's not suggesting anyone ingest metal or wires—but how about a lick of an augmented lollipop? There's a secret message encoded on its surface by an algorithm. Or consider her robot gummies that wiggle on the plate. Soft robots are often made with silicone; her variation, created with roboticist Jun Shintake, is made with a different material, this one edible— gelatin. Shintake believes soft robotics could one day become a go-to vehicle for delivering internal medicine. ¶ "Our tech will become more and more invisible, and it will be in everything," Marthins says. "I think we can have that next level in our meals." She envisions a future in which restaurants can serve up a completely personalized eating experience. Say a chef discovers Marthins' Swedish background. Maybe dessert will be some enhanced, interactive take on her favorite Nordic indulgence: salt licorice.

—MICHELLE Z. DONAHUE

Tasteful Portfolio

Dessert à l'Air
An edible robot that moves via inflatable chambers molded out of lemon-licorice-flavored gelatin.

Lumière Sucrée
Subtle distortions algorithmically engraved in the surface of a minty lollipop bend light to display a hidden image.

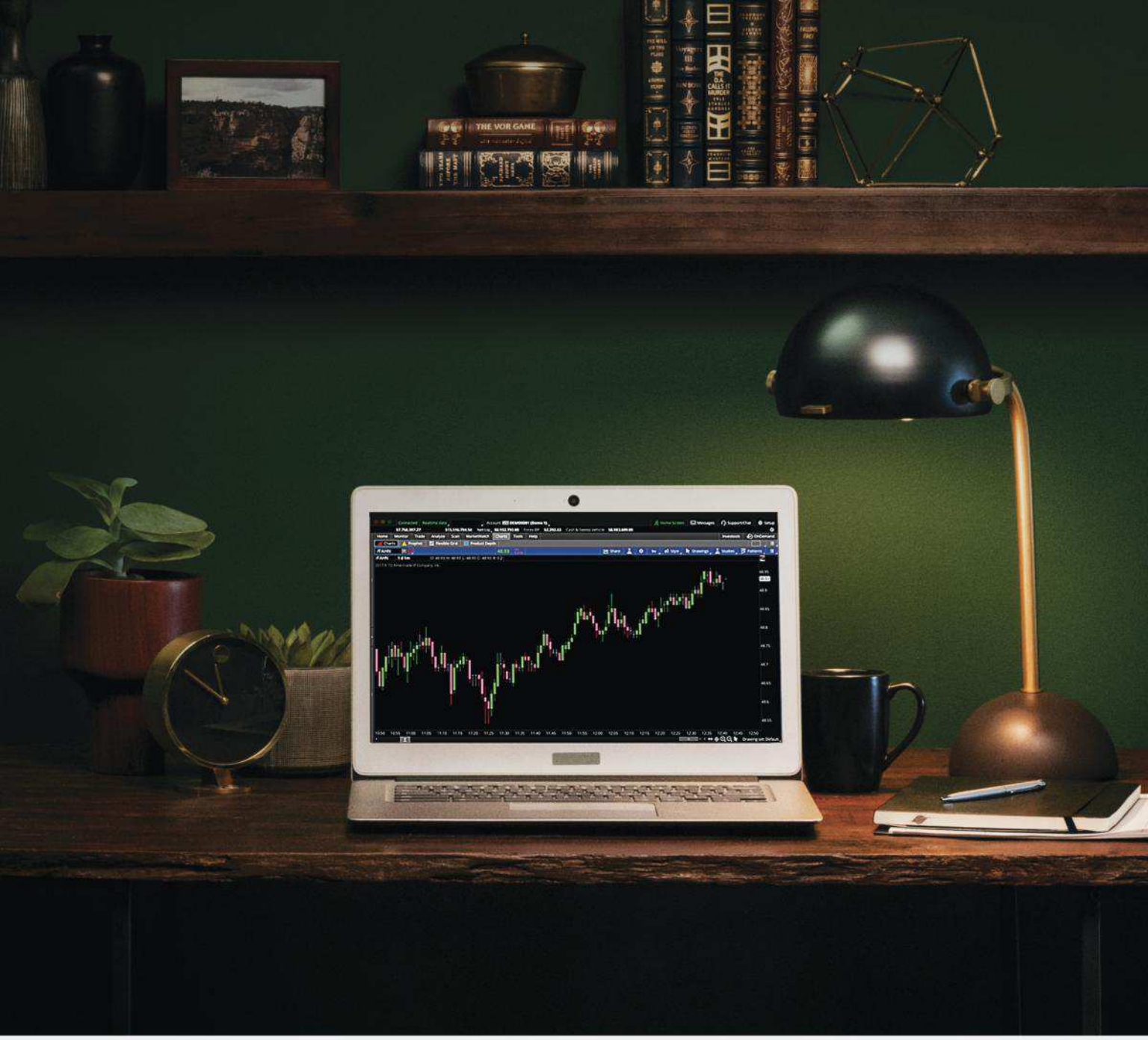
Mange Disque
Dark chocolate, Marthins found, works better than milk chocolate for creating a vinyl-like record (that really plays tunes).

WHO: Erika Marthins, 26, interactive designer

INFLUENCES: Danish sustainability designer Kaave Pour; experimental digital artist Thomas Traum; San Francisco poet-chef Dominique Crenn

FAVORITE FOOD: Burger with bacon, chèvre, and honey. "But in the summer, Swedish crayfish."

DJAMILA GROSSMAN



Goodnight, normal trading hours.

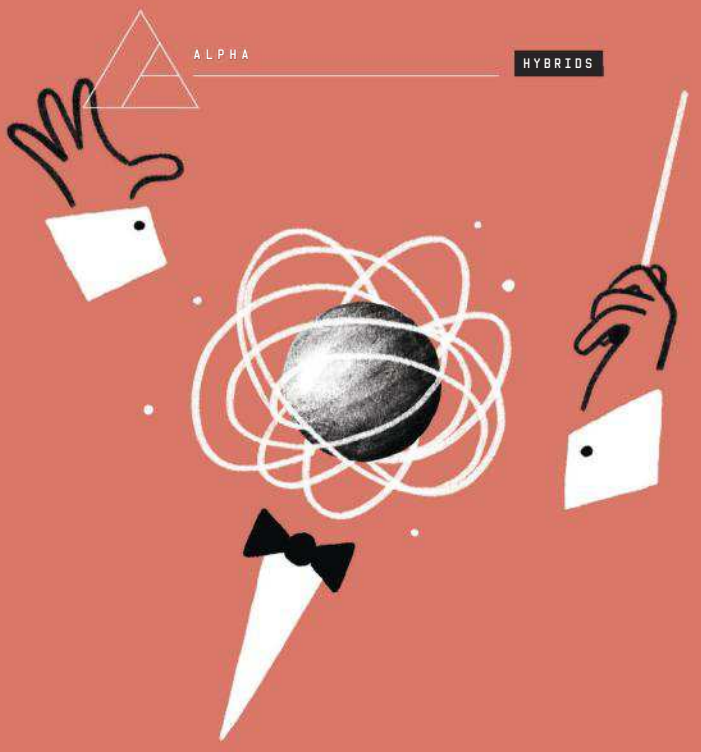
Say hello to 24-hour trading, five days a week. TD Ameritrade is the first retail brokerage to offer around-the-clock trading on select securities. The future of trading has arrived.

Get up to $600 when you open and fund an account.

TD Ameritrade®

Visit **tdameritrade.com/trade24-5** to learn more.

Extended hours trading is subject to unique rules and risks, including lower liquidity and higher volatility. Extended hours trading not available on market holidays. See tdameritrade.com/600offer for offer details and restrictions. This is not an offer or solicitation in any jurisdiction where we are not authorized to do business. TD Ameritrade, Inc., member FINRA/SIPC. © 2018 TD Ameritrade.



SONGS IN THE KEY OF AI

MUSIC WRITTEN by teams, David Byrne once wrote, is arguably more accessible than that written by a sole composer. Collaborations, he mused, may result in more "universal" sentiments. But what if your partner isn't human at all, but artificial intelligence? Now music producers are enlisting AI to crank out hits. —MATT JANCER

Style Counsel

Created by Sony's Computer Science Laboratories, **Flow Machines** analyzes tracks from around the world, then suggests scores that artists—including electropop musician ALB and jazz vocalist Camille Bertault—interpret into songs. For its debut album, *Hello World,* the AI also surveyed syllables and words from existing music to create original (albeit gibberish) vocals. **Recommended track:** The Beatles-inspired "Daddy's Car"

Mood Music

Jukedeck was originally developed to compose background tracks for user-generated videos; now it's being adopted by K-pop stars like Kim Bo-hyung and Highteen. Using deep neural networks, the AI predicts note sequences to compose brand new songs. After users select parameters such as mood, genre, and beats per minute, the AI cranks out a track that artists can embellish. **Recommended track:** Highteen's ultra-processed hit "Digital Love"

Classical Decomposer

The Artificial Intelligence Virtual Artist, a.k.a **Aiva**, combs through the works of composers such as Bach, Beethoven, and Mozart and uses the principles of music theory to make predictions and generate musical models. The program, developed by computer scientist Pierre Barreau, reconfigures those models into an original piece and arranges new sheet music. **Recommended track:** "Among the Stars," in the style of composer John Williams

Mix Master

Landr automates the audio mastering process in minutes. The AI compares nearly finished tracks to a database of 7 million already mastered singles and tweaks each song based on previous adjustments. By processing the tracks as a batch, Landr hones a unified sound. **Recommended track:** R&B single "Your World," produced by Kosine

Beats by Watson

YouTube personality Taryn Southern used IBM's Watson to make her debut album, *I AM AI*. Watson Beat studies patterns among keys and rhythms in 20-second clips of existing songs, then translates its findings into new tracks. Artists can use the open source application to layer their own instrumentals on top of the AI composite. **Recommended track:** Southern's synth-pop track "New World"

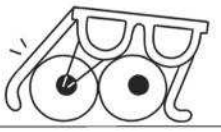
HYBRID GADGETS, FROM POINTLESS TO (SORT OF) PROMISING

BY LAUREN MURROW

Colgate E1 Smart Electronic Toothbrush
Maps your mouth and critiques your sluggish brushing technique. **For:** Mouth-breathers

Somnox Robot Cuddle Pillow
Regulates your breathing to induce zzz's. **For:** Anxious spooners

Petrics Smart Pet Bed
Tracks your pup's weight, temperature, and naps. **For:** Paunchy pooches



Intel Vaunt Smart Glasses
Conveniently projects notifications *directly onto your retinas.* **For:** Inveterate Glassholes

CareOS Health & Beauty Hub Mirror
Plays beauty tutorials and takes hands-free selfies. **For:** "Influencers"

L'Oreal UV Tattoos and Nail Decals
Detect deadly rays, look cute. **For:** Swedes, gingers, gamers

Raven Dashboard Camera
Monitors snogging/brawling/unconscious backseat passengers while navigating traffic. **For:** Chuck, silver Prius, 3.8 stars

LG InstaView ThinQ Fridge
Makes grocery lists, reads recipes, and, uh, plays music. **For:** Bachelors

HYBRID GADGETS: ILLUSTRATIONS BY LENNARD KOK

GREAT TASTE. ONLY 96 CALORIES.

MILLER LITE. HOLD TRUE.

GREAT BEER
GREAT RESPONSIBILITY®
©2018 MILLER BREWING CO., MILWAUKEE, WI

MARVEL'S INFINITE SUPERHERO PARTY

EIGHTEEN MOVIES OVER 10 YEARS costing $3.3 billion—all so every Marvel hero could get invited to the biggest shindy in all the galaxy, *Avengers: Infinity War*. Nobody sends their regrets. Thor's bringing the Guardians. Black Panther RSVP'd +1 with Captain America. Tony Stark—well, he likes to arrive alone. So does supervillain Thanos, except his intentions are far more worlds-destroyingly nefarious. It'll be, in the proper cosmic sense of the word, awesome. To celebrate, we've tracked how everyone got here (and how many times Loki betrayed them). Of course, because this is Marvel we're talking about, there's already a sequel planned for next year. To *Infinity* and beyond. —EMMA GREY ELLIS AND ANGELA WATERCUTTER

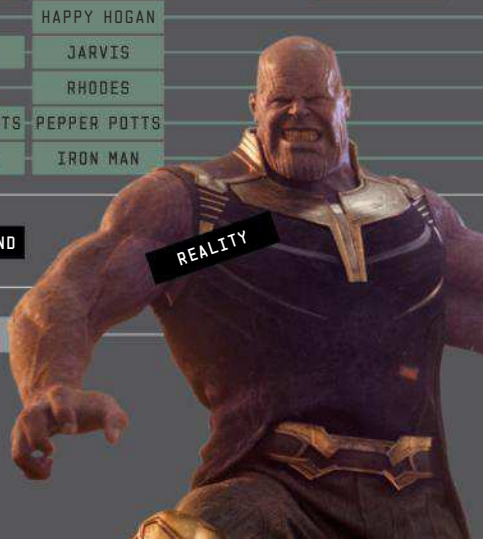
SOME CHARACTERS CHANGE IDENTITIES: **BUCKY BARNES** IS TURNED INTO **WINTER SOLDIER** (RIGHT) AND **RHODES** BECOMES **WAR MACHINE**.

JARVIS STARTS OUT AS TONY STARK'S ROBO ASSISTANT BEFORE AN ACCIDENT TRANSFORMS HIM INTO THE SUPERPOWERED **VISION**.

	Iron Man 2008	*The Incredible Hulk* 2008	*Iron Man 2* 2010	*Thor* 2011	*Captain America: The First Avenger* 2011	*The Avengers* 2012	*Iron Man 3* 2013	*Thor: The Dark World* 2013	*Captain America: Winter Soldier* 2014
HEROES ▶	IRON MAN	IRON MAN	IRON MAN	HAWKEYE	BUCKY BARNES	CAPTAIN AMERICA	HULK	THE COLLECTOR	SCARLET WITCH
	PEPPER POTTS		PEPPER POTTS	HEIMDALL	CAPTAIN AMERICA	HAWKEYE	HAPPY HOGAN	HEIMDALL	FALCON
	RHODES		RHODES	LOKI		LOKI	JARVIS	LOKI	WINTER SOLDIER
	JARVIS		JARVIS	THOR		THOR	RHODES	THOR	CAPTAIN AMERICA
	HAPPY HOGAN		HAPPY HOGAN			HULK	PEPPER POTTS		BLACK WIDOW
	HULK		BLACK WIDOW			BLACK WIDOW	IRON MAN		
INFINITY STONES ▶				SPACE	SPACE	SPACE, MIND			
VILLAIN ▶						THANOS			

FIVE OF SIX OF THESE FANCILY NAMED INGOTS HAVE SHOWN UP SO FAR.

ONCE **THANOS** COLLECTS ALL SIX INFINITY STONES, HE'LL TRY TO DESTROY THE COSMOS. OR SOMETHING.



PHOTOGRAPHS BY GETTY IMAGES (LEE); EVERETT COLLECTION

BY OUR COUNT, **LOKI** (SLIMIEST TRICKSTER GOD IN THE EIGHT REALMS) DOUBLE-CROSSES MARVEL HEROES 10 TIMES IN THREE MOVIES.

Guardians of the Galaxy 2014
NEBULA
ROCKET
GROOT
DRAX
GAMORA
STAR-LORD
THE COLLECTOR

Ant-Man 2015
ANT-MAN

Avengers: Age of Ultron 2015
SCARLET WITCH
FALCON
WINTER SOLDIER
CAPTAIN AMERICA
HAWKEYE
HEIMDALL
THOR
HULK
BLACK WIDOW
VISION
WAR MACHINE
IRON MAN

Captain America: Civil War 2016
BLACK PANTHER
SPIDER-MAN
ANT-MAN
SCARLET WITCH
FALCON
WINTER SOLDIER
CAPTAIN AMERICA
HAWKEYE
VISION
WAR MACHINE
IRON MAN

Doctor Strange 2016
WONG
DOCTOR STRANGE
THOR
BLACK WIDOW

Guardians of the Galaxy Vol. 2 2017
MANTIS
NEBULA
ROCKET
GROOT
DRAX
GAMORA
STAR-LORD

STAN LEE, CHAIRMAN EMERITUS OF MARVEL COMICS, MAKES A CAMEO IN EVERY MARVEL MOVIE, SPEAKING AN AVERAGE OF NINE WORDS.

Spider-Man Homecoming 2017
SPIDER-MAN
CAPTAIN AMERICA
IRON MAN

Thor: Ragnarok 2017
DOCTOR STRANGE
HEIMDALL
LOKI
THOR
HULK
HAPPY HOGAN
PEPPER POTTS

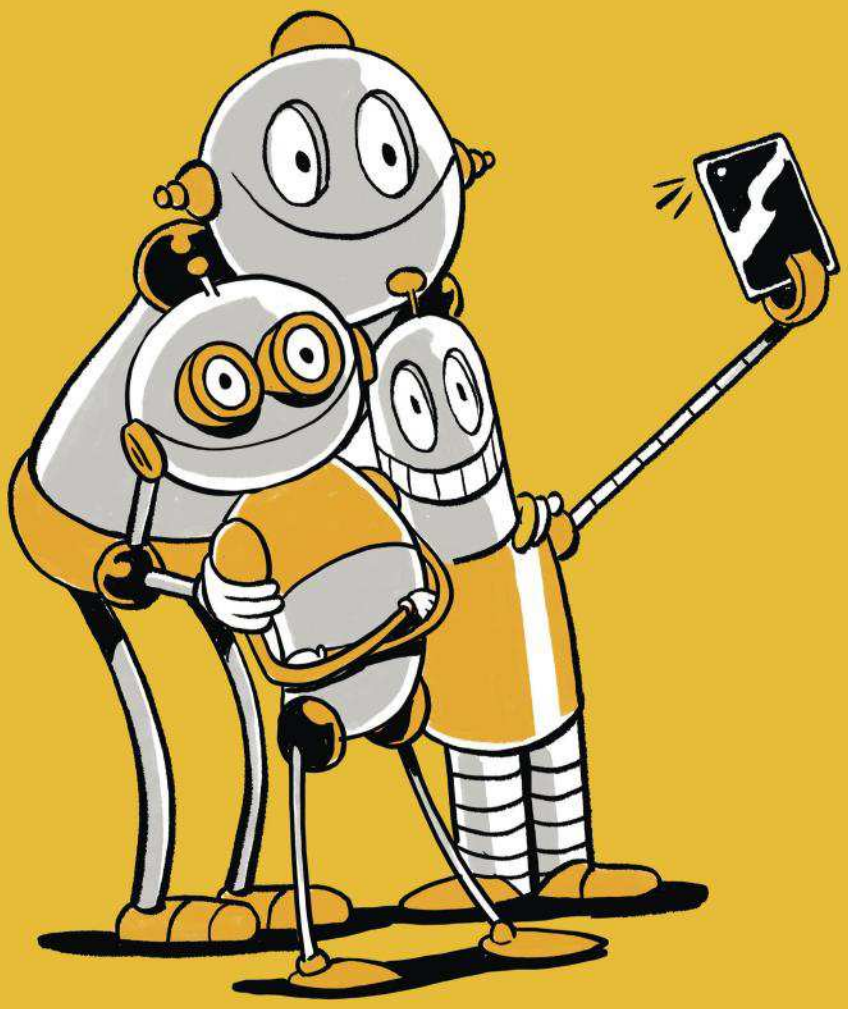
Black Panther 2018
M'BAKU
SHURI
OKOYE
BLACK PANTHER
BUCKY BARNES

Avengers: Infinity War 2018
M'BAKU
SHURI
OKOYE
BLACK PANTHER
WONG
DOCTOR STRANGE
SPIDER-MAN
ANT-MAN
MANTIS
NEBULA
ROCKET
GROOT
DRAX
GAMORA
STAR-LORD
THE COLLECTOR
SCARLET WITCH
FALCON
BUCKY BARNES
CAPTAIN AMERICA
HAWKEYE
HEIMDALL
LOKI
THOR
HULK
BLACK WIDOW
HAPPY HOGAN
VISION
WAR MACHINE
PEPPER POTTS
IRON MAN

MIND | MIND | TIME | SPACE | SPACE, MIND, REALITY, TIME, POWER, SOUL

THANOS

WIRED



SUBSCRIBERS NOW HAVE UNLIMITED ACCESS TO WIRED.COM

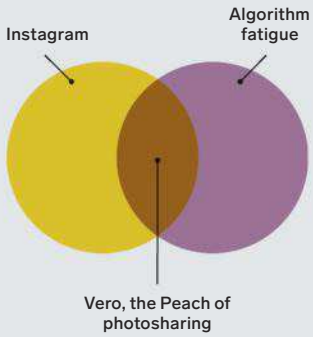
To ensure that our new paywall does not interrupt your experience, register or sign in at: wired.com/account/sign-in

Not yet a subscriber? To start your free trial, visit wired.com/subscription

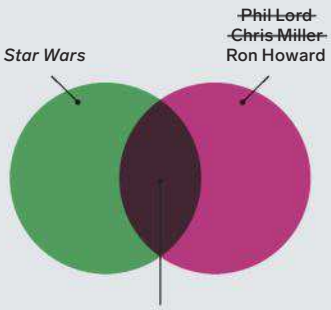
CHARTGEIST

BY JON J. EILENBERG

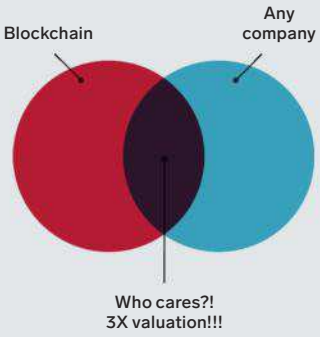
Social Media

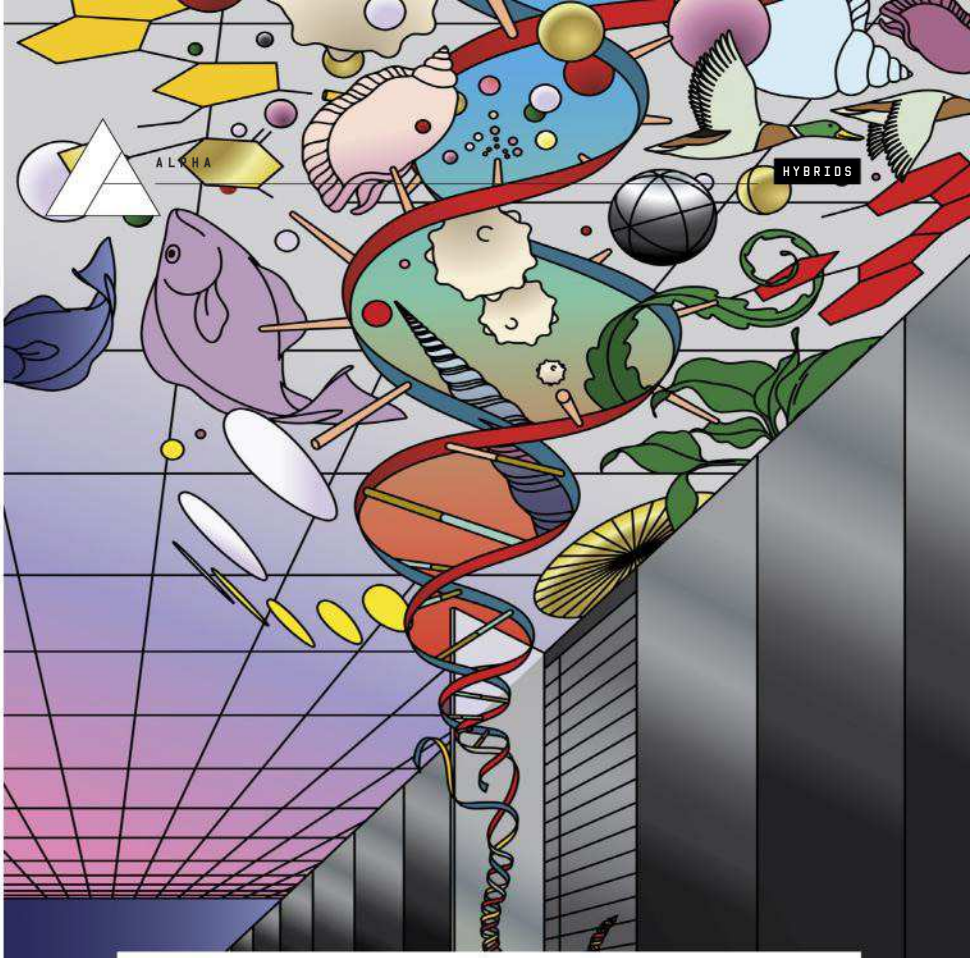


Solo



Business





EXTRA CRISPR

SPEEDING UP GENETIC EDITING

THE SERVER RACKS in Synthego's facility look like any other—big, nondescript black cabinets, whirring and blinking and venting heat. But inside the metal shelving, the company isn't pushing around ones and zeros to keep the internet running. It's making molecules to rewrite the code of life.

Researchers at universities, agtech companies, and biopharma firms want to genetically modify organisms, but they don't want to spend weeks building the Crispr tools necessary to do that. In comes Synthego: The biotech startup uses tech packed into those server cabinets to whip up hundreds of orders a day of guide RNA, the molecules that dictate which segments of DNA should get snipped out in editing. Software directs compressors and pumps to push chemical reagents into rows of instruments, mixing the fluids and catalyzing the 100,000 reactions needed to create a batch of Crispr kits. Within a week, the materials a lab tech needs to begin manipulating the genome of this lab rat or that zebra fish arrive at their bench.

"Being able to do that in a parallel way is the novel part," says Paul Dabrowski, who cofounded the company in 2012 with his brother, Michael. Neither has a background in biology; they're former SpaceX engineers. (They chose server racks because the modular design makes them perfect vehicles for the complex Crispr machinery—but the boxes surely help these computer guys feel more at home.) "The reason we built this hardware, the reason we made these kits, is to speed up research," Dabrowski says. Now scientists can spend less time babysitting cells and more time doing, well, science. —MEGAN MOLTENI

EDWARD CARVALHO-MONAGHAN

TOOL

ARMED RESPONSE

GADGETS GET TOUCHY-FEELY

Ask engineers what the future of communication looks like and they'll show you a fiber-optic cable. Ask artists and they'll conjure something like the Sleeve. For the past year, engineers at Nokia Bell Labs, the famed New Jersey research facility that birthed the transistor, have been developing this wearable armband with input from artistic collaborators. "We're reductionist in our thinking; artists are divergent," research lead Domhnaill Hernon says. The labmates are part of a program called Experiments in Art and Technology, founded in the '60s and newly resurrected in partnership with the design incubator New Inc. In this right-brains-meet-left coalition, engineers and artists team up to explore big questions: Can humans communicate through touch? Is it possible to transfer empathy? What's the successor to smartphones? The Sleeve tries to answer them. This early model gathers information about the user's physical and emotional state through gyroscopes, accelerometers, and optical sensors, then communicates that intel via haptic pulses and screen-displayed messages. The collaborators aim to inspire more engineers to consider the emotional plane. Soon you'll be able to express your heart through your sleeve. —ELIZABETH STINSON

Haptic motors

These motors produce vibrational jolts to transmit emotional messages between users or provide the wearer with environmental feedback.

Screen

A dot matrix LED screen conveys biological signals, messages, and directions, affording richer communication between Sleeve users.

Electromyography wires

An advanced alternative to swiping and tapping, these wires measure subtle electrical signals in your forearm muscles to send messages through the Sleeve.

Inertial measurement unit

Accelerometers and gyroscopes recognize directional movement. The Sleeve could be used to control smart-home devices with gestures.

Optical coherence tomography disc

This device measures how light interacts with tissue to determine the body's chemical makeup. It can detect biomarkers for stress and joy.

NICHOLAS CALCOTT

ALL GLASSHOLES ARE REVOLUTIONARIES

THAD STARNER HAD BEEN wearing a computer for a few years—an LED readout over his left eye, wired to a processor in a shoulder bag and a one-handed keyboard—when he came to Silicon Valley for a conference in 1998. His kludgy, cyberpunk rig was fascinating; two young techies walked up to ask him about it.

"I said, 'It's a wearable computer,'" Starner recalls. "I gave them a demo." He asked them for their business cards so he could demonstrate how he could enter their information into his computer's address book. They handed them over. Guy Number One: Larry Page. Phone number at Stanford. Guy Number Two: Sergey Brin. They were working on some kind of web search project, they said.

A decade later, Starner—by then a researcher at Georgia Tech—looked into his head-up display and realized he still had Brin's email address. He clicked out a note: *You haven't seen wearable stuff in a few years. Come have a look*. "Next thing I knew, I was in Mountain View giving demos, not realizing it was actually a job interview," Starner says. Page and Brin were working on something related, they said. And they had a job for him.

Starner called what he saw through his lens "augmented reality"—a term he coined to describe the superimposition of the digital world onto the real. After agreeing to work with Page and Brin at Google, he was put in charge of designing the first full-on commercial augmented reality system: Google Glass. It would burn ultrabright for a few months in 2012 and 2013, ascending to the acme of cultural hotness only to plummet, Wile E. Coyote–like, to failure. Or so it seemed.

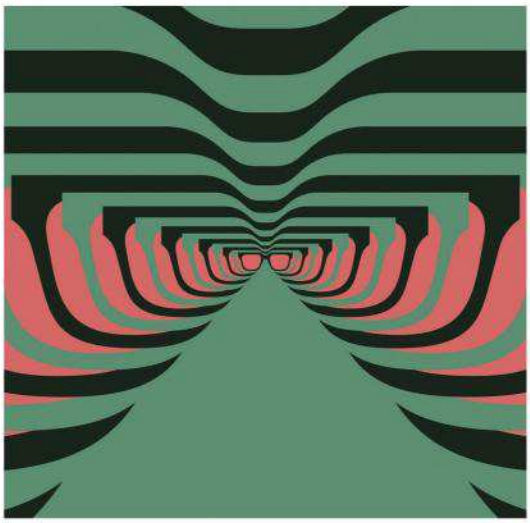
Glass arrived with fanfare, and people had to lobby via hashtag for the privilege of dropping $1,500 for one. But it was more or less a beta release, with a veneer of high fashion and promise of constant access to the internet that couldn't disguise a Rent-a-RoboCop vibe. Turning on the screen required a wearer to assume a discomfitingly dorky head angle; if you wanted to do anything else you had to say "OK, Glass" at what Google's engineers had, it seemed, parametrically determined would be the most awkward moment in any conversation. It didn't actually do much except let you take creepshots. People started calling anyone wearing Google Glass a "Glasshole."

Google pulled the product in January 2015, but anyone who's seen a movie can tell you that cyborgs are hard to kill. Technology that at first seems irrelevant often becomes unavoidable—or inevitable. Sure, Glass became a gossip-tinged metonym for tech bro narcissism. But before you toss Glass into the drawer with your CueCat and your PalmPilot, let's talk about the wristwatch.

Until World War I, men wore pocketwatches. Wristwatches were bracelets, and bracelets were for women. But then macho military dudes learned that having the time on your wrist made it easier to operate heavy machinery and blow stuff up. So would-be macho dudes started wearing them too. Click! The world looked different. "The same thing happened with sunglasses," says Clarissa Esguerra, a curator for costume and textiles at the Los Angeles County Museum of Art. "And the zipper too." Same with headphones; when people started wearing Walkmans in public, it seemed creepy. But now? All cyborgs are revolutionaries. Their modifications look weird and affected until they don't.

At CES 2018, half a dozen companies showed working prototypes for eyeglass-based computing. Magic Leap became one of the most hyped startups of the past few years on the strength of augmented reality goggles. Police in China are using glasses-enabled facial recognition to expand their panopticon surveillance. The end of Google Glass wasn't even the end of Google Glass; X, the incubator that oversees the product, sells them as a head-up display for assembly workers. But more than that, the idea of augmented reality has normalized. Capturing everyday moments with a ubiquitous camera and inserting digital elements into your everyday field of view—well, that's just Snapchat.

Technology, connectivity, and culture have finally caught up with Starner, who says eyeglass computers like Glass aren't science projects anymore—now you can hardly tell they're there. "People no longer think of it as a separate device," he says. "They think of it as them." Which was his vision all along. W



By **Adam Rogers** *(@jetjocko), who wrote about director Luc Besson in issue 25.07.*

AUTONOMOUS METROPOLIS

A CITY OF SELF-DRIVING CARS

YOU DON'T LOOK FOR the essence of a city in its monuments or its museums. You look for it in its streets, where the covenant at the core of urban life—the sharing of space—plays out. For the past century, the personal car has dominated that arena, shaping the streets and environments around it. Roads are straight and wide for faster travel; intersections are regulated to protect distracted humans; businesses are located near open spaces for better parking. But as cars start to drive themselves, we have some ideas for how urban planners of the future might reimagine those outdated layouts—and transform the city into a joyful mess of throughways and byways optimized not for cars but for people. —ALEX DAVIES AND AARIAN MARSHALL

MENGXIN LI

SPERMBOTS ILLUSTRATION BY SIMON LANDREIN

1. Major Arteries

While main thoroughfares will still exist (so self-driving buses and trams can quickly get people where they need to go), there won't need to be as many. Autonomous tech will never be perfect, but limiting the places where cars can go fast should mitigate crashes.

2. Green Space

Even little bits of green—a tree here, a parklet there—can improve mental health. Great news: With less space needed for everybody's personal cars, nature can be everywhere. Also, why not move water runoff above ground as streams, for pedestrians to enjoy?

3. Nest Stops

Imagine: no need for curbside parking or sprawling garages. But parking won't go away entirely. It'll be too expensive for taxi companies to operate their driverless vehicles during off-peak hours, so cities will scatter small "nests"—pit stops for autonomous vehicles—throughout their streetscapes. Larger "hives" will house facilities for vehicle maintenance and charging.

4. Zombie Tax

With parking meters and traffic enforcement cops off the streets (no more towing!), the city will need new ways to raise funds. One idea: a per-minute tax on driverless cars with empty seats—zombie-mobiles only congest roadways.

5. Designated Stations

In roads optimized for self-driving taxis, ride hailers won't have to dash across lanes to catch cars—pickup and drop-off stations will be strewn throughout cities.

6. Zoning Free-for-All

Building height restrictions meant to reduce traffic and parking space requirements lose their justification in the self-driving city, so zoning laws can chill out.

7. Less Signage

Speed limits, stop signs, traffic lights: These are the trappings of a streetscape built for needy human drivers. In this future, cars will know the rules. The only street signs you'll see will provide ETAs for public transit. No delays, hopefully.

8. Call Centers

Self-driving cars won't be infallible. In case they get stuck or stumped by things like road construction, humans in call centers (maybe former Uber and Lyft drivers) will be ready to take control and get them out of jams.

9. Winding Roads

Side streets will serve people first, not cars. They'll meander around buildings and restaurants, stores and schools. Everyone's welcome: self-driving cars, cyclists, skateboarders, pedestrians. (Jaywalking, as crime and concept, has disappeared.)

10. Specialization

Large self-driving vehicles will serve different functions at different times: take kids to school in the morning, make some deliveries during the day, take kids home in the evening, assist with birthday bar crawls late into the night.

11. Lobby Boom

When cars don't park, no one enters buildings through the garage—they'll always enter through the lobby. Architects expect that everything from apartment complexes to dreary office buildings will have more elaborate entrances. Time to invest in that koi pond startup.

12. Delivery Bots

Street droids will make house calls for mail, groceries, and supplies, while fleets of flying drones handle bigger orders. At the end of their shifts, the delivery bots return to the mothership—a self-driving van.

Senior associate editor **Alex Davies** *(@adavies47) and staff writer* **Aarian Marshall** *(@aarianmarshall) cover transportation for* WIRED.

RELEASE THE SPERMBOTS

Chemotherapy is brutal. The drugs are delivered in near-toxic doses to penetrate tumor tissues, indiscriminately vanquishing the patient's appetite, hair, and immune system alongside cancer cells. Scientists have tried everything from nanoparticles to homing-beacon bacteria to better target the disease. Now researchers at Germany's Institute for Integrative Nanosciences are deploying a natural-born infiltrator: sperm. ¶ The team had been working for years on a robotic power-boost for slow swimmers—originally intended to help couples with low sperm motility conceive. But when they discovered that the sperm's double-lipid-lined head could also be coaxed into carrying a payload of chemo drugs, they shifted their focus from inducing life to slaying reproductive cancer. ¶ The little guys won't be going into battle naked. Using a two-photon laser, the scientists created a set of sperm harnesses—tiny tubes with flexible arms that cling to the head. By coating the harnesses in iron, they were able to steer the machines using an external magnetic field. As the ironclad Trojan horses collide with tumors, the force of impact causes them to shed their harnesses, burrow into the tissue, and drop their killer payload. When the researchers sicced the spermbots on a cancerous mass, they killed more than 90 percent of the rogue cells. ¶ So far, the technique has been tested using bull sperm in microfluidic plastic chambers, not yet in animals or humans. Still, the technology reveals a promising new army of drug carriers—like guided missiles for cancer.

—MEGAN MOLTENI

CLIVE THOMPSON

CRANK IT UP
THE TWO-WHEELED FUTURE OF MOBILITY

WHAT'S THE SHINIEST, most exciting new technology for transportation? Well, there are plenty of candidates! We've got the self-driving car and drones big enough to carry people. Elon Musk is getting ready to bore hyperloop tunnels. When it comes to moving humans around, the future looks to be merging with sci-fi. ¶ But from where I stand, the most exciting form of transportation technology is more than 100 years old—and it's probably sitting in your garage. It's the bicycle. The future of transportation has two thin wheels and handlebars. ¶ Modern tech has transformed the humble two-wheeler, making the bike-share model possible: You check out a bike from a docking station, use it for an hour or so, then return to any other docking station. The concept was tried back in the '60s but failed miserably because no one could track where the bikes went. ¶ Today, that's been solved with smartphone-ized tech: GPS, Bluetooth, RFID, and mobile-payment systems. And bike sharing has unlocked a ton of American interest in navigating cities on a bike: Usage has grown from 320,000 rides in 2010 to 28 million in 2016. In China, where gridlock in cities like Beijing is infamous, the trend has grown even faster. ¶ But cooler tricks are possible. We're now seeing dockless bike sharing, where all the tech is crammed into each bike, eliminating the need for docking stations. When riders are done, they just park and lock the bike and walk away; the bike simply awaits the next user. This makes the systems cheaper (those docks cost a lot), so dockless bikes can be rented for as little as a buck an hour.

"It's personal mobility for the last mile," as Euwyn Poon, cofounder of dockless bike-sharing firm Spin, says.

Dockless also creates something like self-governing internet logic, with bikes as packets routed where they're needed, rather than where docks will fit. This seems to make bike sharing more fair: Seattle city councilmember Mike O'Brien has observed anecdotally that dockless bike sharing is used by a broader demographic, in part because it's super cheap and the bikes can circulate outside the well-off downtown neighborhoods.

Want even more inventiveness and innovation? Behold the next phase arriving in a few years: dockless electric bikes. Batteries are cheaper and lighter than ever. One US firm, Jump Bikes, has custom-designed dockless ebikes sprinkled around San Francisco and Washington, DC. CEO Ryan Rzepecki suspects they'll eclipse the appeal of regular bike sharing, because you could arrive at work without being drenched in sweat. "The number of people who are willing to ride electric bikes is probably 10X that of people who are willing to ride a regular one," he says.

Clearly the bike-share revolution has limits. It probably won't work outside urban areas. And if too many bikes flood a city, dockless systems can produce chaotic piles of bikes on certain sidewalks and streets, as has happened in China. This is a pretty solvable problem, though, if cities decide to limit the number of dockless bikes.

So sure, bring on the self-driving cars. Dig those hyperloops! But for a world that's rapidly urbanizing and heating, the truly cool tech is bikes. And bike sharing has oodles of civic benefits too, says Elliot Fishman, director of Australia's Institute for Sensible Transport: It relieves pressure on public transit, produces vanishingly small emissions compared to cars, and, at least with nonelectric bikes, boosts the overall exercise level (duh!).

Best of all, the bike-tech revolution reminds us that innovation isn't always about the totally new. It's often just as powerful to blend a robust, old tool that works well with a bit of new tech to make it better. Sometimes you truly don't need to reinvent the wheel. W

Write to clive@clivethompson.net.

Introducing the...

GQ BEST STUFF BOX

The **GQ BEST STUFF BOX** is a quarterly subscription box featuring the things we love—rigorously tested and loved by GQ editors. It includes our favorite electronics, grooming products, and accessories. The first of four boxes will include brands like:

ACQUA DI PARMA

BAXTER'S OF CALIFORNIA

JLAB

JASON MARRKS

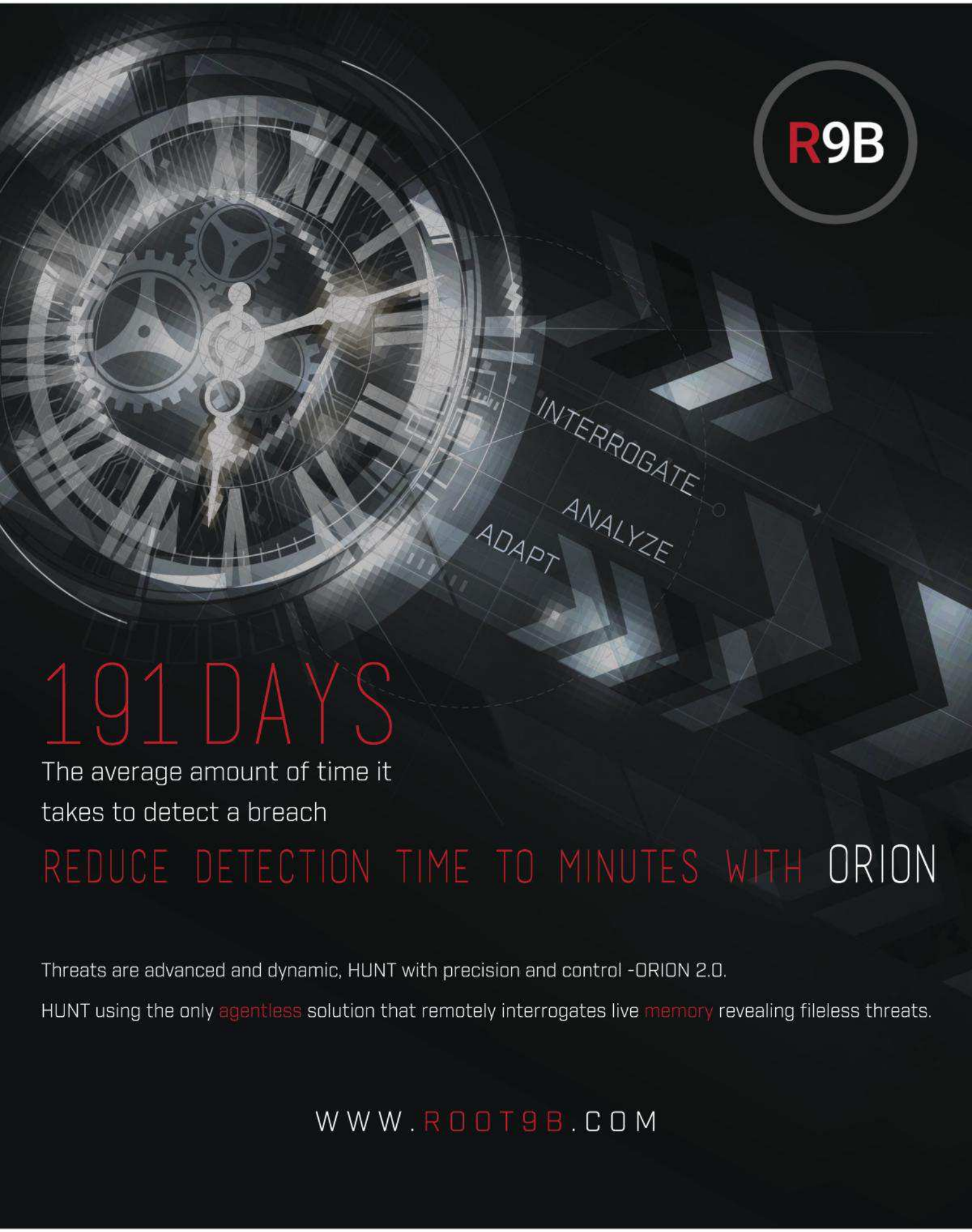
NICE LAUNDRY

RUDY'S BARBER SHOP

$215 VALUE
FOR ONLY $49

JLab Epic2 Bluetooth
Wireless Sport Earbuds

Pre-order now at
GQ.COM/BESTSTUFFBOX


R9B
INTERROGATE
ANALYZE
ADAPT
191 DAYS
The average amount of time it
takes to detect a breach
REDUCE DETECTION TIME TO MINUTES WITH ORION
Threats are advanced and dynamic, HUNT with precision and control -ORION 2.0.
HUNT using the only agentless solution that remotely interrogates live memory revealing fileless threats.
WWW.ROOT9B.COM

ENTERTAINMENT

SONY LSPX-A1

FETISH
OFF THE WALL

THE MAGIC IN SONY'S new entertainment system is that it doesn't resemble a TV at all. The 4K HDR laser projector casts gleaming, lifelike video onto any surface above it. Pushed up against the wall, the coffee-table-sized unit projects an 85-inch image. Slide it out a foot, and the picture blooms to 120 inches. The speaker system stays fully concealed: a pair of glass tube tweeters in the aluminum legs, three midrange speakers hidden behind the front panel, a subwoofer on the bottom, and a rear driver that deepens the immersive effect. The projector's eye is tucked just below the marble tabletop while the wooden shelf below provides ample space for your art books. —JEFFREY VAN CAMP

$30,000

STYLING BY GRACE SUH AND ANDRIA LO

TOP 3 GAME BOYS

Don't leave your latest gaming obsession at your desk. With these powerful laptops, you can level up wherever, whenever. —BRENDAN NYSTEDT

1

Razer Blade

The newest Blade laptop comes with top-tier Nvidia graphics, a quad-core Intel processor, and an optional 14-inch, 4K touchscreen. Razer's customizable Chroma LED system lets you choose the color and animation style of your keyboard backlighting, so the Blade looks as good as it games.

$1,899 and up

2

Alienware 13

The chunky black Alienware is one of the only laptops with a 13-inch OLED touchscreen. Like the Blade, Nvidia graphics and quad-core Intel power mean it's no slouch for gaming, VR, or multimedia. It's not the slimmest machine, but the 5-pound body is stacked with every port you need for connecting your myriad peripherals.

$1,150 and up

For buying advice for these products and more, visit wired.com/shop.

3

Asus ROG Zephyrus M

This transforming Asus laptop comes straight from Cybertron. When you flip up the 15.6-inch screen, the back of the case eases open 6 millimeters to help vent all the hot air pumped out by that brawny Nvidia GeForce GTX 1070p graphics chip and a new eighth-gen Intel processor.

$2,199 and up

3

HEAD-TO-HEAD BRIGHT EYES

Whether you're beaming up to the *Enterprise* or crashing your friend's destination wedding from your sofa, these headsets take you there. —JEFFREY VAN CAMP

HTC Vive Pro

BEST FOR: Holodeck dreamers

HTC's first Vive headset was the pinnacle of home VR; the new Vive Pro improves on every feature. Paired with a powerful PC, the Pro transforms your room into a near-limitless virtual gamescape. Cyberspace gets more immersive thanks to a higher-res display for each eye and integrated headphones with 3-D audio. The optional wireless adapter frees you from pesky cords.

$799

Lenovo Mirage Solo

BEST FOR: Casual enthusiasts

The VR ideal is a stand-alone headset, with no phone or PC required. The Mirage Solo doesn't require either, but it can play any of the mobile games available in Google's Daydream store. Connect to Wi-Fi, and the Mirage Solo's motion controller and space-sensing exterior cameras grant full freedom of movement, letting you duck and dodge during play.

$400

Introducing

GQ Recommends

The easiest way to find the clothes, goods, and gear you want, all of it chosen by our editors. **Get yourself something nice.**

gq.com/recommends

GEARHEAD SWITCHIVERSE

A rich ecosystem of Switch add-ons makes Nintendo's compact console even more fun. —BRENDAN NYSTEDT

1

3

2

1

Nintendo Joy-Con

Nobody prefers watching everyone else have all the fun. Get an extra set of Joy-Con controllers and invite more friends to join you in games like *Overcooked*, or line up for a four-way race in *Mario Kart 8*. These have all the same motion sensors and rumble effects as the Joy-Con that came with your Switch.

$80

2

RavPower Xtreme 26800 PD

Any battery pack can juice up your system in sleep mode, but most aren't powerful enough to charge the Switch while you game. Thanks to this pack's USB-C Power Delivery standard, you can keep *Splatoon*-ing as your console rejuvenates. The massive 26,800-mAh battery quadruples your *Zelda* time.

$80

4

Nintendo Switch $300

◀

3

Nintendo Labo

These flat-pack DIY kits let you build playful supplemental Switch controllers out of precut cardboard. There are six available Labo rigs, including this adorable toy piano, a fishing pole for virtual catch-and-release, and a mecha set that lets you pilot an onscreen robot.

$70 and up

4

Nintendo Pro Controller

If you're exploring Hyrule for hours on end, the official Pro Controller is a worthy upgrade for fending off cramps, especially if your adult hands struggle with the kid-friendly Joy-Con. You get big buttons, haptic feedback, motion control, and 80 hours of playtime between charges.

$70

5

Turtle Beach Earforce Recon 50 Headset

Whether you're playing in bed, on the bus, or crammed into seat 31B, a headset is a must. These affordable cans plug into just about any gaming system with a headphone jack, which Switch thankfully has. At a light 7 ounces, they're great for kids too.

$40

5

HEAD-TO-HEAD PROG ROCKS

Alexa's fine, but if you want superior audio with your AI, try one of these chatty speakers. —MICHAEL CALORE

Apple HomePod

BEST FOR: Demanding audiophiles

Few compact speakers, smart or otherwise, sound better than this 7-inch-tall cylinder. It listens to the sound waves bouncing around the room, then adjusts the output for pristine audio. Chat interactions are a bit limited for now, but Siri's an ace DJ. The AI can play songs or podcasts from Apple Music and control connected outlets and smart LED bulbs.

$349

Google Home Max

BEST FOR: Inquisitive beat freaks

We found the Assistant inside Google's largest Home speaker smarter than other AIs, answering queries, bossing connected devices, and sending driving directions to a Pixel phone. It can also cue up audio from your fave streaming platform. The Max puts out a beastly thump, with enough low end to make the neighbors think Janelle Monáe has moved in.

$399

SMALL BUSINESS

Dell recommends Windows 10 Pro.

THERE'S NOTHING SMALL ABOUT WHAT I DO.

Dell Small Business Technology Advisors give you the tech, advice and one-on-one partnership to fuel your business' growth.

TECH. ADVICE. PARTNERSHIP.

Contact an advisor today:
VISIT DELL.COM/SMALLBUSINESSPARTNER
CALL 877-BUY-DELL

VOSTRO 15 5000
Starting at $549

intel CORE i3 inside

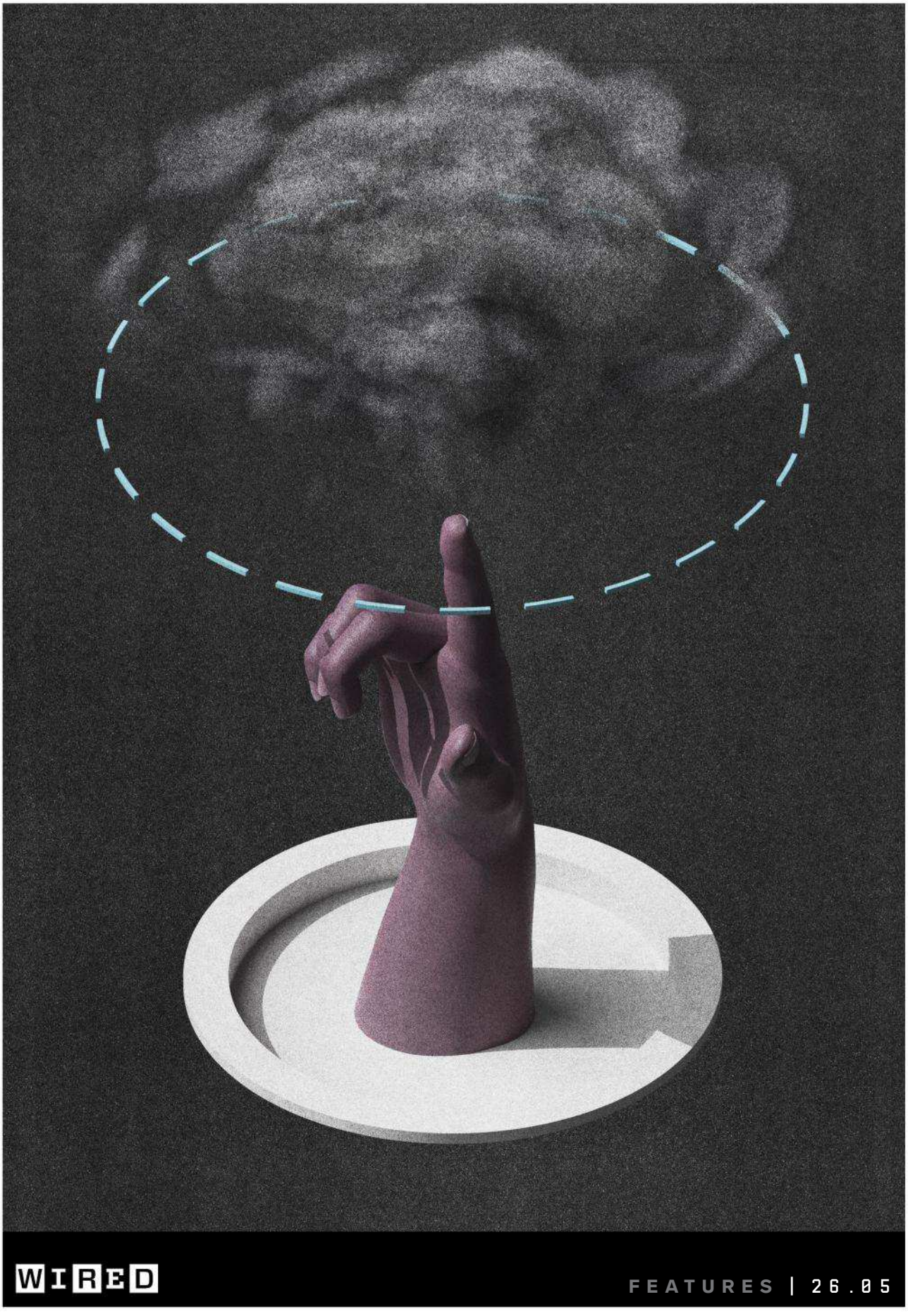
*Offers subject to change. Taxes, shipping, and other fees apply. Dell reserves the right to cancel orders arising from pricing or other errors. Intel, the Intel Logo, Intel Inside, Intel Core, and Core Inside are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. Microsoft and Windows are trademarks of Microsoft Corporation in the U.S. and/or other countries. Screens simulated, subject to change. Windows Store apps sold separately. App availability and experience may vary by market. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. © 2018 Dell Inc. All rights reserved.

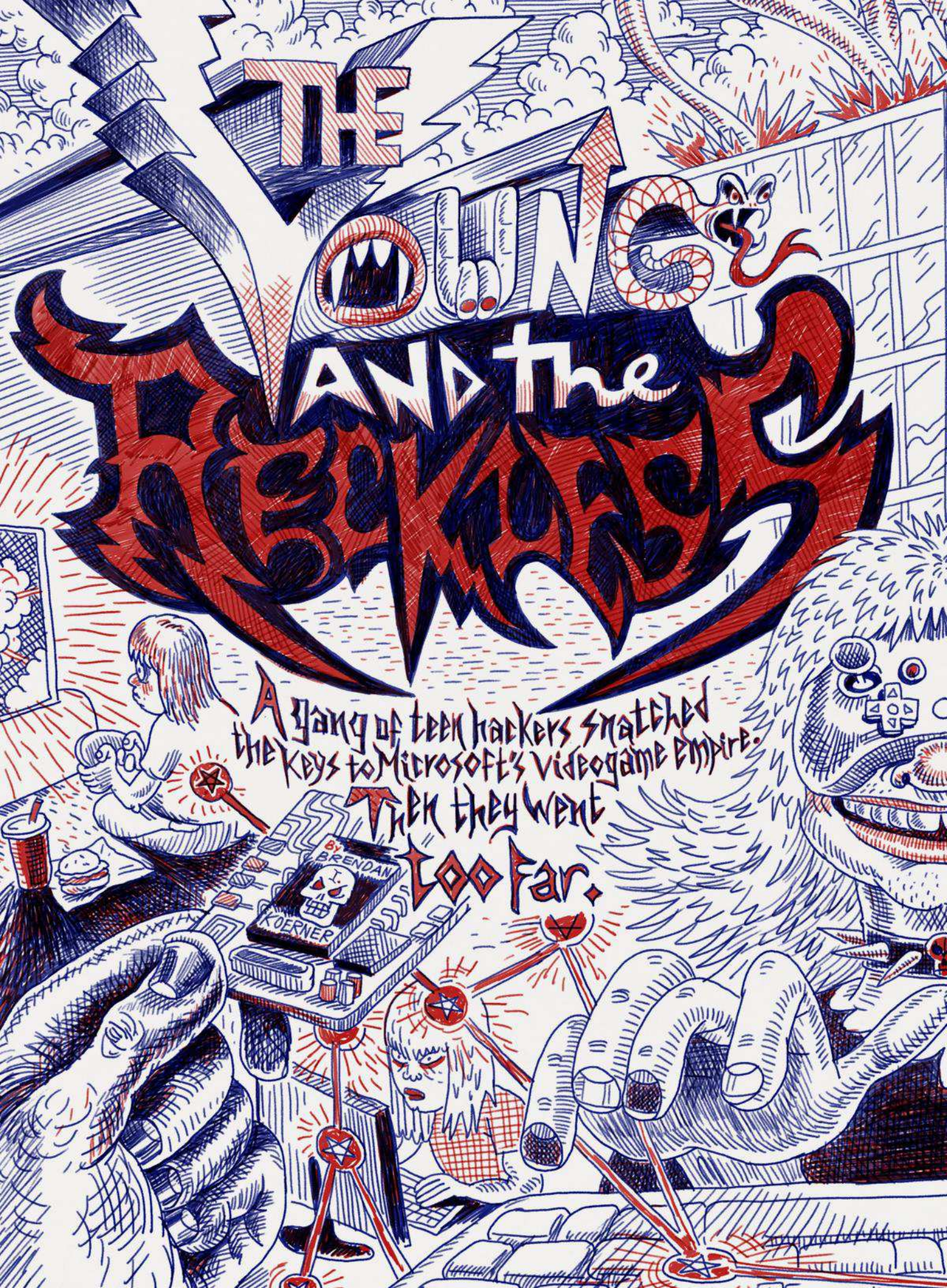
PROMOTION

Breadth. Depth.
The Best Technology Journalism.

ars TECHNICA

arstechnica.com




THE
KING
AND the
HACKERS
A gang of teen hackers snatched the keys to Microsoft's videogame empire.
Then they went too far.
BY BRENDAN I. KOERNER


MicroSoft
FBI
FBI
BOX
UNDERGROUND
CASH
CALL OF DUTY
ILLUSTRATIONS
BY
ZOHAR
LAZAR
047

David Pokora, a bespectacled University of Toronto senior with scraggly blond hair down to his shoulders, needed to travel south to fetch a bumper that he'd bought for his souped-up Volkswagen Golf R.

The American seller had balked at shipping to Canada, so Pokora arranged to have the part sent to a buddy, Justin May, who lived in Wilmington. The young men, both ardent gamers, shared a fascination with the inner workings of the Xbox; though they'd been chatting and collaborating for years, they'd never met in person. Pokora planned to make the eight-hour drive on a Friday, grab a leisurely dinner with May, then haul the metallic-blue bumper back home to Mississauga, Ontario, that night or early the next morning. His father offered to tag along so they could take turns behind the wheel of the family's Jetta.

An hour into their journey on March 28, 2014, the Pokoras crossed the Lewiston–Queenston Bridge and hit the border checkpoint on the eastern side of the Niagara Gorge. An American customs agent gently quizzed them about their itinerary as he scanned their passports in his booth. He seemed ready to wave the Jetta through when something on his monitor caught his eye.

"What's ... Xenon?" the agent asked, stumbling over the pronunciation of the word.

David, who was in the passenger seat, was startled by the question. Xenon was one of his online aliases, a pseudonym he often used—along with Xenomega and DeToX—when playing *Halo* or discussing his Xbox hacking projects with fellow programmers. Why would that nickname, familiar to only a handful of gaming fanatics, pop up when his passport was checked?

Pokora's puzzlement lasted a few moments before he remembered that he'd named his one-man corporation Xenon Development Studios; the business processed payments for the Xbox service he operated that gave monthly subscribers the ability to unlock achievements or skip levels in more than 100 different games. He mentioned the company to the customs agent, making sure to emphasize that it was legally registered. The agent instructed the Pokoras to sit tight for just a minute longer.

As he and his father waited for permission to enter western New York, David detected a flutter of motion behind the idling Jetta. He glanced back and saw two men in dark uniforms approaching the car, one on either side. "Something's wrong," his father said, an instant before a figure appeared outside the passenger-side window. As a voice barked at him to step out of the vehicle, Pokora realized he'd walked into a trap.

In the detention area of the adjoining US Customs and Border Protection building, an antiseptic room with a lone metal bench, Pokora pondered all the foolish risks he'd taken while in thrall to his Xbox obsession. When he'd started picking apart the console's software a decade earlier, it had seemed like harmless fun—a way for him and his friends to match wits with the corporate engineers whose ranks they yearned to join. But the Xbox hacking scene had turned sordid over time, its ethical norms corroded by the allure of money, thrills, and status. And Pokora had gradually become enmeshed in a series of schemes that would have alarmed his younger self: infiltrating game developers' networks, counterfeiting an Xbox prototype, even abetting a burglary on Microsoft's main campus.

Pokora had long been aware that his misdeeds had angered some powerful interests, and not just within the gaming industry; in the course of seeking out all things Xbox, he and his associates had wormed into American military networks too. But in those early hours after his arrest, Pokora had no clue just how much legal wrath he'd brought upon his head: For eight months he'd been under sealed indictment for conspiring to steal as much as $1 billion worth of intellectual property, and federal prosecutors were intent on making him the first foreign hacker to be convicted for the theft of American trade secrets. Several of his friends and colleagues would end up being pulled into the vortex of trouble he'd helped create; one would become an informant, one would become a fugitive, and one would end up dead.

Pokora could see his father sitting in a room outside the holding cell, on the other side of a thick glass partition. He watched as a federal agent leaned down to inform the elder Pokora, a Polish-born construction worker, that his only son wouldn't be returning to Canada for a very long time; his father responded by burying his head in his calloused hands.

Gutted to have caused the usually stoic man such anguish, David wished he could offer some words of comfort. "It's going to be OK, dad," he said in a soft voice, gesturing to get his attention. "It's going to be OK." But his father couldn't hear him through the glass.

II.

KINDERGARTEN SECURITY MISTAKES

Well before he could read or write, David Pokora mastered the intricacies of first-person shooters. There is a grainy video of him playing *Blake Stone: Aliens of Gold* in 1995, his 3-year-old fingers nimbly dancing around the keyboard of his parents' off-brand PC. What captivated him about the game was not its violence but rather the seeming magic of its controls; he wondered how a boxy beige machine could convert his physical actions into onscreen motion. The kid was a born programmer.

Pokora dabbled in coding throughout elementary school, building tools like basic web browsers. But he became wholly enamored with the craft as a preteen on a family trip to Poland. He had lugged his bulky laptop to the sleepy town where his parents' relatives lived. There was little else to do, so as chickens roamed the yards he passed the time by teaching himself the Visual Basic .NET programming language. The house where he stayed had no internet access, so Pokora couldn't Google for help when his programs spit out errors. But he kept chipping away at his code until it was immaculate, a labor-intensive process that filled him with unexpected joy. By the time he got back home, he was hooked on the psychological rewards of bending machines to his will.

As Pokora began to immerse himself in programming, his family bought its first Xbox. With its ability to connect to multiplayer sessions on the Xbox Live service and its familiar Windows-derived architecture, the machine made Pokora's Super Nintendo seem like a relic. Whenever he wasn't splattering aliens in *Halo*, Pokora scoured the internet for technical information about his new favorite plaything. His wanderings brought him into contact with a community of hackers who were redefining what the Xbox could do.

To divine its secrets, these hackers had cracked open the console's case and eavesdropped on the data that zipped between the motherboard's various components—the CPU, the RAM, the Flash chip. This led to the discovery of what the cryptography expert Bruce Schneier termed "lots of kindergarten security mistakes." For example, Microsoft had left the decryption key for the machine's boot code lying around in an accessible area of the machine's memory. When an MIT graduate student named Bunnie Huang located that key in 2002, he gave his hacker compatriots the power to trick the Xbox into booting up homebrew programs that could stream music, run Linux, or emulate Segas and Nintendos. All they had to do first was tweak their consoles' firmware, either by soldering a so-called mod-chip onto the motherboard or loading a hacked game-save file from a USB drive.

Once Pokora hacked his family's Xbox, he got heavy into tinkering with his cherished *Halo*. He haunted IRC channels and web forums where the best *Halo* programmers hung out, poring over tutorials on how to alter the physics of the game. He was soon making a name for himself by writing *Halo 2* utilities that allowed players to fill any of the game's landscapes with digitized water or change blue skies into rain.

The hacking free-for-all ended with the release of the second-generation Xbox, the Xbox 360, in November 2005. The 360 had none of the glaring security flaws of its predecessor, to the chagrin of programmers like the 13-year-old Pokora who could no longer run code that hadn't been approved by Microsoft. There was one potential workaround for frustrated hackers, but it required a rare piece of hardware: an Xbox 360 development kit.

Dev kits are the machines that Microsoft-approved developers use to write Xbox content. To the untrained eye they look like ordinary consoles, but the units contain most of the software integral to the game development process, including tools for line-by-line debugging. A hacker with a dev kit can manipulate Xbox software just like an authorized programmer.

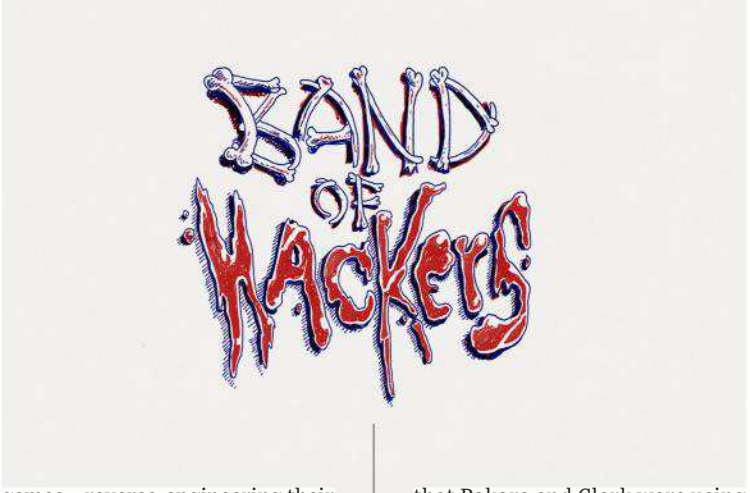
Microsoft sends dev kits only to rigorously screened game-development companies. In the mid-2000s a few kits would occasionally become available when a bankrupt developer dumped its assets in haste, but for the most part the hardware was seldom spotted in the wild. There was one hacker, however, who lucked into a mother lode of 360 dev kits and whose eagerness to profit off his good fortune would help Pokora ascend to the top of the Xbox scene.

III.

THE ONLY EDUCATION THAT MATTERED

In 2006, while working as a Wells Fargo technology manager in Walnut Creek, California, 38-year-old Rowdy Van Cleave learned that a nearby recycling facility was selling Xbox DVD drives cheap. When he went to inspect the merchandise, the facility's owners mentioned they received regular deliveries of surplus Microsoft hardware. Van Cleave, who'd been part of a revered Xbox-hacking crew called Team Avalaunch, volunteered to poke around the recyclers' warehouse and point out any Xbox junk that might have resale value.

Contributing editor **BRENDAN I. KOERNER** *(@brendankoerner) wrote about silicon theft in issue 25.10.*



After sifting through mountains of Xbox flotsam and jetsam, Van Cleave talked the recyclers into letting him take home five motherboards. When he jacked one of them into his Xbox 360 and booted it up, the screen gave him the option to activate debugging mode. "Holy shit," Van Cleave thought, "this is a frickin' dev motherboard!"

Aware that he had stumbled on the Xbox scene's equivalent of King Tut's tomb, Van Cleave cut a deal with the recyclers that let him buy whatever discarded Xbox hardware came their way. Some of these treasures he kept for his own sizable collection or handed out to friends; he once gave another Team Avalaunch member a dev kit as a wedding present. But Van Cleave was always on the lookout for paying customers he could trust to be discreet.

The 16-year-old Pokora became one of those customers in 2008, shortly after meeting Van Cleave through an online friend and impressing him with his technical prowess. In addition to buying kits for himself, Pokora acted as a salesman for Van Cleave, peddling hardware at significant markup to other *Halo* hackers; he charged around $1,000 per kit, though desperate souls sometimes ponied up as much as $3,000. (Van Cleave denies that Pokora sold kits on his behalf.) He befriended several of his customers, including a guy named Justin May who lived in Wilmington, Delaware.

Now flush with dev kits, Pokora was able to start modifying the recently released *Halo 3*. He kept vampire hours as he hacked, coding in a trance-like state that he termed "hyperfocus" until he dropped from exhaustion at around 3 or 4 am. He was often late for school, but he shrugged off his slumping grades; he considered programming on his dev kit to be the only education that mattered.

Pokora posted snippets of his *Halo 3* work on forums like Halomods.com, which is how he came to the attention of a hacker in Whittier, California, named Anthony Clark. The 18-year-old Clark had experience disassembling Xbox games—reverse-engineering their code from machine language into a programming language. He reached out to Pokora and proposed that they join forces on some projects.

Clark and Pokora grew close, talking nearly every day about programming as well as music, cars, and other adolescent fixations. Pokora sold Clark a dev kit so they could hack *Halo 3* in tandem; Clark, in turn, gave Pokora tips on the art of the disassembly. They cowrote a *Halo 3* tool that let them endow the protagonist, Master Chief, with special skills—like the ability to jump into the clouds or fire weird projectiles. And they logged countless hours playing their hacked creations on PartnerNet, a sandbox version of Xbox Live available only to dev kit owners.

As they released bits and pieces of their software online, Pokora and Clark began to hear from engineers at Microsoft and Bungie, the developer behind the *Halo* series. The professional programmers offered nothing but praise, despite knowing that Pokora and Clark were using ill-gotten dev kits. *Cool, you did a good job of reverse-engineering this*, they'd tell Pokora. The encouraging feedback convinced him that he was on an unorthodox path to a career in game development—perhaps the only path available to a construction worker's son from Mississauga who was no classroom star.

But Pokora and Clark occasionally flirted with darker hijinks. By 2009 the pair was using PartnerNet not only to play their modded versions of *Halo 3* but also to swipe unreleased software that was still being tested. There was one *Halo 3* map that Pokora snapped a picture of and then shared too liberally with friends; the screenshot wound up getting passed around among *Halo* fans. When Pokora and Clark next returned to PartnerNet to play *Halo 3*, they encountered a message on the game's main screen that Bungie engineers had expressly left for them: "Winners Don't Break Into PartnerNet."

GIFTED CANADIAN HACKER AND THE BRAINS OF THE XBOX UNDERGROUND

PROGRAMMER WHO MADE MILLIONS BY TRICKING *FIFA SOCCER* INTO MINTING VIRTUAL COINS

AUSTRALIAN TEENAGE HACKER WHO TURNED RECKLESS AS THE FBI CLOSED IN

The two hackers laughed off the warning. They considered their mischief all in good fun—they'd steal a beta here and there, but only because they loved the Xbox so much, not to enrich themselves. They saw no reason to stop playing cat and mouse with the Xbox pros, whom they hoped to call coworkers some day.

IV.

I MEAN, IT'S JUST VIDEOGAMES

The Xbox 360 remained largely invulnerable until late 2009, when security researchers finally identified a weakness: By affixing a modchip to an arcane set of motherboard pins used for quality-assurance testing, they managed to nullify the 360's defenses. The hack came to be known as the JTAG, after the Joint Test Action Group, the industry body that had recommended adding the pins to all printed circuit boards in the mid-1980s.

When news of the vulnerability broke, Xbox 360 owners rushed to get their consoles JTAGed by services that materialized overnight. With 23 million subscribers now on Xbox Live, multiplayer gaming had become vastly more competitive, and a throng of gamers whom Pokora dubbed "spoiled kids with their parents' credit cards" were willing to go to extraordinary lengths to humiliate their rivals.

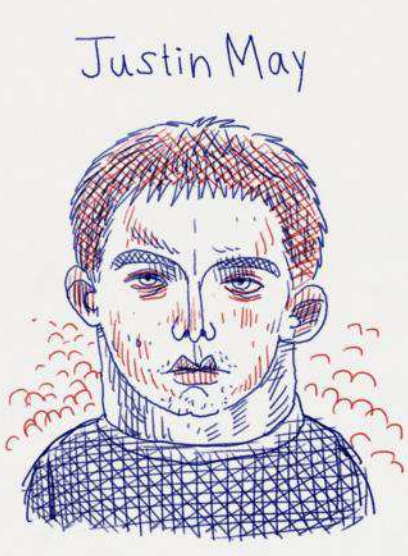
For Pokora and Clark, it was an opportunity to cash in. They hacked the *Call of Duty* series of military-themed shooters to create so-called modded lobbies—places on Xbox Live where *Call of Duty* players could join games governed by reality-bending rules. For fees that ranged up to $100 per half-hour, players with JTAGed consoles could participate in death matches while wielding superpowers: They could fly, walk through walls, sprint with Flash-like speed, or shoot bullets that never missed their targets.

For an extra $50 to $150, Pokora and Clark also offered "infections"—powers that players' characters would retain when they joined nonhacked games. Pokora was initially reluctant to sell infections: He knew his turbocharged clients would slaughter their hapless opponents, a situation that struck him as contrary to the spirit of gaming. But then the money started rolling in—as much as $8,000 on busy days. There were so many customers that he and Clark had to hire employees to deal with the madness. Swept up in the excitement of becoming an entrepreneur, Pokora forgot all about his commitment to fairness. It was one more step down a ladder he barely noticed he was descending.

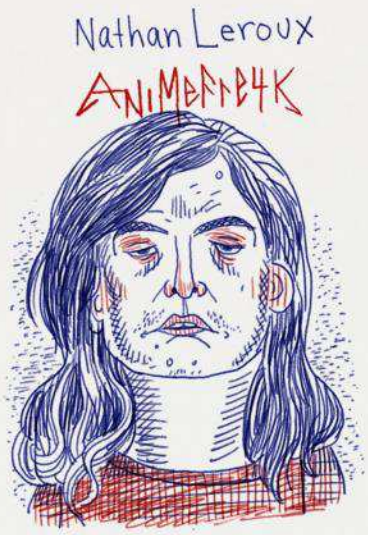
Microsoft tried to squelch breaches like the *Call of Duty* cheats by launching an automated system that could detect JTAGed consoles and ban them. But Pokora reverse-engineered the system and devised a way to beat it: He wrote a program that hijacked Xbox Live's security queries to an area of the console where they could be filled with false data, and thus be duped into certifying a hacked console.

Pokora reveled in the perks of his success. He still lived with his parents, but he paid his tuition as he entered the University of Toronto in the fall of 2010. He and his girlfriend dined at upscale restaurants every night and stayed at $400-a-night hotels as they traveled around Canada for metal rock shows. But he wasn't really in it for the money or even the adulation of his peers; what he most coveted was the sense of glee and power he derived from making $60 million games behave however he wished.

Pokora knew there was a whiff of the illegal about his *Call of Duty* business, which violated numerous copyrights. But he interpreted the lack of meaningful pushback from either Microsoft or Activision, *Call of Duty*'s developer, as a sign that the companies would tolerate his enterprise, much as Bungie had put up with his *Halo 3* shenanigans. Activision did send a series of cease-and-desist letters, but the company never followed through on its threats.



POKORA'S FRIEND IN DELAWARE. ARRESTED IN 2010 FOR TRYING TO STEAL A GAME'S SOURCE CODE



ABRUPTLY VANISHED FROM THE XBOX HACKING SCENE, CAUSING WIDESPREAD PARANOIA

OWNER OF A HACKED MODEM THAT HE USED TO HELP THE XBOX UNDERGROUND STEAL SOFTWARE

"I mean, it's just videogames," Pokora told himself whenever another Activision letter arrived. "It's not like we're hacking into a server or stealing anyone's information." That would come soon enough.

V.

TUNNELS

Dylan Wheeler, a hacker in Perth, Australia, whose alias was SuperDaE, knew that something juicy had fallen into his lap. An American friend of his who went by the name Gamerfreak had slipped him a password list for the public forums operated by Epic Games, a Cary, North Carolina, game developer known for its *Unreal* and *Gears of War* series. In 2010 Wheeler started poking around the forums' accounts to see if any of them belonged to Epic employees. He eventually identified a member of the company's IT department whose employee email address and password appeared on Gamerfreak's list; rummaging through the man's personal emails, Wheeler found a password for an internal EpicGames.com account.

Once he had a toehold at Epic, Wheeler wanted a talented partner to help him sally deeper into the network. "Who is big enough to be interested in something like this?" he wondered. Xenomega—David Pokora—whom he'd long admired from afar and was eager to befriend, was the first name that popped to mind. Wheeler cold-messaged the Canadian and offered him the chance to get inside one of the world's preeminent game developers; he didn't mention that he was only 14, fearing that his age would be a deal breaker.

What Wheeler was proposing was substantially shadier than anything Pokora had attempted before: It was one thing to download *Halo* maps from the semipublic PartnerNet and quite another to break into a fortified private network where a company stores its most sensitive data. But Pokora was overwhelmed by curiosity about what software he might unearth on Epic's servers and titillated by the prospect of reverse-engineering a trove of top-secret games. And so he rationalized what he was about to do by setting ground rules—he wouldn't take any credit card numbers, for example, nor peek at personal information about Epic's customers.

Pokora and Wheeler combed through Epic's network by masquerading as the IT worker whose login credentials Wheeler had compromised. They located a plugged-in USB drive that held all of the company's passwords, including one that gave them root access to the entire network. Then they pried into the computers of Epic bigwigs such as design director Cliff "CliffyB" Bleszinski; the pair chortled when they opened a music folder that Bleszinski had made for his Lamborghini and saw that it contained lots of Katy Perry and Miley Cyrus tunes. (Bleszinski, who left Epic in 2012, confirms the hackers' account, adding that he's "always been public and forthright about my taste for bubblegum pop.")

To exfiltrate Epic's data, Wheeler enlisted the help of Sanadodeh "Sonic" Nesheiwat, a New Jersey gamer who possessed a hacked cable modem that could obfuscate its location. In June 2011 Nesheiwat downloaded a prerelease copy of *Gears of War 3* from Epic, along with hundreds of gigabytes of other software. He burned Epic's source code onto eight Blu-ray discs that he shipped to Pokora in a package marked WEDDING VIDEOS. Pokora shared the game with several friends, including his dev kit customer Justin May; within days a copy showed up on the Pirate Bay, a notorious BitTorrent site.

The *Gears of War 3* leak triggered a federal investigation, and Epic began working with the FBI to determine how its security had been breached. Pokora and Wheeler found out about the nascent probe while reading Epic's emails; they freaked out when one of those emails described a meeting between the company's brain trust and FBI agents. "I need your help—I'm going to get arrested," a panicked Pokora wrote to May that July. "I need to encrypt some hard drives."

But the email chatter between Epic and the FBI quickly died down, and the company made no apparent effort to block the hackers' root access to the network—a sign that it couldn't pinpoint their means of entry. Having survived their first brush with the law, the hackers felt emboldened—the brazen Wheeler most of all. He kept trespassing on sensitive areas of Epic's network, making few efforts to conceal his IP address as he spied on high-level corporate meetings through webcams he'd commandeered. "He knowingly logs into Epic knowing that the feds chill there," Nesheiwat told Pokora about their Australian partner. "They were emailing FBI people, but he still manages to not care."

Owning Epic's network gave the hackers entrée to a slew of other organizations. Pokora and Wheeler came across login credentials for Scaleform, a so-called middleware company that provided technology for the engine at the heart of Epic's games. Once they'd broken into Scaleform, they discovered that the company's network was full of credentials for Silicon Valley titans, Hollywood entertainment conglomerates, and Zombie Studios, the developer of the *Spec Ops* series of games. On Zombie's network they uncovered remote-access "tunnels" to its clients, including branches of the American military. Wriggling through those poorly secured tunnels was no great challenge, though Pokora was wary of leaving behind too many digital tracks. "If they notice any of this," he told the group, "they're going to come looking for me."

As the scale of their enterprise increased, the hackers discussed what they should do if the FBI came knocking. High off the feeling of omnipotence that came from burrowing into supposedly impregnable networks, Pokora proposed releasing all of Epic's proprietary data as an act of revenge: "If we ever go disap-


2014
FIFA
WORLD CUP
THE MOTHER OF ALL BOARDS
ARMAN THE Cyber
DURANGO

pearing, just, you know, upload it to the internet and say fuck you Epic."

The group also cracked jokes about what they should call their prison gang. Everyone dug Wheeler's tongue-in-cheek suggestion that they could strike fear into other inmates' hearts by dubbing themselves the Xbox Underground.

VI.

HOW DO WE END IT?

Pokora was becoming ever more infatuated with his forays into corporate networks, and his old friends from the Xbox scene feared for his future. Kevin Skitzo, a Team Avalaunch hacker, urged him to pull back from the abyss. "Dude, just stop this shit," he implored Pokora. "Focus on school, because this shit? I mean, I get it—it's a high. But as technology progresses and law enforcement gets more aware, you can only dodge that bullet for so long."

But Pokora was too caught up in the thrill of stockpiling forbidden software to heed this advice. In September 2011 he stole a prerelease copy of *Call of Duty: Modern Warfare 3*. "Let's get arrested," he quipped to his friends as he started the download.

Though he was turning cocky as he swung from network to network without consequence, Pokora still took pride in how little he cared about money. After seizing a database that contained "a fuckton of PayPals," Pokora sang his own praises to his associates for resisting the temptation to profit off the accounts. "We could already have sold them for Bitcoins which would have been untraceable if we did it right. It could have already been easily an easy fifty grand."

But with each passing week, Pokora became a little bit more mercenary. In November 2011, for example, he asked his friend May to broker a deal with a gamer who went by Xboxdevguy, who'd expressed an interest in buying prerelease games. Pokora was willing to deliver any titles Xboxdevguy desired for a few hundred dollars each.

Pokora's close relationship with May made his hacker cohorts uneasy. They knew that May had been arrested at a Boston gaming convention in March 2010 for trying to download the source code for the first-person shooter *Breach*. A spokesperson for the game's developer told the tech blog Engadget that, upon being caught after a brief foot chase, May had said he "could give us bigger and more important people and he could 'name names.'" But Pokora trusted May because he'd watched him participate in many crooked endeavors; he couldn't imagine that anyone in cahoots with law enforcement would be allowed to do so much dirt.

By the spring of 2012, Pokora and Wheeler were focused on pillaging the network of Zombie Studios. Their crew now included two new faces from the scene: Austin "AAmonkey" Alcala, an Indiana high school kid, and Nathan "animefre4k" Leroux, the homeschooled son of a diesel mechanic from Bowie, Maryland. Leroux, in particular, was an exceptional talent: He'd cowritten a program that could trick Electronic Arts' soccer game *FIFA 2012* into minting the virtual coins that players get for completing matches, and which are used to buy character upgrades.

While navigating through Zombie's network, the group stumbled on a tunnel to a US Army server; it contained a simulator for the AH-64D Apache helicopter that Zombie was developing on a Pentagon contract. Ever the wild man, Wheeler downloaded the software and told his colleagues they should "sell the simulators to the Arabs."

The hackers were also busy tormenting Microsoft, stealing documents that contained specs for an early version of the Durango, the codename for the next-generation Xbox—a machine that would come to be known as the Xbox One. Rather than sell the documents to a Microsoft competitor, the hackers opted for a more byzantine scheme: They would counterfeit and sell a Durango themselves, using off-the-shelf components. Leroux volunteered to do the assembly in exchange for a cut of the proceeds; he needed money to pay for online computer science classes at the University of Maryland.

The hackers put out feelers around the scene and found a buyer in the Seychelles who was willing to pay $5,000 for the counterfeit console. May picked up the completed machine from Leroux's house and promised to ship it to the archipelago in the Indian Ocean.

But the Durango never arrived at its destination. When the buyer complained, paranoia set in: Had the FBI intercepted the shipment? Were they now all under surveillance?

Wheeler was especially unsettled: He'd thought the crew was untouchable after the Epic investigation appeared to stall, but now he felt certain that everyone was about to get hammered by a racketeering case. "How do we end this game?" he asked himself. The answer he came up with was to go down in a blaze of glory, to do things that would ensure his place in Xbox lore.

Wheeler launched his campaign for notoriety by posting a Durango for sale on eBay, using photographs of the one that Leroux had built. The bidding for the nonexistent machine reached $20,100 before eBay canceled the auction, declaring it fraudulent. Infuriated by the media attention the saga generated, Pokora cut off contact with Wheeler.

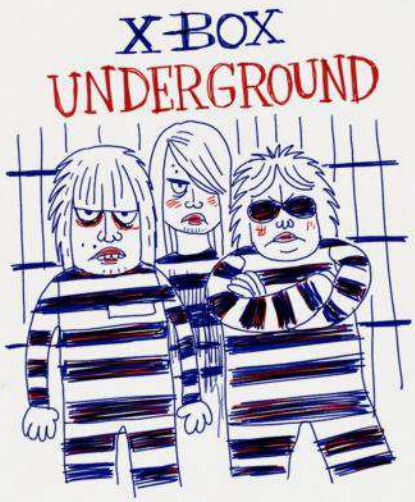
A few weeks later, Leroux vanished from the scene; rumors swirled that he'd been raided by the FBI. Americans close to Pokora began to tell him they were being tailed by black cars with tinted windows. The hackers suspected there might be an informant in their midst.

VII.

PERSON A

The relationship between Pokora and Clark soured as Pokora got deeper into hacking developers. The two finally fell out over staffing issues at

THE HACKERS CRACKED JOKES ABOUT WHAT THEY SHOULD CALL THEIR PRISON GANG. EVERYONE DUG WHEELER'S TONGUE-IN-CHEEK SUGGESTION THAT THEY COULD STRIKE FEAR INTO THE HEARTS OF OTHER INMATES BY DUBBING THEMSELVES THE XBOX UNDERGROUND.



their *Call of Duty* business—for example, they hired some workers whom Pokora considered greedy, but Clark refused to call them out. Sick of dealing with such friction, both men drifted into other ventures. Pokora focused on Horizon, an Xbox cheating service that he built on the side with some friends; he liked that Horizon's cheats couldn't be used on Xbox Live, which meant fewer potential technical and legal headaches. Clark, meanwhile, refined Leroux's *FIFA* coin-minting technology and started selling the virtual currency on the black market. Austin Alcala, who'd participated in the hack of Zombie Studios and the Xbox One counterfeiting caper, worked for Clark's new venture.

As the now 20-year-old Pokora split his energies between helping to run Horizon and attending university, Wheeler continued his kamikaze quest for attention. In the wake of his eBay stunt, Microsoft sent a private investigator named Miles Hawkes to Perth to confront him. Wheeler posted on Twitter about meeting "Mr. Microsoft Man," who pressed him for information about his collaborators over lunch at the Hyatt. According to Wheeler, Hawkes told him not to worry about any legal repercussions, as Microsoft was only interested in going after "real assholes." (Microsoft denies that Hawkes said this.)

In December 2012 the FBI raided Sanadodeh Nesheiwat's home in New Jersey. Nesheiwat posted an unredacted version of the search warrant online. Wheeler reacted by doxing the agents in a public forum and encouraging people to harass them; he also spoke openly about hiring a hitman to murder the federal judge who'd signed the warrant.

Wheeler's bizarre compulsion to escalate every situation alarmed federal prosecutors, who'd been carefully building a case against the hackers since the *Gears of War* leak in June 2011. Edward McAndrew, the assistant US attorney who was leading the investigation, felt he needed to accelerate the pace of his team's work before Wheeler sparked real violence.

On the morning of February 19, 2013, Wheeler was working in his family's home in Perth when he noticed a commotion in the yard below his window. A phalanx of men in light tactical gear was approaching the house, Glocks holstered by their sides. Wheeler scrambled to shut down all of his computers, so that whoever would be dissecting his hardware would at least have to crack his passwords.

Over the next few hours, Australian police carted away what Wheeler estimated to be more than $20,000 worth of computer equipment; Wheeler was miffed that no one bothered to place his precious hard drives in antistatic bags. He wasn't jailed that day, but his hard drives yielded a bounty of incriminating evidence: Wheeler had taken frequent screenshots of his hacking exploits, such as a chat in which he proposed running "some crazy program to fuck the fans


PERSON
A
CANADA
It's going to be OK, Dad.
THIS LIFE AIN'T FOR YOU.
OHIO

up" on Zombie Studios' servers.

That July, Pokora told Justin May he was about to attend Defcon, the annual hacker gathering in Las Vegas—his first trip across the border in years. On July 23, McAndrew and his colleagues filed a sealed 16-count indictment against Pokora, Nesheiwat, and Leroux, charging them with crimes including wire fraud, identify theft, and conspiracy to steal trade secrets; Wheeler and Gamerfreak, the original source of the Epic password list, were named as unindicted coconspirators. (Alcala would be added as a defendant four months later.) The document revealed that much of the government's case was built on evidence supplied by an informant referred to as Person A. He was described as a Delaware resident who had picked up the counterfeit Durango from Leroux's house, then handed it over to the FBI.

Prosecutors also characterized the defendants as members of the "Xbox Underground." Wheeler's prison-gang joke was a joke no longer.

Though he knew nothing about the secret indictment, Pokora was too busy to go to Defcon and pulled out at the last minute. The FBI worried that arresting his American coconspirators would spur him to go on the lam, so the agency decided to wait for him to journey south before rolling up the crew.

Two months later, Pokora went to the Toronto Opera House for a show by the Swedish metal band Katatonia. His phone buzzed as a warm-up act was tearing through a song—it was Alcala, now a high school senior in Fishers, Indiana. He was tittering with excitement: He said he knew a guy who could get them both the latest Durango prototypes—real ones, not counterfeits like the machine they'd made the summer before. His connection was willing to break into a building on Microsoft's Redmond campus to steal them. In exchange, the burglar was demanding login credentials for Microsoft's game developer network plus a few thousand dollars. Pokora was baffled by the aspiring burglar's audacity. "This guy's stupid," he thought. But after years of pushing his luck, Pokora was no longer in the habit of listening to his own common sense. He told Alcala to put them in touch.

The burglar was a recent high school graduate named Arman, known on the scene as ArmanTheCyber. (He agreed to share his story on the condition that his last name not be used.) A year earlier he'd cloned a Microsoft employee badge that belonged to his mother's boyfriend; he'd been using the RFID card to explore the Redmond campus ever since, passing as an employee by dressing head to toe in Microsoft swag. (Microsoft claims he didn't copy the badge but rather stole it.) The 18-year-old had already stolen one Durango for personal use; he was nervous about going back for more but also brimming with the recklessness of youth.

Around 9 pm on a late September night, Arman swiped himself into the building that housed

the Durangos. A few engineers were still roaming the hallways; Arman dove into a cubicle and hid whenever he heard footsteps. He eventually climbed the stairs to the fifth floor, where he'd heard there was a cache of Durangos. As he started to make his way into the darkened floor, motion detectors sensed his presence and light flooded the room. Spooked, Arman bolted back downstairs.

He finally found what he was looking for in two third-floor cubicles. One of the Durangos had a pair of stiletto heels atop the case; Arman put the two consoles in his oversize backpack and left the fancy shoes on the carpet.

A week after he sent the stolen Durangos to Pokora and Alcala, Arman received some surprising news: A Microsoft vendor had finally reviewed an employment application he'd submitted that summer and hired him as a quality-assurance tester. He lasted only a couple weeks on the job before investigators identified him as the Durango thief; a stairwell camera had caught him leaving the building. To minimize the legal fallout, he begged Pokora and Alcala to send back the stolen consoles. He also returned the Durango he'd taken for himself, and not a moment too soon: Jealous hackers had been scoping out his house online, as a prelude to executing a robbery.

Pokora spent all winter hacking the Xbox 360's games for Horizon. But as Toronto was beginning to thaw out in March 2014, he figured he could spare a weekend to drive down to Delaware and pick up the bumper he'd ordered for his Volkswagen Golf.

"Y'know, there's a chance I could get arrested," he told his dad as they prepared to leave. His father had no idea what he was talking about and cracked a thin smile at what was surely a bad joke.

VIII.

"THIS LIFE AIN'T FOR YOU"

After an initial appearance at the federal courthouse in Buffalo and a few days in a nearby county jail, Pokora was loaded into a van alongside another federal inmate, a gang member with a powerlifter's arms and no discernible neck. They were being transported to a private prison in Ohio, where Pokora would be held until the court in Delaware was ready to start its proceedings against him. For kicks, he says, the guards tossed the prisoners' sandwiches onto the floor of the van, knowing that the tightly shackled men couldn't reach them.

During the three-hour journey, the gang member, who was serving time for beating a man with a hammer, counseled Pokora to do whatever was necessary to minimize his time behind bars. "This life ain't for you," he said. "This life ain't for nobody, really."

Pokora took those words to heart when he was finally brought to Delaware in early April 2014. He quickly accepted the plea deal that was offered, and he helped the victimized companies identify the vulnerabilities he'd exploited—for example, the lightly protected tunnels that let him hopscotch among networks. As he sat in rooms and listened to Pokora explain his hacks with professorial flair, McAndrew, the lead prosecutor, took a shine to the now 22-year-old Canadian. "He's a very talented kid who started down a bad path," he says. "A lot of times when you're investigating these things, you have to have a certain level of admiration for the brilliance and creativity of the work. But then you kind of step back and say, 'Here's where it went wrong.'"

One day, on the way from jail to court, Pokora was placed in a marshal's vehicle with someone who looked familiar—a pale 20-year-old guy with a wispy build and teeth marred by a Skittles habit. It was Nathan Leroux, whom Pokora had never met in person but recognized from a photo. He had been arrested on March 31 in Madison, Wisconsin, where he'd moved after the FBI raid that had scared him into dropping out of the Xbox scene. He'd been flourishing in his new life as a programmer at Human Head Studios, a small game developer, when the feds showed up to take him into custody.

As he and Leroux rode to court in shackles, Pokora tried to pass along the gang member's advice. "Look, a lot of this was escalated because of DaE—DaE's an asshole," he said, using the shorthand of Wheeler's nickname, SuperDaE. "You can rat on me or do whatever, because you don't deserve this shit. Let's just do what we got to do and get out of here."

Unlike Pokora, Leroux was granted bail and was allowed to live with his parents as his case progressed. But as he lingered at his Maryland home, he grew convinced that, given his diminutive stature and shy nature, he was doomed to be raped or murdered if he went to prison. His fear became so overpowering that, on June 16, he clipped off his ankle monitor and fled.

He paid a friend to try to smuggle him into Canada, nearly 400 miles to the north. But their long drive ended in futility: The Canadians flagged the car at the border. Rather than accept that his escape had failed, Leroux pulled out a knife and tried to sprint across the bridge onto Canadian soil. When officers surrounded him, he decided he had just one option left: He stabbed himself multiple times. Doctors at an Ontario hospital managed to save his life. Once he was released from intensive care and transported back to Buffalo, his bail was revoked.

When it came time for Pokora's sentencing, his attorney argued for leniency by contending that his client had lost the ability to differentiate play from crime. "David in the real world was something else entirely from David online," he wrote in his sentencing memorandum. "But it was in this tenebrous world of anonymity, frontier rules, and private communication set at a remove from everyday life that David was incrementally desensitized to an online culture in which the line between playing a videogame and hacking into a computer network narrowed to the vanishing point."

After pleading guilty, Pokora, Leroux, and Nesheiwat ultimately received similar punishments: 18 months in prison for Pokora and Nesheiwat, 24 months for Leroux. Pokora did the majority of his time at the Federal Detention Center in Philadelphia, where he made use of the computer room to send emails or listen to MP3s. Once, while waiting for a terminal to open up, a mentally unstable inmate got in his face, and Pokora defended himself so he wouldn't appear weak; the brawl ended when a guard blasted him with pepper spray. After finishing his prison sentence, Pokora spent several more months awaiting deportation to Canada in an immigration detention facility in Newark, New Jersey. That jail had PCs in the law library, and Pokora got to use his hacker skills to find and play a hidden version of *Microsoft Solitaire*.

When he finally returned to Mississauga in October 2015, Pokora texted his old friend Anthony Clark, who was now facing a legal predicament of his own. Alcala had told the government all about Clark's *FIFA* coin-minting operation. The enterprise had already been on the IRS's radar: One of Clark's workers had come under suspicion for withdrawing as much as $30,000 a day from a Dallas bank account. Alcala connected the dots for the feds, explaining to them that the business could fool Electronic Arts' servers into spitting out thousands of coins per second: The group's code automated and accelerated *FIFA*'s gameplay, so that more than 11,500 matches could be completed in the time it took a human to finish just one. The information he provided led to the indictment of Clark and three others for wire fraud; they had allegedly grossed $16 million by selling the *FIFA* coins, primarily to a Chinese businessman they knew only as Tao.

Though Clark's three codefendants had all pleaded guilty, he was intent on going to trial. He felt that he had done nothing wrong, especially since Electronic Arts' terms of service state that its *FIFA* coins have no real value. Besides, if Electronic Arts executives were really upset about his operation, why didn't they reach out to discuss the matter like adults? Perhaps Electronic Arts was just jealous that he—not they—had figured out how to generate revenue from in-game currencies.

"Yeah, I'm facing 8+ years," Clark wrote in a text to Pokora. "And if I take the plea 3½. Either way fuck them. They keep trying to get me to plea."

"They roof you if you fail at trial," Pokora warned. "My only concern is to educate you a bit about what it will be like. Because it's a shitty thing to go through." But Clark wouldn't be swayed—he was a man of principle.

That Fourth of July, Pokora wrote to Clark again. He jokingly asked why Clark hadn't yet sent him a custom video that he'd requested: Clark and his Mexican-American relatives

dancing to salsa music beneath a Donald Trump piñata. "Where's the salsa?" Pokora asked.

The reply came back: "On my chips," followed by the smiling-face-with-sunglasses emoji. It was the last time Pokora ever heard from his *Halo 3* comrade.

Clark's trial in federal district court in Fort Worth that November did not go as he had hoped: He was convicted on one count of conspiracy to commit wire fraud. His attorneys thought he had excellent grounds for appeal, since they believed that the prosecution had failed to prove the *FIFA* coin business had caused Electronic Arts any actual harm.

But Clark's legal team never got the chance to make that case. On February 26, 2017, about a month before he was scheduled to be sentenced, Clark died in his Whittier home. People close to his family insist that the death was accidental, the result of a lethal interaction between alcohol and medication. Clark had just turned 27 and left behind an estate valued at more than $4 million.

IX.

"I WANTED TO SEE HOW FAR IT COULD GO"

The members of the Xbox Underground have readjusted to civilian life with varying degrees of success. In exchange for his cooperation, Alcala received no prison time; he enrolled at Ball State University and made the dean's list. The 20-year-old brought his girlfriend to his April 2016 sentencing hearing—"my first real girlfriend"—and spoke about a talk he'd given at an FBI conference on infrastructure protection. "The world is your oyster," the judge told him.

Leroux's coworkers at Human Head Studios sent letters to the court on his behalf, commending his intelligence and kindness. "He has a very promising game development career ahead of him, and I wouldn't think he'd ever again risk throwing that away," one supporter wrote. On his release from prison, Leroux returned to Madison to rejoin the company.

Nesheiwat, who was 28 at the time of his arrest, did not fare as well as his younger colleagues. He struggled with addiction and was rearrested last December for violating his probation by using cocaine and opiates; his probation officer said he'd "admitted to doing up to 50 bags of heroin per day" before his most recent stint in rehab.

Because Wheeler had been a juvenile when most of the hacking occurred, the US decided to leave his prosecution to the Australian authorities. After being given 48 hours to turn in his passport, Wheeler drove straight to the airport and absconded to the Czech Republic, his mother's native land. The Australians imprisoned his mother for aiding his escape, presumably to pressure him into returning home to face justice. (She has since been released.) But Wheeler elected to remain a fugitive, drifting through Europe on an EU passport before eventually settling in the UK. During his travels he tried to crowdfund the purchase of a $500,000 Ferrari, explaining that his doctor said he needed the car to cope with the anxiety caused by his legal travails. (The campaign did not succeed.)

Pokora, who is now 26, was disoriented during his first months back in Canada. He feared that his brain had permanently rotted in prison, a place where intellectual stimulation is in short supply. But he reunited with his girlfriend, whom he'd begged to leave him while he was behind bars, and he reenrolled at the University of Toronto. He scraped together the tuition by taking on freelance projects programming user-interface automation tools; his financial struggles made him nostalgic for the days when he was rolling in *Call of Duty* cash.

When he learned of Clark's death, Pokora briefly felt renewed bitterness toward Alcala, who'd been instrumental to the government's case against his friend. But he let the anger pass. There was nothing to be gained by holding a grudge against his onetime fellow travelers. He couldn't even work up much resentment against Justin May, whom he and many others are certain was the Delaware-based FBI informant identified as Person A in the Xbox Underground indictment. ("Can't comment on that, sorry," May responded when asked whether he was Person A. He is currently being prosecuted in the federal district of eastern Pennsylvania for defrauding Cisco and Microsoft out of millions of dollars' worth of hardware.)

Pokora still struggles to understand how his love for programming warped into an obsession that knocked his moral compass so far askew. "As much as I consciously made the decisions I did, I never meant for it to get as bad as it did," he says. "I mean, I wanted access to companies to read some source code, I wanted to learn, I wanted to see how far it could go—that was it. It was really just intellectual curiosity. I didn't want money—if I wanted money, I would've taken all the money that was there. But, I mean, I get it—what it turned into, it's regrettable."

Pokora knows he'll forever be persona non grata in the gaming industry, so he's been looking elsewhere for full-time employment since finishing the classwork for his computer science degree last June. But he's had a tough time putting together a portfolio of his best work: At the behest of the FBI, Canadian authorities seized all of the computers he'd owned prior to his arrest, and most of the software he'd created during his Xbox heyday was lost forever. They did let him keep his 2013 Volkswagen Golf, however, the car he adores so much that he was willing to drive to Delaware for a bumper. He keeps it parked at his parents' house in Mississauga, the place where he played his first game at the age of 2, and where he's lived ever since leaving prison.

"I NEVER MEANT FOR IT TO GET AS BAD AS IT DID," POKORA SAYS.

MOVE SLOW AND TEST THINGS

Uber CEO Dara Khosrowshahi | Photograph by Floto + Warner

THINGS

UBER'S NEW CEO IS A CHAMPION OF EVERYTHING UBER ONCE REJECTED: CAUTION, DISCIPLINE, AND TACT. CAN HE REFORM THE MOST AUDACIOUS, RULE-FLOUTING COMPANY IN SILICON VALLEY?

BY_ JESSI HEMPEL

IN THE LATE 1950S, A WEAPONS MAKER CALLED the Martin Company received a contract to build the first Pershing missile. It was to be the most sophisticated mobile weapons system on earth: 5 tons of metal and precision technology designed to deliver a nuclear warhead from up to 460 miles away. Should it ever be used, there would be no margin for error. It had to be perfect. And the US Army wanted it delivered quickly.

The task of ensuring this timely perfection fell to Philip Crosby, a quality-control manager at Martin. To break with his industry's wartime habit of tolerating small mistakes in feverish production, Crosby came up with a philosophy he would later call Zero Defects. The idea was, basically, to instill in workers the will to prevent problems during design and manufacture rather than go back and fix them later. Crosby's philosophy went on to become a management buzzword, especially in the aerospace and auto industries, where a faulty gasket or a weak bearing could mean a fiery catastrophe. During the Apollo program, NASA even gave out little Zero Defects trophies—each one a cute pewter spaceman standing on the moon with the letters "ZD" emblazoned on his chest.

"I'm a big believer in the Zero Defects strategy," said Dara Khosrowshahi, the CEO of Uber. It was an overcast day in January, and Khosrowshahi leaned back in a chair at Uber's San Francisco headquarters. Khosrowshahi had been running Uber for four months at that point. He'd left a stable perch at Expedia, the travel-booking service, to take over a company that had become synonymous with scandal and rule-breaking excess. And, having doused some of the raging fires left behind by his predecessor, Travis Kalanick, Khosrowshahi had determined that what Uber needed most was a quality-control philosophy borrowed from the middle of the last century.

This was, it must be said, a bit weird. Tech companies tend to celebrate the inverse of Zero Defects. Push out new code, experiment, screw things up, and fix them. "Move fast and break things," as Mark Zuckerberg famously said in the early days of Facebook. And arguably, few companies have moved faster and broken more things than Uber.

In just nine years, Kalanick's company grew from a vague notion that anyone should be able to summon a ride from their phone into a business valued at $54 billion and available in more than 600 cities on six continents. And it kept adding new services: Today Uber can facilitate a carpool to work and deliver your Dos Toros burritos so they're still hot when they reach your table. Not satisfied with merely replacing taxis, Kalanick's Uber began developing autonomous cars and trucks and even set up a skunkworks for flying electric cars. Along the way, the company left a trail of wreckage. It disregarded and even undermined laws and regulations; it squandered the loyalty of its drivers, who felt mistreated under its contractor system; and it became notorious for a workplace cul-

1

2

[1]
In San Francisco, Uber is trying to improve its mapping.

Alex Walsh

[2]
The self-driving hardware team works in an R&D lab in Pittsburgh.

Floto + Warner

ture that exemplified the worst tendencies of the Silicon Valley bro. By the time investors moved to demand Kalanick's resignation in June 2017, observers were calling Uber the world's most dysfunctional startup.

But where others saw Uber's travails as a symbol of Silicon Valley comeuppance, Khosrowshahi saw something less loaded: a sophisticated tech company that had taken on too much, too quickly, and whose systems groaned under the weight and confusion. Growth, not quality, had been its guiding principle for too long, he said.

Khosrowshahi, 48, has a neatly trimmed salt-and-pepper beard. On that day in January, he wore a long-sleeved black crewneck sweater, black pants, loafers, and brightly colored striped socks. In contrast to Kalanick, who is an inveterate pacer, he sat very still with his ankle crossed over his knee. Khosrowshahi's vision for Uber, as he relayed it, was to ask people to do their jobs correctly every single day. "It's a game of inches," he said.

At the time, Khosrowshahi was referring to the need to fix small-bore things—a rider has to wait a few minutes longer than the app promised, a driver can't get help with a technical issue—that add up to larger reputational problems. Then, in mid-March, came a true catastrophe. An Uber car operating in self-driving mode struck and killed a woman crossing the street in Tempe, Arizona. Within a few hours, the company announced that it was suspending its testing of driverless vehicles. When this article went to press, there was no official answer as to what had gone wrong, or whether quality controls would have made a difference. But suddenly, getting things right, every single time, seemed a lot more consequential.

T

THE STORY OF UBER IS SO WELL KNOWN NOW that it feels almost like a parable: Kalanick, a reader of Ayn Rand and self-styled badass, teamed up with a friend to start a service that would help their buddies get around San Francisco "like ballers." Uber blasted through every expectation to become a new genre of company, inspiring a bonanza of "Like Uber, but for X" clones (along with direct competitors like Lyft and, in China, Didi). The company came to embody a culture in which almost anything was acceptable. In a 2013 email instructing employees not to party too hard during a retreat in Miami, Kalanick summed up the ethos: "We do not have a budget to bail anyone out of jail. Don't be that guy. #clm"—internet slang for "career limiting move." The subtext: Your career won't be limited by bad behavior, so long as it stops short of arrest.

Kalanick also fostered an undercurrent of paranoia and suspicion in the ranks. He had architects design difficult-to-find conference rooms at the end of dead-end hallways. The glass partitions were often covered over with paper, and inside small groups of people worked, empowered to launch new projects that no one else at the company knew about.

This cloak-and-dagger behavior extended outside the company. Richard Jacobs, a former Uber security employee, asserted that in 2016 the company hacked into competitors' networks, impersonated riders on their platforms, secretly recorded people, and communicated internally using the encrypted Wickr app "for the express purpose of destroying evidence of illegal or unethical practices," as Jacobs' lawyer wrote in a letter in May of last year. (Uber says it hasn't substantiated those claims but intends to "compete honestly and fairly" going forward.)

To Kalanick, any outward display of insecurity was a liability. He didn't show it, nor did he tolerate it in others. He ran toward conflict, an attitude that helped the company push into new markets, and inspired staffers to put in long hours. But when Uber began to enter a tailspin—as it did precipitously in early 2017—this approach no longer conveyed authority.

The final unraveling of Kalanick's reign started the week after Donald Trump was inaugurated as president. On January 27, Trump signed an executive order barring people from seven predominantly Muslim countries from entering the United States. Protests sprang up all over, and New York City taxi drivers went on a one-hour work stoppage at JFK Airport to protest the ban. Uber, however, kept its drivers on the road, fueling the perception that the company was profiteering. A #deleteuber social media campaign went viral, and more than 200,000 people wiped out their accounts.

Things got much worse from there. In February a former Uber engineer named Susan Fowler published a blog post alleging that her manager had propositioned her and that, when she complained to human resources, the company not only failed to act but lied to her and other women about his history of transgressions. The company, she wrote, defended the harasser as a "high performer."

Just days later, another crisis hit. Waymo, the self-driving division of Alphabet, Google's parent company, filed a suit against Uber, charging that the company had stolen trade secrets and technology. Then, in March, *The New York Times* revealed that Uber had used a secret software tool to circumvent government inspections. That same week, a video surfaced in which Kalanick sat, legs splayed, between two female companions in the back of an upscale Uber Black car. When he berated the driver, he didn't come off as powerful. He came off as an asshole.

By then, Uber was in full-on crisis, and it didn't have systems in place to fix itself. For six months there had been no head of human resources. Liane Hornsey, who'd worked at Google in its fast-growth days, finally came aboard in January, just three weeks before Fowler published her post. Hornsey remembers attending her first all-hands meeting the next Tuesday. It was then that she realized the enormity of the task ahead. As Kalanick—the guy who'd referred to his startup in a 2014 *GQ* article as "Boob-er," for the way it delivered women to him on demand—promised that things would get better, she watched a range of emotions play across employees' faces from her seat on the stage. "There were people crying," she recalls.

In the following weeks, Hornsey held listening groups. Many people began reporting their own mistreatment, while others defended Kalanick. Hornsey received 215 complaints about sexual harassment, discrimination, bullying, or retaliation. More than 20 people lost their jobs.

As scandal and reports of feuding between Kalanick and his board surfaced in the press, the company's midlevel managers struggled to hold together what's known at Uber as "the marketplace"—the network of drivers and riders, as mediated by the company's technology. Daniel Graf, who worked in the product division, recalled "nonstop fire drills" during this period. His team knew the problem: The Uber app's technological foundation needed an overhaul. Because the company had built its tech for a smaller service and added to it rapidly as Uber expanded, it had to be fortified and rebuilt. Meanwhile, the senior managers kept disappearing. Kalanick asked Graf to head the product division after his predecessor resigned abruptly. Then, on June 20, after a long battle with investors on his board, Kalanick resigned."I had three bosses in one week," Graf said. It was a destabilizing time.

Both Hornsey and Graf were named to a 14-person executive leadership team that ran the company while the board looked for a new CEO. Some, like Hornsey, were new. Others, like Graf, had been promoted when their bosses left or were fired. Among them were a vocal group of Kalanick supporters, who felt that even if he had been a belligerent jerk, his vision was essential to Uber's future. Most knew little about any part of the company other than their own.

There was nothing glamorous about leading a fast-growing tech company by committee. The business was in chaos; Uber lost about 10 points in North American market share in less than a year. The team agreed

Liane Hornsey received 215 complaints about sexual harassment, retaliation, bullying, or discrimination in her early days as head of Uber human resources.

Alex Walsh

that Uber was doing too much. It needed to address the basics. "We put 100 projects on pause right away," Graf remembers. One project they prioritized, however, was building a new app for drivers, codenamed Carbon.

0

OF ALL THOSE UBER HAS MANAGED TO ANGER—regulators, cabbies, riders—it has done worst by its own drivers. Treated as contractors, not employees, drivers have complained that they can't make enough money under Uber's pricing system. They have protested the service's constantly changing rules. They've been frustrated when no one at Uber has helped to resolve problems quickly. At best, Kalanick seemed to ignore them, and at worst he intimated they'd be eventually replaced by autonomous vehicles.

By the start of 2017, the company recognized it had a problem. Only a quarter of the people who'd signed up to drive for Uber were still doing so a year later, according to news reports. Uber hadn't made it easy for them. It hadn't overhauled its driver app since 2015, and in that time it had added new services like Eats, in which drivers deliver food. To find their way, drivers had to switch back and forth between Uber and mapping apps like Waze, creating friction and frustration. Anything that goes wrong—a rider is standing on the other side of a busy intersection, say, or a carpool rider asks for a different drop-off spot—costs time, which is money.

The goal of Carbon—the new driver app—was to foster a perfectly efficient ride that would reduce the chance a driver would also drive for Lyft. But there was no way to roll out a driver app quickly, or even sort of fast. As Graf had found, the technology underlying the app needed a total rebuild.

There was also much more to address beyond building a sturdy tech foundation. To achieve maximum efficiency, Uber needed to create a map of a constantly changing world exactly as it exists in any given moment. A garbage truck is blocking a lane. There's road work. A fender bender stops traffic for half an hour. All of these things can slow a driver down. And Uber provides rides in real time. Order a package on Amazon and you hope it'll arrive tomorrow. Order a ride on Uber and you hope it's already here.

With newer food delivery and also carpooling services, the challenges grow exponentially. Say a driver is delivering a burger. How do they locate an apartment on the seventh floor of one of several buildings in an apartment complex? Where do they leave the car while making the drop-off? The challenge of simply locating customers in three-dimensional space is huge.

Consider the blue dot that signals where you are when you open the app as a rider. If you've been using Uber for a while, you've probably noticed that the placement of that blue dot is more accurate than it used to be. But it still often locates you pretty far from where you are in real life, particularly when you're in a dense city. Uber— or, more specifically, Danny Iland and Andrew Irish, whose startup, ShadowMaps, was bought by Uber in 2016—are working on that gnarly problem.

Mapping services typically use the government-owned Global Positioning System, but GPS, Iland explains, was designed for things that fly or sail. Buildings can block your phone from receiving satellite signals, which can cause your phone to misidentify your location. Uber, along with many other mapping companies, has tried to solve this problem through map-matching, which combines GPS data with mapping software from a number of sources to guess your location. But it's far from perfect.

Iland and Irish, who were PhD students at UC Santa Barbara when they started ShadowMaps, use a different process. They superimpose the signals your phone is picking up against a 3-D map—a technique called occlusion modeling—so they can see which signals are coming from satellites that have you in their direct line of sight. They combine the data points from those satellites to make a more accurate guess about your location. The process can even correctly identify whether you're on the south or north side of the street.

This is just one of the technologies Uber is developing to improve maps and navigation. Another uses digital imagery to improve the accuracy of a driver's estimated time of arrival. A different team is trying to improve the navigation system for drivers.

Carbon needed to combine these efforts elegantly, a process that would take at least 18 months. But in 2017, as competitors tried to lure Uber's disgruntled drivers to their services, the company began introducing a series of small changes that drivers wanted. Riders could now tip, and drivers could organize their lives a bit better by setting in advance a general location for a few pickups each day, a feature known as Star Power. Uber also provided a phone line so drivers could speak to a customer service rep rather than sending urgent emails into the ether.

These changes bought Uber some time to build and test Carbon, but also introduced glitches. Over the summer, the new features had altered the delicate balance of demand and supply, so that riders were waiting slightly longer for pickups in some markets. At first it was hard to tell which features were responsible. Then, in August, the company put out a Star Power update that let drivers choose six daily destinations. If a driver wanted to, say, end up near their child's school around 3 pm, they could request a trip in that direction. It was such a good idea that too many drivers used it. Gradually it became obvious that allowing drivers to choose so many daily destinations was the problem.

KHOSROWSHAHI'S DELIBERATE PACE MAKES SOME PEOPLE UNCOMFORTABLE.

The Star Power update came in the same month that Khosrowshahi was named Uber's CEO. He leaned on the product team to solve the wait-time problem.

0

ONE DAY IN JANUARY, THREE MONTHS BEFORE Carbon was due to roll out, Yuhki Yamashita, a senior product manager, kicked off a presentation about the driving app. Half a dozen

engineers and product managers sat around a conference table made from a live-edged black walnut slab. A team member beamed in via videoconference from the Los Angeles office. Graf, Yamashita's boss, was at the table too. After testing Carbon for months, they'd finally arrived at a working beta version and had tested it with drivers, and they were ready to show Khosrowshahi.

As Yamashita described drivers' reactions to the app's improved features, Khosrowshahi leaned forward, elbow on table, chin in palm, a furrow deepening between his eyebrows. He seemed worried. Remember that in Uber lingo the "marketplace" is the platform where data is collected and processed to determine everything about how Uber works—from pricing to the routes drivers are encouraged to travel. Khosrowshahi jumped in during Yamashita's presentation to ask whether any of the new features could "eff with the marketplace." (Khosrowshahi is a man who doesn't often swear.)

Yamashita responded that, sure, any number of features could alter marketplace dynamics. He described a new pop-up bubble that was intended to predict the number of minutes a driver would have to wait until the next ride request. If the wait is too long, a driver might head to a different neighborhood or pull up a competitor's app. With 3 million drivers completing 15 million rides every day, any small change could ripple through a system in unexpected ways.

Khosrowshahi reminded everyone that a new technology platform is usually a disaster at first. Why compound those difficulties by introducing so many new features? "I know we think they're really cool, but I would first roll this out with some features off—the features that might affect the marketplace," he said. "If something happens, we're not going to know why."

Yamashita exchanged a quick glance with Graf, who sat at the corner of the table, his laptop flipped open. Most of the team remained poker-faced. Moving products into the world slowly was not how Uber had become a worldwide phenomenon in just nine years.

Yamashita had already noted that the team had been testing the app for 12 weeks. They'd launched beta versions with more than 500 drivers in six cities. They'd gone on ride-alongs and set up WhatsApp chats between engineers and drivers. This was way more testing than he'd ever done in his three years at Uber. "Usually we just do an A/B test, think it's fine, and then start rolling it out," he said.

Khosrowshahi was unmoved. Still fresh in his mind was the amount of time it took to isolate which feature had caused riders to wait longer over the summer. "Dude, with Star Power we found out four months later," Khosrowshahi said. That would have been less likely had the company rolled out features more systematically.

Khosrowshahi would rather go at a pace slow enough to hit perfection than tolerate pretty good. In other words, something like Zero Defects. But these values are so antithetical to the way Uber's engineers have worked that even if the people gathered around the table wanted to work differently, they might not know how to go about it.

As the meeting wrapped up, Yamashita and Graf acquiesced. Graf suggested the rollout could move a bit more deliberately. "Let's see if we can stage it a little more," he said, marking the compromise on which, temporarily, they agreed to settle.

B

BORN INTO A WEALTHY FAMILY IN IRAN, Khosrowshahi fled the country with his parents and two brothers in 1978 during the Iranian revolution. His family settled in Westchester County, New York. After graduating from Brown University, he worked as an analyst at the private bank Allen & Company and then landed at Barry Diller's internet holding company, InterActiveCorp. That's where he made his name. In 2002, just after the September 11 terrorist attacks, IAC bought a controlling stake in Expedia. Travel in the US had ground to a halt, but Diller thought it would come back, and it did. Expedia spun off from IAC in 2005, with Khosrowshahi at the helm.

When we talked in January, Khosrowshahi admitted that he was only just diving into Uber's product strategy. He'd been too busy initially dealing with the company's many emergencies: the Waymo trial; London's ban on Uber drivers. And he'd had to resolve the fallout from a hack of data from 57 million customer and driver accounts that Uber had failed to disclose for more than a year.

In January, Uber shareholders agreed to sell $8 billion worth of stock to a group of investors led by Softbank. The deal also eliminated the super-voting stock rights that gave some board members, including Kalanick, heightened decisionmaking control. And a few weeks later, the company settled its lawsuit with Waymo, paying between $163 million and $245 million in company shares, depending on how you count Uber's worth, to Waymo.

With those issues wrapped up, Khosrowshahi was ready to focus on his idea of quality. In February his deputies appeared at an all-hands meeting to sell the company's 18,000 employees on the importance of one metric: the ratio of driver or rider complaints to rides booked. That ratio needs to be reduced—a lot—in 2018, he told them. (He won't specify the company's 2018 target, but he said, completely deadpan, "Zero is zero." Note: Even the Pershing didn't have zero defects.) He believes the ratio is a good metric to use because it can be improved only if operations, technology, and customer service work together. "It's a unifier," he said. At Expedia, he worked on reducing a similar complaint metric, and the experience cemented his belief: As the measure improved, so did sales.

No one I talked to described Khosrowshahi as charismatic. I watched him at an all-hands meeting in January where he took the stage for less than five minutes to introduce speakers, then stood along the wall with colleagues, arms crossed, apparently listening. His message—"driving quality is just as important as driving new features," as he told me—offers a steady reassurance, but his deliberate pace has made some people uncomfortable. Among the product teams, in particular, there's still some question about his acuity. Though he has a degree in electrical engineering, he's a business guy. One former executive told me that there were many people "carefully watching whether Dara can step into and excel in the role of product leader and visionary."

One current employee, who largely approves of the new leadership, said he also misses the adrenaline rush that came with working under Kalanick. At Khosrowshahi's Uber, people go home for dinner.

Then there are employees and alumni who believe the worst aspects of the culture Kalanick created can't be so easily uprooted. "In everything from the way performance reviews were geared to the way bonuses were distributed, people were incentivized to backstab and undercut each other constantly," says one longtime employee who left recently. "They were incentivized to be assholes." That's not something that changes in six months, even with new performance review metrics, new leadership, and an emphasis on getting things right the first time. Already, some people have moved on. Aaron Schildkrout, who started Carbon's development, resigned in December. He's now in New Zealand, meditating. In February, Graf announced he was leaving too.

JESSI HEMPEL *(@jessiwrites) is a senior writer for* WIRED.

Yuhki Yamashita worked on one of Uber's big priorities—a new app that would keep drivers from jumping to the competition.

Alex Walsh

Replacing Graf turned into a bit of a blunder. The company rescinded an offer it made to a former Amazon executive to fill Graf's product chief role after discovering the guy wasn't working for Amazon when Uber hired him. He'd left in 2017. This is the type of information you'd expect a company to know before extending an offer for a crucial executive position. Nor has Kalanick completely disappeared. He no longer has super-voting rights, but he does still sit on the board. The relationship between the two men, Khosrowshahi told CNBC in January, is "fine, but strained." (Kalanick declined to be interviewed.)

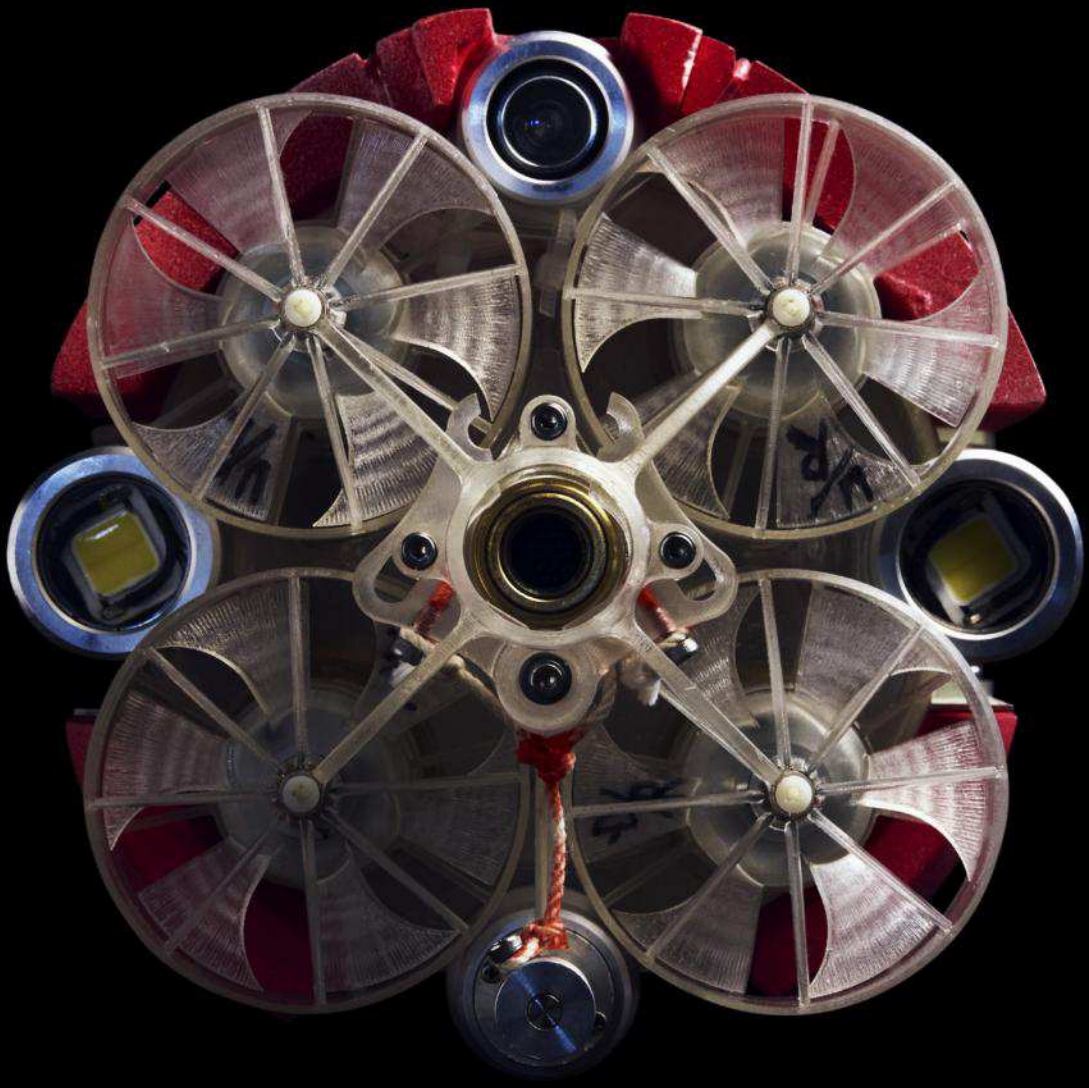
For most of last year, Uber's efforts to develop self-driving cars were under scrutiny while the company faced allegations it had stolen Waymo's technology. I spoke to the head of the unit, Eric Meyerhoff, early one February morning as he was preparing for the trial in the case. He said that the distraction of the suit had slowed his team down. "It's like pulling an anchor along," he said.

Settling that case should have provided some relief. But then came the fatal accident in March. After the Tempe police released a dashcam video of the woman being hit by an Uber Volvo, several academics suggested the self-driving technology should have prevented the accident. The human operator in the car, whose role is to step in when the tech fails, didn't stop the crash either. The incident suggested deeper problems. *The New York Times* reported that Uber's self-driving cars were having trouble with basic maneuvers, like operating next to big rigs, and its safety drivers had to intervene far more often than those of competing autonomous car projects. Then Reuters reported that Uber's Volvos lacked enough sensors and so had a blind zone. (An Uber spokesperson said, "Safety is our primary concern" in developing self-driving technology.) In late March, Arizona governor Doug Ducey demanded that Uber suspend its road tests in the state indefinitely for its "unquestionable failure to comply" with the duty to prioritize public safety. The accident and Uber's conduct was becoming a political issue as well as a corporate one. The company had intended to offer driverless cars within 18 months, but with testing suspended, that's unlikely.

When I talked to Khosrowshahi in January, he had not yet visited the Phoenix self-driving operation or the autonomous group in Pittsburgh (he would make his first trip there in March). As with other, less-urgent issues, he hadn't gotten there. But he had been thinking about the particular challenge of testing a software product that powers a large object made of heavy metal traveling at high speeds in spaces populated with humans. "In software, the edge cases are a bug, and you follow a bug and you fix it," he told me. "In autonomous, the edge cases are accidents that risk human lives." The Tempe accident was just the sort of edge case he had hoped to avoid. The kind of problem that no one can fix after the fact. W

THE ROBOT ASSAULT ON FUKUSHIMA

THE 2011 EARTHQUAKE AND TSUNAMI IN JAPAN TRIGGERED A DEVASTATING CATASTROPHE IN ONE OF THE COUNTRY'S LARGEST NUCLEAR POWER PLANTS. THE CLEANUP WILL TAKE DECADES, AND OFFICIALS WILL NEED TO LOCATE ALL THE LETHAL FUEL REMAINING IN THE PITCH-BLACK, DEBRIS-STREWN, WATER-FILLED VESSELS. IT'S NO JOB FOR HUMANS.



BY VINCE BEISER

SPENCER LOWELL

THE NIGHT BEFORE THE MISSION, KENJI MATSUZAKI COULD NOT SLEEP.

For more than a year, Matsuzaki and a team of engineers had been developing their little robot—a bread-loaf-sized, red and white machine equipped with five propellers, a transparent dome, front and rear video cameras, and an array of lights and sensors. Nicknamed Little Sunfish, it was engineered to operate underwater, in total darkness, amid intense radiation. And after three months of testing, training, and fine-tuning, it was deemed ready to fulfill its mission: to find and photograph the melted-down radioactive fuel that had gone missing inside the Fukushima Daiichi nuclear power plant.

More than six years had passed since an earthquake and tsunami hammered northeastern Japan and reduced the Fukushima facility to radioactive ruin. In all that time, no one had been able to locate the hundreds of tons of fuel inside the three reactors that had suffered core meltdowns. The uranium fuel had overheated, turned into lava, and burned through its steel container. That much was known. What happened after that was the big question. Did all the fuel flow out of the reactors, or was some still inside? Did it pile up in a heap, spread out in a puddle, spatter on the walls? Without knowing the answers to those questions, it was nearly impossible to devise a plan to get rid of it. And getting rid of it is imperative. Every day, as much as 165 tons of groundwater seeps into the reactors, becoming contaminated with radiation. And there's always the possibility that another earthquake or some other disaster could rupture the reactors again, sending radiation spilling out into the air, sea, or both.

Human beings couldn't go into the heart of Fukushima's reactors to find the missing fuel, though—at least not without absorbing a lethal dose of radiation. The job would have to be done by robots. But no robot had ever carried out such a mission before. Many had already tried and failed. Debris tripped them up. Yard-thick concrete walls threatened to block their wireless signals. Radiation fouled up their microprocessors and camera components. And so it fell to Matsuzaki, a shy-eyed , 41-year-old senior scientist with Toshiba's nuclear technology branch, to help build a machine that wouldn't end up as another one of the robot corpses already littering the reactors.

Just getting the Sunfish and its support gear into position inside the enormous concrete building that housed one of the crippled reactors took two days. Four separate teams took turns setting up the control panel, cable drum, and other equipment the robot would need to function. Even in full protective bodysuits, each group of workers could spend only a few minutes inside the structure, working by the light of portable electric lamps amid a thicket of machinery, pipes, and catwalks. When one team absorbed its maximum permitted daily dose of radiation, it was replaced by another group. Matsuzaki himself made two forays inside to put the final touches on the Sunfish, sweating inside his face mask and bodysuit in the summer heat, his nerves jumping each time his portable monitor dinged to indicate he'd received another increment of his allowable radiation dose.

The plan was for the Sunfish to spend three days mapping the debris and searching for signs of the missing fuel. Matsuzaki would monitor its progress from a control room about 500 yards away. He would be joined by a half-dozen top officials from his employer, Toshiba, and Tokyo Electric Power Company (Tepco), the mammoth utility that owns the plant. His success—or failure—would be broadcast daily around the world.

Beyond the immediate danger, cleaning up Fukushima remains critical to repairing the image of Japan's energy industry. In the wake of the disaster, Japan shut down every one of

its dozens of nuclear plants, which had provided some 27 percent of the nation's power. To cover the loss, it had to massively increase imports of expensive fossil fuels. A few nuclear plants have since been permitted to restart, following years of safety upgrades, but Fukushima cost the industry much of its public support. Polls consistently show that a majority of the public opposes nuclear power. Two of Japan's former prime ministers, including the one in office at the time of the disaster, have flipped from supporting nuclear plants to calling for their elimination.

The disaster also dealt a severe blow to the global nuclear industry, which had been gaining favor even among some environmentalists as a carbon-free alternative to fossil fuels. In the aftermath of the meltdown, Germany announced it would phase out nuclear power altogether, Vietnam dropped plans to build reactors, and the whole industry was thrown on the defensive. Every proposed new reactor now has to answer the question: How do we know this won't be another Fukushima?

Small wonder that in the nights leading up to the mission, Matsuzaki was feeling the pressure. "I've been having nightmares about failing," he confessed to his boss, Akira Tsuyuki. "Me too," Tsuyuki said. Late at night on July 18, 2017, the mission start time just a few hours away, Matsuzaki lay awake, wondering whether his team's technology would be any match for Fukushima.

THE EARTHQUAKE ON MARCH 11, 2011, WAS the biggest ever recorded in Japanese history, a 9.0 monster that devastated northeastern Japan and triggered a series of tsunamis that slammed into the coast, killing nearly 16,000 people. The tsunamis also knocked out power to the Fukushima Daiichi plant, shutting down the pumps needed to keep cooling water circulating in the reactor cores. Over the next several days, as Tepco engineers worked by flashlight to regain control, the fuel in three of the plant's six reactors—Units 1, 2, and 3—melted down. Gases unleashed by the damage exploded, sending plumes of radioactive particles like iodine, cesium, and plutonium into the atmosphere. The government ordered everyone within a 12-mile radius to evacuate, with about 165,000 people eventually displaced.

Government officials originally estimated it would take about 40 years and $50 billion to clean up the plant, decontaminate the surrounding area, and compensate the disaster's victims. In December 2016, they more than tripled that estimate to $188 billion. "We have never experienced a disaster as big as Fukushima," Hiroshige Seko, the head of Japan's Ministry of Economy, Trade, and Industry, told reporters at the time, according to Bloomberg. "With our limited knowledge, it was very difficult to make the previous forecast."

The Fukushima cleanup is a project far bigger and more complex than those of even the world's worst previous nuclear catastrophes. Chernobyl was literally covered up: The Soviets simply encased the whole thing in concrete and steel. Three Mile Island was tiny by comparison. Only a single reactor melted down, and none of its fuel escaped. "Fukushima is orders of magnitude more difficult," says Lake Barrett, an American who oversaw the cleanup of Three Mile Island and who signed on as a consultant to Tepco and the Japanese government in 2013.

In the first chaotic weeks after the meltdown, with radiation levels far too intense for anyone to work inside the reactors, Tepco scrambled to deploy robots to assess and contain the damage. Tractor-treaded bots from iRobot, drones from Honeywell, and a prototype disaster-response mech from Tohoku University scouted the rubble-strewn facility and tried to measure the intensity of the radiation. A remote-controlled concrete pumping truck was adapted so that its extendable spout could pour water into the reactors, cooling and stabilizing the overheated chambers.

In the months and years that followed, Fukushima became both a market and a proving ground for ever-advancing robot technologies designed to operate in hazardous conditions. Remote-controlled front-end loaders, backhoes, and other heavy equipment were put to work breaking up radioactive debris and loading it onto remote-controlled dump trucks. A four-legged walking robot investigated the reactor buildings. Robots with 3-D scanners were sent in to gather imagery and map radiation levels. Swimming robots inspected pools where spent fuel rods were stored, taking pictures.

But none of these robots were capable of penetrating the innermost areas of the reactors. In August 2013, the Japanese government assembled a consortium of public utilities and private companies, including Mitsubishi, Hitachi, and Toshiba, to create robots specifically for the most challenging environments. Dubbed the International Research Institute for Nuclear Decommissioning, it has developed some 20 machines that have been deployed onsite. Their ranks include a snakelike bot that crawled through a tiny accessway into Unit 1, then bent itself into a more stable U-shape to explore inside. Then there was the Scorpion, a tank-tread-driven machine with a camera mounted on an elevating "tail" that was sent into Unit 2. The Japanese government is bankrolling a $100 million, state-of-the-art R&D center near the nuclear plant where robot operators train on digital models of the reactors in a giant 3-D Holo Stage and on life-size physical mock-ups.

But even with the massive government investment, many of the new robots still couldn't hack it inside the reactors. The camera on one of them, sent to clear a path for the Scorpion, was shut down by radiation; the Scorpion itself got tripped up by fallen debris. The first version of the snakelike bot got stuck; the second did better but failed to find any melted fuel. "It's very difficult to design a robot to operate in an unknown environment,"

PREVIOUS SPREAD:
INSIDE TOSHIBA'S RESEARCH FACILITY, ENGINEERS LOOK INTO A POOL [LEFT] WHERE ROBOTS LIKE THE SUNFISH [RIGHT] ARE TESTED BEFORE BEING DEPLOYED IN A NUCLEAR REACTOR.

OPPOSITE PAGE:
THE EXTERIOR OF UNIT 2, ONE OF FUKUSHIMA DAIICHI'S SIX REACTORS.

says Hajime Asama, a professor at the University of Tokyo who was one of the first roboticists the government turned to for help. "Until we send the bot in, we don't know what the conditions are. And after it's sent, we can't change it."

Kenji Matsuzaki has worked in Toshiba's nuclear technology branch for more than 10 years, and by May 2016, when he was assigned to the team developing a robot to explore inside Unit 3 of Fukushima, he was familiar with the plant's basic architecture. All six of its reactors are boiling-water reactors, a type designed in the late 1960s and early 1970s and found all over the world, including in the United States. They generate electricity by circulating water through their infernally hot cores, converting it to steam that is used to turn turbine generators. Each reactor has three containers set one inside another like Russian nesting dolls. The smallest container, a steel capsule about the length of a tennis court, is called the reactor pressure vessel. That's where the nuclear fission reaction takes place, powered by fuel composed of uranium dioxide baked into ceramic pellets. This capsule is enclosed inside a primary containment vessel, a concrete and steel structure shaped like a massive light bulb, designed to capture any radiation that might

THE SUNFISH HAD TO BE ABLE TO SWIM [RIGHT], FIT INTO THE SMALL OPENING OF THE CONTAINMENT VESSEL [TOP LEFT], AND WITHSTAND CHALLENGES THAT CRIPPLED AN EARLIER ROBOT, THE SCORPION [BOTTOM LEFT].

accidentally escape. The containment vessel in turn is housed inside the reactor building, a concrete and metal rectangle that offers only minimal protection from radiation.

Technicians in protective gear can work for short periods inside the reactor building, but they can't enter the far more radioactive containment vessel, which is where they were likely to find at least some of the missing fuel. Building a robot

that could get inside and maneuver around the containment vessel presented several unique challenges. First, the containment vessel was only practically accessible through a 5.5-inch circular maintenance opening about 8 feet above the floor of the reactor building, so the robot would have to be small. Second, because the containment vessel had been pumped full of water to cool it down, the robot would have to be able to swim. Third, since the water and thick walls would defeat wireless signals, this small, swimming robot would need to be powerful enough to move underwater while dragging as much as 65 yards of electric cable behind it.

It took months of research, experimentation, and testing in Toshiba's labs and in an enormous simulation tank at the government-run Port and Airport Research Institute to balance all these capabilities inside the little machine. Matsuzaki's team had to try different configurations of propellers, cameras, and sensors, boost the power of the propeller motors, develop a new type of coating to make the cable move more smoothly, and ensure the whole package could withstand a blistering level of radiation.

At midnight on July 19, the day the Sunfish was scheduled to make its first foray into the reactor, Matsuzaki's alarm went off in his hotel room. He and his team were staying in Iwaki, the closest habitable city with a hotel, about an hour south of the plant. Starting their day in the dark of night was the only way to have enough time to drive to the plant, suit up in protective gear, and hold a last round of meetings before their start time. That would give them about eight hours; by noon it would be too hot inside the reactor building for the technicians monitoring the robot to do their jobs.

At about 4:30 am, a group of Toshiba techs in full protective gear darted into the reactor building. They fast-walked to the outer wall of the containment vessel and climbed a step ladder up to the opening where the Sunfish and its equipment had been pre-positioned. They unsealed the valve over the opening, then pushed in a heavy guiding pipe, with the Sunfish at its tip, all the way through to the other side. Slowly and carefully, they angled the pipe until the bot slid into the water below.

Inside, it was completely dark. On their monitors in the control room, Matsuzaki's team, connected to the Sunfish's controls via the electric cable, could see only a narrow swath cut through the turbid water by the Sunfish's lights. Seated at a long table, one technician "drove" the Sunfish with a videogame-type controller. Another reeled its cable in and out, keeping it taut so it wouldn't get tangled as the bot swam this way and that. A third did his best to estimate the machine's position using a 3-D software model of the containment vessel. Matsuzaki oversaw them all, trying to forget about the platoon of corporate officials watching over his shoulder.

The first day, the Sunfish spent most of its time reconnoitering. The damage inside the containment vessel was worse than expected. Unidentifiable clumps of pebble-sized debris and pieces of half-destroyed equipment littered the floor. But there was no sign of the fuel, and after eight hours of searching, the team pulled the Sunfish back to the surface. They gave it a rest the next day while they discussed their findings and strategized their next steps.

The following morning, they sent the Sunfish back into the water. The team drove it slowly and carefully, but time after time, the bot's powerful propellers would stir up a blinding cloud of sediment, forcing them to wait until the water cleared again. After several hours of maneuvering, and with the noon deadline looming, Matsuzaki was growing nervous. Then, something startling appeared on the monitors.

"What is that?" said Matsuzaki.

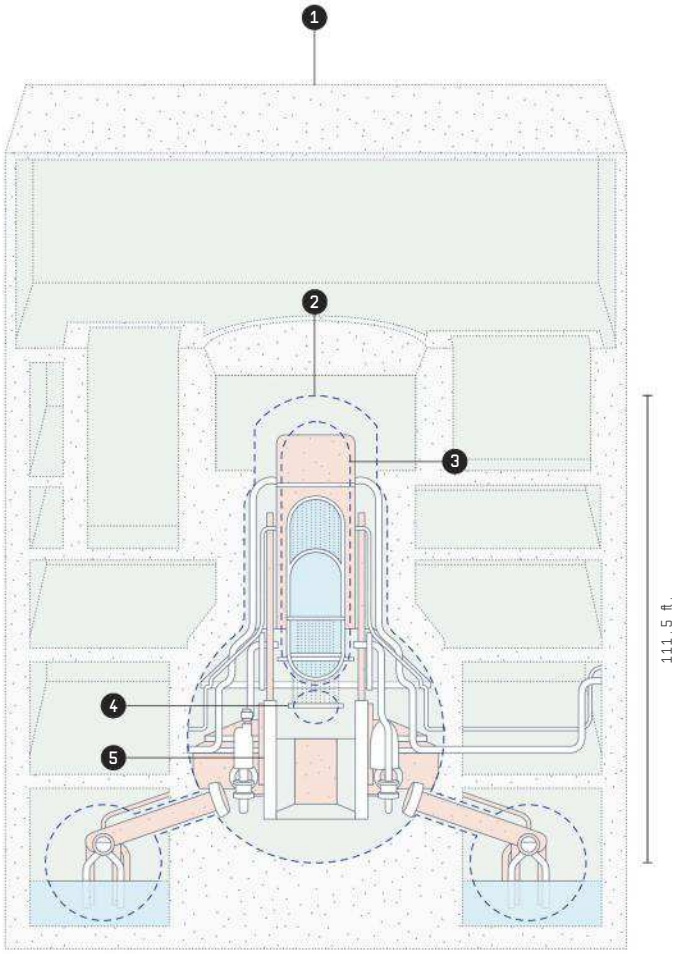
Everyone began talking at once and pointing to what they saw on the screens: murky glimpses of what appeared to be stalactites of something dripping like candle wax from the bottom of the reactor pressure vessel. They'd found the first signs of the missing fuel.

They maneuvered the Sunfish around the area, documenting as much as possible, before pulling the bot out. When Matsuzaki declared the mission complete, the control room burst into applause.

BY NOW, MUCH OF FUKUSHIMA DAIICHI itself, an expansive complex covering some 860 acres, is a lot safer than you'd expect. Most areas have been decontaminated to the point where full bodysuits are no longer required. The 5,000-plus workers tasked with cleaning the place up have cut down hundreds of the cherry trees that used to enliven the grounds, torn up and paved over once-grassy open areas,

INSIDE UNIT 3

Each reactor is made up of three containers, one set inside another, that hold critical equipment.



1. REACTOR BUILDING A LARGE CONCRETE AND STEEL STRUCTURE THAT ACTS AS THE LAST LINE OF DEFENSE TO KEEP RADIATION FROM ESCAPING INTO THE OUTSIDE WORLD.

2. PRIMARY CONTAINMENT VESSEL AN AIRTIGHT ENCLOSURE MADE OF STEEL AND CONCRETE.

3. REACTOR PRESSURE VESSEL A THICK STEEL CONTAINER THAT HOLDS THE URANIUM FUEL, WHICH POWERS THE NUCLEAR REACTOR.

4. CONTROL-ROD DRIVE A MECHANICAL SYSTEM THAT USES THIN RODS TO SPEED UP OR SLOW DOWN A NUCLEAR FISSION REACTION. THE RODS WORK BY ABSORBING THE STRAY NEUTRONS THAT TRIGGER A CHAIN REACTION.

5. PEDESTAL A CIRCULAR CONCRETE STRUCTURE THAT HOLDS UP THE REACTOR. FROM INSIDE, WORKERS CAN ACCESS THE CONTROL-ROD DRIVE.

DIAGRAM BY FEDERICA FRAGAPANE

and scrubbed down buildings. They have covered the seafloor just off the coast with clay to seal in cesium that seeped into the mud after the disaster. Using an enormous, purpose-built fuel-handling machine, they have removed the hundreds of spent uranium fuel rods from Unit 4, a reactor that was damaged by an explosion but did not melt down.

Still, when I visited the site last December with Lake Barrett, Tepco's American consultant, we had to put on gloves, safety glasses, surgical masks, three pairs of socks, and plastic booties over our shoes, as well as a personal radiation detector, before being allowed inside the facility.

At 72, Barrett is tall, fit, and astonishingly energetic. I first met him at the Narita airport outside Tokyo, where he bounced right off a 20-hour trip from his home in Florida, joined me in a car without stopping for so much as a cup of coffee, and talked cheerily for the entire two-hour drive to Fukushima prefecture.

When Barrett heard the first news reports about the disaster, he "didn't think much of it," he says. "There's always so much hype around these things." Then he saw the picture of Unit 1 exploding. "I said, 'Holy shit. I know exactly what that was.' I knew they were in deep doo-

THE HOT ZONE

Following the meltdown, nearly 165,000 people had to evacuate the area surrounding the Fukushima plant to avoid radioactive exposure. Today, even after extensive cleanup efforts, 50,000 people still can't go home.

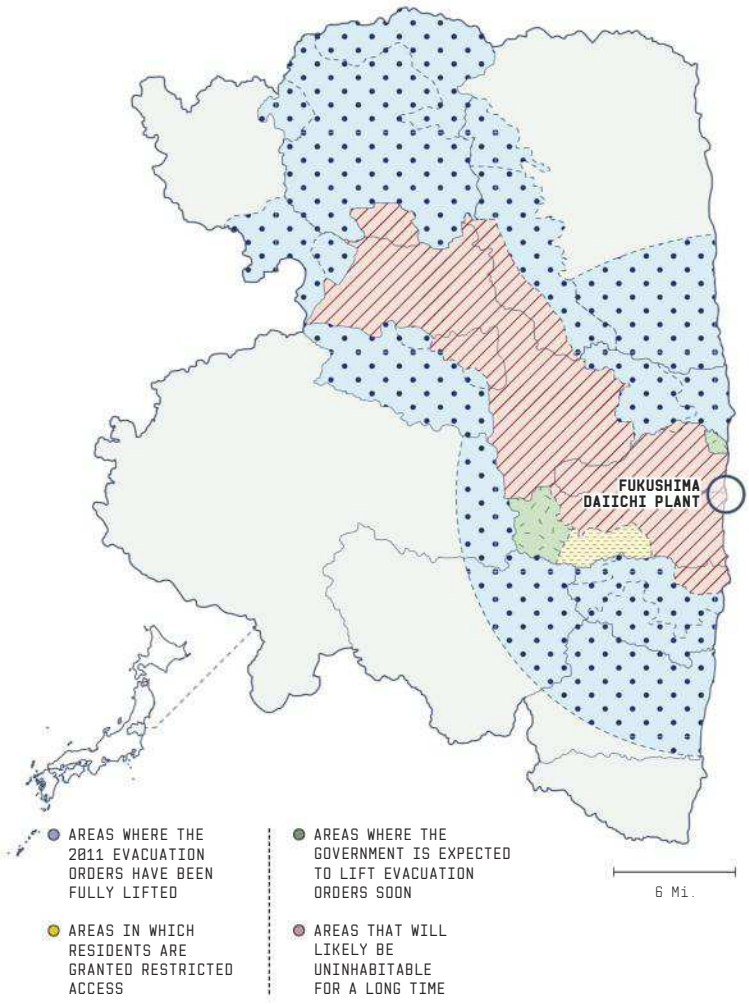


DIAGRAM BY FEDERICA FRAGAPANE

doo." When the call came to help out, he didn't hesitate. "It's personal for me," he says. "Japan was the only country that helped us at Three Mile Island. We owe Japan."

From atop a small hill, once covered with grass and now encased in concrete, Barrett and I survey the trio of hulking buildings outlined against the blues of the winter sky and the Pacific Ocean behind them. Remotely operated orange-and-white cranes lean over them like reverent metal giraffes. These are the reactor buildings: the intractable core of the disaster zone, the radioactive redoubts the robots must penetrate.

Each poses a unique challenge. The amount and type of damage inflicted on each is different, as is the depth of the water flooding their bases. Of course, at the heart of each is a mess of melted fuel, presumed to have flowed in different ways to different places.

Less than half a mile from these three reactors sits Unit 5, one of the three other reactors that had been shut down for regular maintenance when the tsunami hit. Since it escaped largely unscathed and is nearly identical to the damaged reactors, Tepco engineers use it to plan robot missions. Inside is a baffling maze of machines, ducts, cables, and catwalks. "You can see how hard it is to run the robots around in here," Barrett says.

We navigate our way through the building to the containment vessel. "That's just like where the Sunfish went in," he says, pointing up to an unassuming circular opening in the wall of the vessel.

We enter the containment vessel and make our way through a narrow doorway into a chamber below the reactor pressure vessel. Control rod assemblies stud the reactor vessel's underside; we have to crouch to avoid bumping our heads on them. Pointing out key areas and components, Barrett walks me through the current theories on what happened to the fuel in each of the meltdown units. "No one knows if the lava made a nice neat vertical pile or whether

A ROBOT UNDERGOES TESTING AT THE GOVERNMENT'S NEW $100 MILLION R&D CENTER NEAR THE NUCLEAR PLANT [FAR LEFT]. INSIDE THE FUKUSHIMA PLANT, EACH OF THESE BLUE TOWERS [MIDDLE] HOLDS 100 PERSONAL RADIATION DETECTORS. KENJI MATSUZAKI [BELOW], THE LEAD SCIENTIST BEHIND LITTLE SUNFISH.

it flowed sideways," he says. "Hot molten fuel could have fallen into the water and caused a steam explosion that would have blown it everywhere."

In Unit 3, at least, thanks to the Sunfish, Tepco is relatively certain about a few things. The pictures it took show that the control-rod mechanisms at the bottom of the reactor vessel disintegrated. Molten fuel mixed with melted metal dripped down through the openings they left behind, presumably creating the stalactites seen in the videos. The lava-like mixture burned through both the steel grate beneath the reactor pressure vessel and a refrigerator-sized machine used to insert the control rods, and some of it dripped down to the floor of the containment vessel. There also appear to be chunks of fuel on the vessel's walls.

In January, a robotic probe using a remote-controlled camera mounted on a long pole spotted for the first time what appears to be melted fuel inside Unit 2. There may be another Sunfish mission, though it won't be the same robot that found the fuel in Unit 3. Despite emerging from the reactor undamaged, it had still absorbed a dangerous amount of radioactivity. Tepco engineers sealed it in a steel cask and interred it with other radioactive waste on the plant site.

A FEW MILES FROM THE FUKUSHIMA PLANT, IN THE TOWN OF OKUMA, VISITORS MUST WEAR FULL-BODY TYVEK SUITS, FACE MASKS, GLOVES, SOCKS, AND BOOTIES WHEN WALKING ALONG THE ABANDONED STREETS.

That still leaves an awful lot unknown. At the end of the day, "how much did we learn from the Sunfish mission?" Barrett asks. "It was a step, not a leap. We're getting closer and closer, but we have a long, long way to go." Tepco is continuing its efforts to scout the inside of the reactors.

Limited and uncertain as the Sunfish's findings are, they have helped move the ball forward. Engineers have now begun thinking about how to build the next generation of robots that will have to carry out the most complicated undertaking of all: removing the melted fuel.

Their first challenge will be enabling the bots to reach their target. "These are cramped spaces

VINCE BEISER *(@vincelb) is the author of* The World in a Grain*, to be published in August.*

filled with huge pieces of equipment that weigh many tons. You have to cut them up in pieces and pull them out," Barrett says. One idea currently in favor is to build a massive 20-foot robot arm that would enter the reactor building on rails, reach into the reactor pressure vessel, and scoop up the fuel. Another is to send in a bot the size of a small refrigerator on tractor treads, equipped with cutting and gripping tools to wrangle debris. A second robot would lift the detritus into containers, seal it, and put it on a conveyor belt to the outside.

Either system will take years to develop. Either or both might fail. Tepco has pegged 2021 as the target year to begin removing fuel debris. How long might the entire Fukushima cleanup take? "Good question. Nobody knows. No one in human history has experience with this," says Naoaki Okuzumi, a senior manager with the decommissioning institute. "The government says 30 to 40 years. I think that is optimistic."

While the robots' work inside Fukushima Daiichi drags on, human beings who once lived near the plant are waiting to go home. The national government has decontaminated several towns and urged residents to return. At the time of my visit in December, though, roughly 130 square miles of land was still off-limits, including the better part of a town called Okuma, perched in the hills a few miles from the plant.

Yoshihiro Takada, a former resident who now works with the local government agency in charge of rebuilding, agreed to show me around. Takada spent almost his entire life in Okuma and had to escape with his wife, child, and parents when the disaster hit. They've relocated to another town 65 miles away.

I met up with Takada in a parking lot just outside the exclusion zone, where we put on full-body Tyvek suits, face masks, gloves, socks, and booties over our shoes to protect us from the particles of cesium and strontium. Inhaling even a dust speck of one of those isotopes can be dangerous. That's part of what makes radiation so terrifying: You can't feel it, see it, or smell it. It can kill you without you ever knowing you encountered it.

There was no one in the train station, the barbershop, the restaurants, or the stores. The modest houses and apartment buildings on the residential streets were all empty. The only sound I heard as we walked down the middle of the deserted main street was the chirping of clueless birds who didn't realize they'd chosen to nest in a radioactive hot zone.

"I remember this place—their pizza was so good," Takada says, gesturing at a shuttered restaurant as we walk through town. Several shop windows have been smashed by wild boar that have come down from the hills to ransack the deserted town for food. Cars sit in driveways half-hidden by overgrown weeds. Takada only occasionally checks in on his own house. "Rats are running all over it inside. There are droppings and garbage all over," he says.

The area around Fukushima is mostly scenic farmland fringed with thickly wooded hills. But drive along practically any road and you pass fields filled with rows and rows of boulder-sized, black polypropylene bags. They are filled with contaminated earth; as part of the cleanup, a layer of topsoil is being scraped up from gardens, schoolyards, and fields all across the region. Roughly 20 million of the bags are scattered around the prefecture. Many of them will eventually be moved to the outskirts of Fukushima Daiichi itself for indefinite storage, along with an ever-growing array of tanks holding the radioactive water Tepco continues to pump out of the reactors.

Ultimately, there is no technology that can simply fix what happened at Fukushima. The only certainty is that it will be a slow, incremental, frustrating process that may not even be completed in Kenji Matsuzaki's lifetime. For now, all the scientists, engineers, and their allies can do is keep the radioactivity under control, track down its source, and try to capture it. But first, they need to create the robots to do it.

Ray Ozzie thinks he's come up with an approach for accessing encrypted devices that attains the impossible: It satisfies both law enforcement and privacy purists.

Step 1: Obtain warrant for locked, encrypted phone that is evidence in a criminal investigation. Step 2: Access special screen that generates a QR code containing an encrypted PIN. Step 3: Send picture of QR code to the phone's manufacturer, which confirms the warrant is legal. Step 4: Manufacturer transmits decrypted PIN to investigators, who use it to unlock the phone.

Cracking the Crypto War

BY STEVEN LEVY
COLE WILSON

On December 2, 2015, a man named Syed Rizwan Farook and his wife, Tashfeen Malik, opened fire on employees of the Department of Public Health in San Bernardino, California, killing 14 people and injuring 22 during what was supposed to be a staff meeting and holiday celebration. The shooters were tracked down and killed later in the day, and FBI agents wasted no time trying to understand the motivations of Farook and to get the fullest possible sense of his contacts and his network. But there was a problem: Farook's iPhone 5c was protected by Apple's default encryption system. Even when served with a warrant, Apple did not have the ability to extract the information from its own product. ¶ The government filed a court order, demanding, essentially, that Apple create a new version of the operating system that would enable it to unlock that single iPhone. Apple defe with CEO Tim Cook framing the threat to individual liberty.

STEVEN LEVY [@STEVENLEVY] WROTE ABOUT THE NEW APPLE HEADQUARTERS IN ISSUE 25.06.

"We have a responsibility to help you protect your data and protect your privacy," he said in a press conference. Then-FBI chief James Comey reportedly warned that Cook's attitude could cost lives. "I just don't want to get to a day where people look at us with tears in their eyes and say, 'My daughter is missing and you have her cell phone—what do you mean you can't tell me who she was texting before she disappeared?' " The controversy over Farook's iPhone reignited a debate that was known in the 1990s as the Crypto Wars, when the government feared the world was "going dark" and tried—and ultimately failed—to impede the adoption of technologies that could encode people's information. Only this time, with supercomputers in everybody's pockets and the endless war on terror, the stakes were higher than ever.

A few months after the San Bernardino shooting, President Obama sat for an interview at the South by Southwest conference and argued that government officials must be given some kind of shortcut—or what's known as exceptional access—to encrypted content during criminal and antiterrorism investigations. "My conclusion so far is that you cannot take an absolutist view on this," he said. "If the tech community says, 'Either we have strong, perfect encryption or else it's Big Brother and an Orwellian world'—what you'll find is that after something really bad happens, the politics of this will swing and it will become sloppy and rushed, and it will go through Congress in ways that have not been thought through. And then you really will have dangers to our civil liberties."

In typical Obama fashion, the president was leaning toward a compromise, a grand bargain between those who insist that the NSA and FBI need all the information they can get to monitor potential terrorists or zero in on child abusers and those who believe building any sort of exceptional access into our phones would be a fast track to a totalitarian surveillance state. And like so many of Obama's proposed compromises, this one went nowhere. To many cryptographers, there was simply no way that companies like Apple and Google could provide the government with legal access to customer data without compromising personal privacy and even national security. Exceptional access was a form of technology, after all, and any of its inevitable glitches, flaws, or bugs could be exploited to catastrophic ends. To suggest otherwise, they argued, was flat wrong. Flat-*Earth* wrong. Which was, as any good engineer or designer knows, an open invitation for someone to prove them wrong.

ended itself,
request as a

This past January, Ray Ozzie took a train

from his home in Massachusetts to New York City for a meeting in a conference room of the Data Science Institute at Columbia University. The 14th-floor aerie was ringed by wide windows and looked out on a clear but chilly day. About 15 people sat around the conference table, most of them middle-aged academics—people from the law school, scholars in government policy, and computer scientists, including cryptographers and security specialists—nibbling on a light lunch while waiting for Ozzie's presentation to begin.

Jeannette Wing—the host of the meeting and a former corporate VP of Microsoft Research who now heads the Data Science Institute—introduced Ozzie to the group. In the invitation to this "private, informal session," she'd referenced his background, albeit briefly. Ozzie was once chief technical officer at Microsoft as well as its chief software architect, posts he had assumed after leaving IBM, where he'd gone to work after the company had purchased a product he created, Lotus Notes. Packed in that sentence was the stuff of legend: Notes was a groundbreaking product that rocketed businesses into internet-style communications when the internet was barely a thing. The only other person who ever held the chief software architect post at Microsoft was Bill Gates, and Ozzie had also helped create the company's cloud business.

He had come to Columbia with a proposal to address the impasse over exceptional access, and the host invited the group to "critique it in a constructive way." Ozzie, trim and vigorous at 62, acknowledged off the bat that he was dealing with a polarizing issue. The cryptographic and civil liberties community argued that solving the problem was virtually impossible, which "kind of bothers me," he said. "In engineering if you think hard enough, you can come up with a solution." He believed he had one.

He started his presentation, outlining a scheme that would give law enforcement access to encrypted data without significantly increasing security risks for the billions of people who use encrypted devices. He'd named his idea Clear.

It works this way: The vendor—say it's Apple in this case, but it could be Google or any other tech company—starts by generating a pair of complementary keys. One, called the vendor's "public key," is stored in every iPhone and iPad. The other vendor key is its "private key." That one is stored with Apple, protected with the same maniacal care that Apple uses to protect the secret keys that certify its operating system updates. These safety measures typically involve a tamper-proof machine (known as an HSM or hardware security module) that lives in a vault in a specially protected building under biometric lock and smartcard key.

That public and private key pair can be used to encrypt and decrypt a secret PIN that each user's device automatically generates upon activation. Think of it as an extra password to unlock the device. This secret PIN is stored on the device, and it's protected by encrypting it with the vendor's public key. Once this is done, no one can decode it and use the PIN to unlock the phone except the vendor, using that highly protected private key.

So, say the FBI needs the contents of an iPhone. First the Feds have to actually get the device and the proper court authorization to access the information it contains—Ozzie's system does not allow the authorities to remotely snatch information. With the phone in its possession, they could then access, through the lock screen, the encrypted PIN and send it to Apple. Armed with that information, Apple would send highly trusted employees into the vault where they could use the private key to unlock the PIN. Apple could then send that no-longer-secret PIN back to the government, who can use it to unlock the device.

Ozzie designed other features meant to reassure skeptics. Clear works on only one device at a time: Obtaining one phone's PIN would not give the authorities the means to crack anyone else's phone. Also, when a phone is unlocked with Clear, a special chip inside the phone blows itself up, freezing the contents of the phone thereafter. This prevents any tampering with the contents of the phone. Clear can't be used for ongoing surveillance, Ozzie told the Columbia group, because once it is employed, the phone would no longer be able to be used.

He waited for the questions, and for the next two hours, there were plenty of them. The word *risk* came up. The most dramatic comment came from computer science professor and cryptographer Eran Tromer. With the flair of Hercule Poirot revealing the murderer, he announced that he'd discovered a weakness. He spun a wild scenario

involving a stolen phone, a second hacked phone, and a bank robbery. Ozzie conceded that Tromer found a flaw, but not one that couldn't be fixed.

At the end of the meeting, Ozzie felt he'd gotten some good feedback. He might not have changed anyone's position, but he also knew that unlocking minds can be harder than unlocking an encrypted iPhone. Still, he'd taken another baby step in what is now a two-years-and- counting quest. By focusing on the engineering problem, he'd started to change the debate about how best to balance privacy and law enforcement access. "I do not want us to hide behind a technological smoke screen," he said that day at Columbia. "Let's debate it. Don't hide the fact that it might be possible."

The first, and most famous, exceptional-access scheme was codenamed Nirvana. Its creator was an NSA assistant deputy director named Clinton Brooks, who realized in the late 1980s that newly discovered advances in cryptography could be a disaster for law enforcement and intelligence agencies. After initial despair, Brooks came up with an idea that he envisioned would protect people's privacy while preserving government's ability to get vital information. It involved generating a set of encryption keys, unique to each device, that would be held by government in heavily protected escrow. Only with legal warrants could the keys be retrieved and then used to decode encrypted data. Everyone would get what they wanted. Thus ... Nirvana.

The plan was spectacularly botched. Brooks' intent was to slowly cook up an impervious technical framework and carefully introduce it in the context of a broad and serious national discussion about encryption policy, where all stakeholders would hash out the relative trade-offs of law enforcement access to information and privacy. But in 1992, AT&T developed the Telephone Security Device 3600, which could scramble phone conversations. Its strong encryption and relatively low price unleashed a crypto panic in the NSA, the FBI, and even the tech-friendly officials in the new Clinton administration. Then the idea came up of using Brooks' key escrow technology, which by that time was being implemented with a specialized component called the Clipper Chip, to combat these enhanced encryption systems. After a few weeks, the president himself agreed to the plan, announcing it on April 16, 1993.

All hell broke loose as technologists and civil libertarians warned of an Orwellian future in which the government possessed a backdoor to all our information. Suddenly the obscure field of cryptography became a hot button. (I still have a T-shirt with the rallying cry "Don't Give Big Brother a Master Key.") And very good questions were raised: How could tech companies sell their wares overseas if foreign customers knew the US could get into their stuff? Wouldn't actual criminals use other alternatives to encrypt data? Would Clipper Chip technology, moving at government speed, hobble the fast-moving tech world?

Ultimately, Clipper's death came not from policy, but science. A young Bell Labs cryptographer named Matt Blaze discovered a fatal vulnerability, undoubtedly an artifact of the system's rushed implementation. Blaze's hack led the front page of *The New York Times*. The fiasco tainted all subsequent attempts at installing government backdoors, and by 1999, most government efforts to regulate cryptography had been abandoned, with barely a murmur from the FBI or the NSA.

For the next dozen or so years, there seemed to be a Pax Cryptographa. You seldom heard the government complain about not having enough access to people's personal information. But that was in large part because the government already had a frightening abundance of access, a fact made clear in 2013 by Edward Snowden. When the NSA contractor revealed the extent of his employer's surveillance capabilities, people were shocked at the breadth of its activities. Massive snooping programs were sweeping up our "metadata"—who we talk to, where we go—while court orders allowed investigators to scour what we stored in the cloud. The revelations were also a visceral blow to the leaders of the big tech companies, who discovered that their customers' data had essentially been plundered at the source. They vowed to protect that data more assiduously, this time regarding the US government as one of their attackers. Their solution: encryption that even the companies themselves could not decode. The best example was the iPhone, which encrypted users' data by default with iOS 8 in 2014.

RAY OZZIE, AT HIS HOME OFFICE OUTSIDE BOSTON, WORKS ON A VOLUNTEER PROJECT DESIGNING AND MAKING KITS FOR PEOPLE IN NUCLEAR RADIATION ZONES TO TEST THEIR SAFETY.

Law enforcement officials, most notably Comey of the FBI, grew alarmed that these heightened encryption schemes would create a safe haven for crooks and terrorists. He directed his staff to look at the potential dangers of increasing encryption and began giving speeches that called for that blast from the past, lingering like a nasty chord from '90s grunge: exceptional access.

The response from the cryptographic community was swift and simple: Can't. Be. Done. In a landmark 2015 paper called "Keys Under Doormats," a group of 15 cryptographers and computer security experts argued that, while law enforcement has reasons to argue for access to encrypted data, "a careful scientific analysis of the likely impact of such demands must distinguish what might be desirable from what is technically possible." Their analysis claimed that there was no foreseeable way to do this. If the government tried to implement exceptional access, they wrote, it would "open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend."

The 1990s Crypto Wars were back on, and Ray Ozzie didn't like what he was hearing. The debate was becoming increasingly politicized. Experts in cryptography, he says, "were starting to pat themselves on the back, taking extreme positions about truisms that weren't so obvious to me." He knew that great achievements of cryptography had come from brilliant scientists using encryption protocols to perform a kind of magic: sharing secrets between two people who had never met, or creating digital currency that can't be duplicated for the purposes of fraud. Could a secure system of exceptional access be so much harder?

So Ozzie set out to crack the problem. He had the time to do it. He'd recently sold a company he founded in 2012, Talko, to Microsoft. And he was, to quote a friend, "post-economic," having made enough money to free him from financial concerns. Working out of his home north of Boston, he began to fool around with some ideas. About two weeks later, he came up with Clear.

Ozzie's The strength of system

lies in its simplicity. Unlike Clinton Brooks, who relied on the government to safeguard the Clipper Chip's encrypted keys, Ozzie is putting his trust in corporations, a decision that came from his experience in working for big companies like Lotus, IBM, and Microsoft. He was intimately familiar with the way that tech giants managed their keys. (You could even argue that he helped invent that structure, since Lotus Notes was the first software product to get a license to export strong encryption overseas and thus was able to build it into its products.) He argues that the security of the entire mobile universe already relies on the protection of keys—those vital keys used to verify operating system updates, whose compromise could put billions of users at risk. (Every time you do an OS update, Apple certifies it by adding a unique ID and "signing" it to let your device know it's really Apple that is rewriting your iPhone's code.) Using that same system to provide exceptional access, he says, introduces no new security weaknesses that vendors don't already deal with.

Ozzie knew that his proposal danced on the third rail of the crypto debate—many before him who had hinted at a technical solution to exceptional access have been greeted with social media pitchforks. So he decided to roll out his proposal quietly, showing Clear to small audiences under an informal nondisclosure agreement. The purpose was to get feedback on his system, and, if he was lucky, to jar some people out of the mindset that regarded exceptional access as a crime against science. His first stop, in September 2016, was in Seattle, where he met with his former colleagues at Microsoft. Bill Gates greeted the idea enthusiastically. Another former colleague, Butler Lampson—a winner of the Turing Award, the Nobel Prize of computer science—calls the approach "completely reasonable ... The idea that there's no way to engineer a secure way of access is ridiculous." (Microsoft has no formal comment.)

Ozzie went on to show Clear to representatives from several of the biggest tech companies—Apple, Google, Facebook—none of whom had any interest whatsoever in voluntarily implementing any sort of exceptional access. Their focus was to serve their customers, and their customers want security. (Or, as Facebook put it in a statement to WIRED: "We have yet to hear of a technical solution to this challenge that would not risk weakening security for all users.") At one company, Ozzie squared off against a technical person who found the proposal offensive. "I've seen this happen to engineers a million times when they get backed into a corner," Ozzie says. "I told him 'I'm not saying you *should* do this. I'm trying to refute the argument that it can't be done.' "

Unsurprisingly, Ozzie got an enthusiastic reception from the law enforcement and intelligence communities. "It's not just whether his scheme is workable," says Rich Littlehale, a special agent in the Tennessee Bureau of Investigation. "It's the fact that someone with his experience and understanding is presenting it." In an informal meeting with NSA employees at its Maryland headquarters, Ozzie was startled to hear that the agency had come up with something almost identical at some point. They'd even given it a codename.

During the course of his meetings, Ozzie learned he was not alone in grappling with this issue. The names of three other scientists work-

ing on exceptional access popped up—Ernie Brickell, Stefan Savage, and Robert Thibadeau—and he thought it might be a good idea if they all met in private. Last August the four scientists gathered in Meg Whitman's boardroom at Hewlett Packard Enterprise in Palo Alto. (Ozzie is a board member, and she let him borrow the space.) Though Thibadeau's work pursued a different course, Ozzie found that the other two were pursuing solutions similar to his. What's more, Savage has bona fides to rival Ozzie's. He's a world-renowned expert on security research, and he and Ozzie share the same motivations. "We say we are scientists, and we let the data take us where they will, but not on this issue," Savage says. "People I very much respect are saying this can't be done. That's not why I got into this business."

Ozzie's efforts come as the government is getting increasingly desperate to gain access to encrypted information. In a speech earlier this year, FBI director Christopher Wray said the agency was locked out of 7,775 devices in 2017. He declared the situation intolerable. "I reject this notion that there could be such a place that no matter what kind of lawful authority you have, it's utterly beyond reach to protect innocent citizens," he said.

Deputy attorney general Rod Rosenstein, in a speech at the Naval Academy late last year, was even more strident. "Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety," he said. What's needed, he said, is "responsible encryption ... secure encryption that allows access only with judicial authorization."

Since Apple, Google, Facebook, and the rest don't see much upside in changing their systems, only a legislative demand could grant law enforcement exceptional access. But there doesn't seem to be much appetite in Congress to require tech companies to tailor their software to serve the needs of law enforcement agencies. That might change in the wake of some major incident, especially if it were discovered that advance notice might have been gleaned from an encrypted mobile device.

As an alternative to exceptional access, cryptographers and civil libertarians have begun promoting an approach known as lawful hacking. It turns out that there is a growing industry of private contractors who are skilled in identifying flaws in the systems that lock up information. In the San Bernardino case, the FBI paid a reported $900,000 to an unnamed contractor to help them access the data on Farook's iPhone. Many had suspected that the mysterious contractor was an Israeli company called Cellebrite, which has a thriving business in extracting data from iPhones for law enforcement agencies. (Cellebrite has refused to confirm or deny its involvement in the case, and its representatives declined to comment for this story.) A report by a think tank called the EastWest Institute concluded that other than exceptional access, lawful hacking is the only workable alternative.

But is it ethical? It seems odd to have security specialists promoting a system that depends on a reliable stream of vulnerabilities for hired hackers to exploit. Think about it: Apple can't access its customers' data—but some random company in Israel can fetch it for its paying customers? And with even the NSA unable to protect its own hacking tools, isn't it inevitable that the break-in secrets of these private companies will eventually fall into the hands of criminals and other bad actors? There is also a danger that forces within the big tech companies could enrich themselves through lawful hacking. As one law enforcement official pointed out to me, lawful hacking creates a marketplace for so-called zero-day flaws—vulnerabilities discovered by outsiders that the manufacturers don't know about—and thus can be exploited by legal and nonlegal attackers. So we shouldn't be surprised if malefactors inside tech companies create and bury these trapdoors in products, with hopes of selling them later to the "lawful hackers."

Lawful hacking is techno-capitalism at its shadiest, and, in terms of security alone, it makes the mechanisms underlying Clear (court orders, tamper-proof contents) look that much more appealing. No matter where you stand in the crypto debate, it makes sense that a carefully considered means of implementing exceptional access would be far superior to a scheme that's hastily concocted in the aftermath of a disaster. (See Clipper.) But such an approach goes nowhere unless people believe that it doesn't violate math, physics, and Tim Cook's vows to his customers. That is the bar that Ozzie hopes he can clear.

The "Keys Under Doormats" gang has raised some good criticisms of Clear, and for the record, they resent Ozzie's implication that their minds are closed. "The answer is always, show me a proposal that doesn't harm security," says Dan Boneh, a celebrated cryptographer who teaches at Stanford. "How do we balance that against the legitimate need of security to unlock phones? I wish I could tell you."

One of the most salient objections goes to the heart of Ozzie's claim that his system doesn't really increase risk to a user's privacy, because manufacturers like Apple already employ intricate protocols to protect the keys that verify its operating system updates. Ozzie's detractors reject the equivalence. "The exceptional access key is different from the signing key," says Susan

rory of the Crypto Wars

1976: Scientists introduce public
rography, in which private and
mplementary keys are used to
nd unlock data. 1982:
mes one of the first companies to
ption to the business and consumer
1989: Lotus Notes becomes the first
software to obtain a license to ex-
port strong encryption overseas.
Clinton administration announces a
e so-called Clipper Chip. 1994:
scientist finds a critical vulner-
Clipper Chip. The US abandons
the program within two years.
1999: The Clinton admin-
oves nearly all restrictions
rt of encryption products.
ner NSA contractor Edward
eals classified information
nment surveillance programs.
2014: Apple introduces default
iOS 8. 2016: After
ting in California, the Feds file
er against Apple to access the
contents of a shooter's phone.

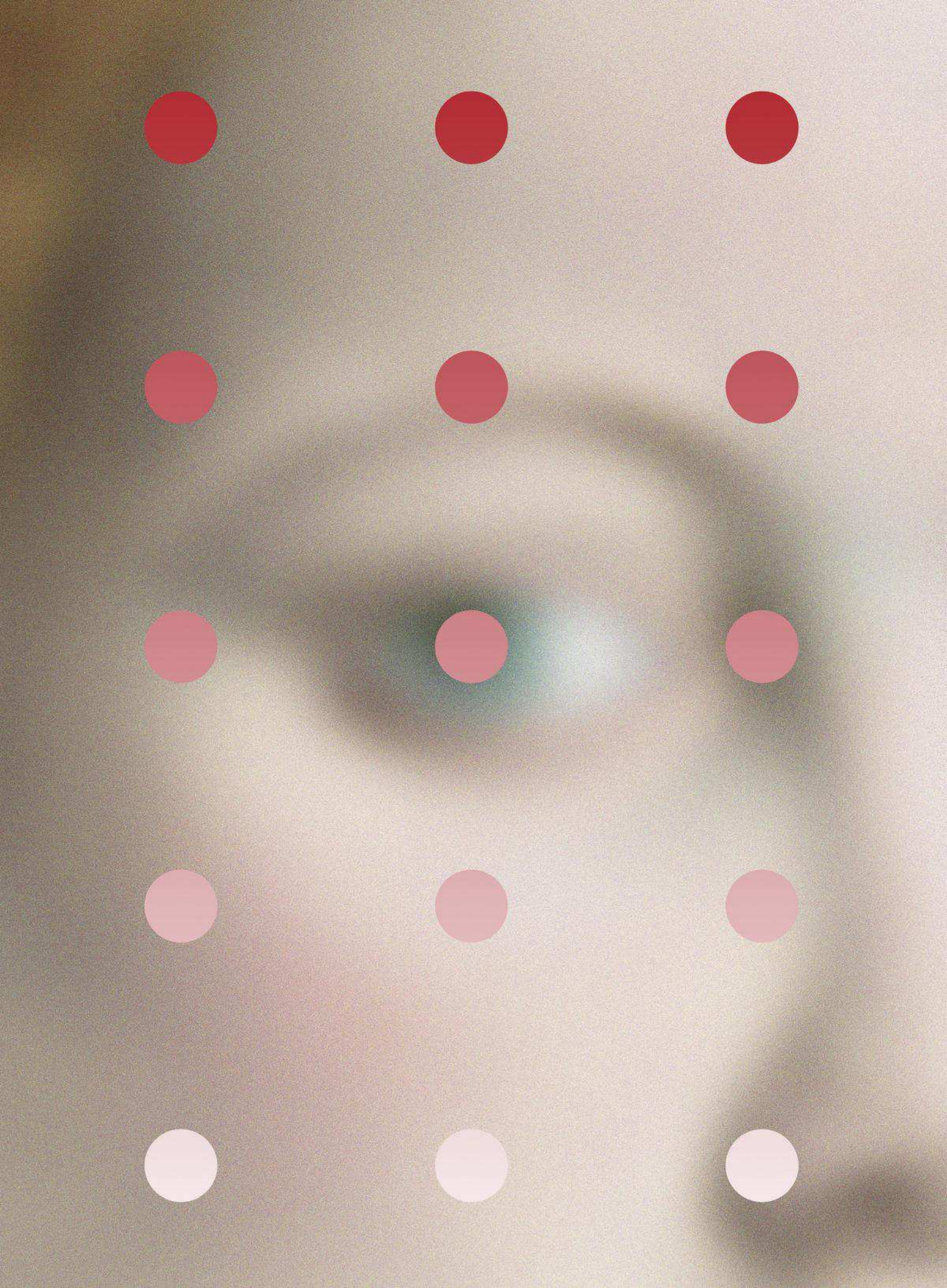
Landau, a computer scientist who was also a coauthor of the "Doormat" paper. "A signing key is used rarely, but the exceptional access key will be used a lot." The implication is that setting up a system to protect the PINs of billions of phones, and process thousands of requests from law enforcement, will inevitably have huge gaps in security. Ozzie says this really isn't a problem. Invoking his experience as a top executive at major tech firms, he says that they already have frameworks that can securely handle keys at scale. Apple, for example, uses a key system so that thousands of developers can be verified as genuine—the iOS ecosystem couldn't work otherwise.

Ozzie has fewer answers to address criticisms about how his system—or any that uses exceptional access—would work internationally. Would every country, even those with authoritarian governments, be able to compel Apple or Google to cough up the key to unlock the contents of any device within its jurisdiction? Ozzie concedes that's a legitimate concern, and it's part of the larger ongoing debate about how we regulate the flow of information and intellectual property across borders. He is also the first to point out that he doesn't have all the answers about exceptional access, and he isn't trying to create a full legal and technological framework. He is merely trying to prove that something could work.

Maybe that's where Ozzie's plan plunges into the choppiest waters. Proving something is nigh impossible in the world of crypto and security. Time and again, supposedly impervious systems, created by the most brilliant cryptographers and security specialists, get undermined by clever attackers, and sometimes just idiots who stumble on unforeseen weaknesses. "Security is not perfect," says Matthew Green, a cryptographer at Johns Hopkins. "We're really bad at it."

But as bad as security can be, we rely on it anyway. What's the alternative? We trust it to protect our phone updates, our personal information, and now even cryptocurrencies. All too often, it fails. What Ozzie is saying is that exceptional access is no different. It isn't a special case singled out by the math gods. If we agree that a relatively benign scheme is possible, then we can debate whether we should do it on the grounds of policy.

Maybe we'd even decide that we don't want exceptional access, given all the other tools government has to snoop on us. Ozzie could return to his post-economic retirement, and law enforcement and civil libertarians would return to their respective corners, ready to slug it out another day. Let the Crypto Wars continue.



By
AMANDA SCHAFFER
-
Illustrations by
CHAD WYS

I N F E C T I O U S

Bill Halford was convinced he'd found a miracle cure, but he was running out of time to prove it. So he teamed up with a Hollywood executive and recruited a band of desperate patients. Inside one man's race against death—and the rules of scientific research.

I

IN A PHOTO FROM 2009, Bill Halford, who was then 40 years old, looks like a schoolboy who hasn't quite grown into his big ears. He wears an ill-fitting red shirt tucked into belted khakis; his jawline is square and his eyes are full of wonder. The picture was taken at Southern Illinois University, where he was a respected professor. A few years before, he had made a significant discovery—one that would determine the course of his life.

Halford, a microbiologist, had taken an interest in the peculiar nature of herpes—how it lies dormant in the nervous system and reactivates to cause disease. Herpes is one of the most pervasive viral infections in the world, sometimes causing painful genital blisters, and it has frustrated scientists attempting to find a cure. But in 2007, Halford realized that a weakened form of the virus he'd been studying might serve as a vaccine. He designed an experiment in which he inoculated mice with this variant, then exposed them to the wild-type form of the virus. In 2011 he published the results: Virtually all the mice survived. By contrast, animals that were not injected with his vaccine died in large numbers. It was promising science.

That same year, however, Halford became seriously ill. At first he thought he had a sinus infection, but it turned out to be a rare and aggressive form of cancer, sinonasal undifferentiated carcinoma. Halford was 42 years old at the time, with two teenage children. He underwent chemotherapy and radiation followed by surgery, but he was told that the form of cancer he had did not usually stay at bay for long. Halford had always been determined—"a 90-hours-a-week sort of researcher," as his wife, Melanie Halford, puts it. The cancer diagnosis only seemed to harden his focus. Others had tried, and failed, to develop a herpes vaccine, but Halford was convinced that his method—using a live, attenuated form of the virus—would succeed. He would use whatever time he had left to show he was right.

Carolyn suffered from debilitating nerve pain, and when Halford asked if she wanted to try the drug, she says, "I felt like I had hit the lottery."

The trouble was that the institutional gatekeepers of science—the agencies that fund research—didn't view his work with the same urgency. He wasn't getting the grants he thought he deserved. He felt "alone in the wilderness," Melanie says, but also certain that his formula held unique promise. The question that drove him was not the practical "Will this work?" but rather an ethical one: "If I can help people suffering from herpes, isn't it my duty to do so?" Melanie told me that "it was completely obvious to him what needed to be done." Halford decided to barrel forward on his own unorthodox terms.

People with herpes who scoured the internet for research on their condition often discovered Halford's scientific writing and blog posts, which combined technical information and a wry frustration with the status quo. Several readers reached out to Halford for help. A woman named Carolyn, who ran a private Facebook group devoted to genital herpes, approached him in 2012, and a few months later, Halford got back in touch and suggested they talk by phone. "That's when he told me he had been fighting cancer and felt he needed to find out if the vaccine he developed could be therapeutic," Carolyn recalls. In his animal research, Halford was testing whether his attenuated virus could prevent herpes, but scientists were also studying whether herpes vaccines could *treat* the disease. Carolyn suffered from debilitating nerve pain, and when Halford asked if she wanted to try the drug, she says, "I felt like I had hit the lottery."

Through his blog and Carolyn's Facebook group, Halford found other potential research subjects. He told them that the vaccine carried risks, as all vaccines do, but claimed that his formulation was "much safer" than those used for measles, mumps, polio, and chicken pox. Halford reassured the skeptical that he had tested his formula on himself, despite being weak from chemo, and had injected family members, and that they had "no side effects," says Carolyn, who did not want to give her last name because of the stigma attached to herpes. Halford answered the potential volunteers' questions by email and in long phone conversations. He sent at least one of them pictures of the large, red welts that were likely to develop on their calves around the injection site.

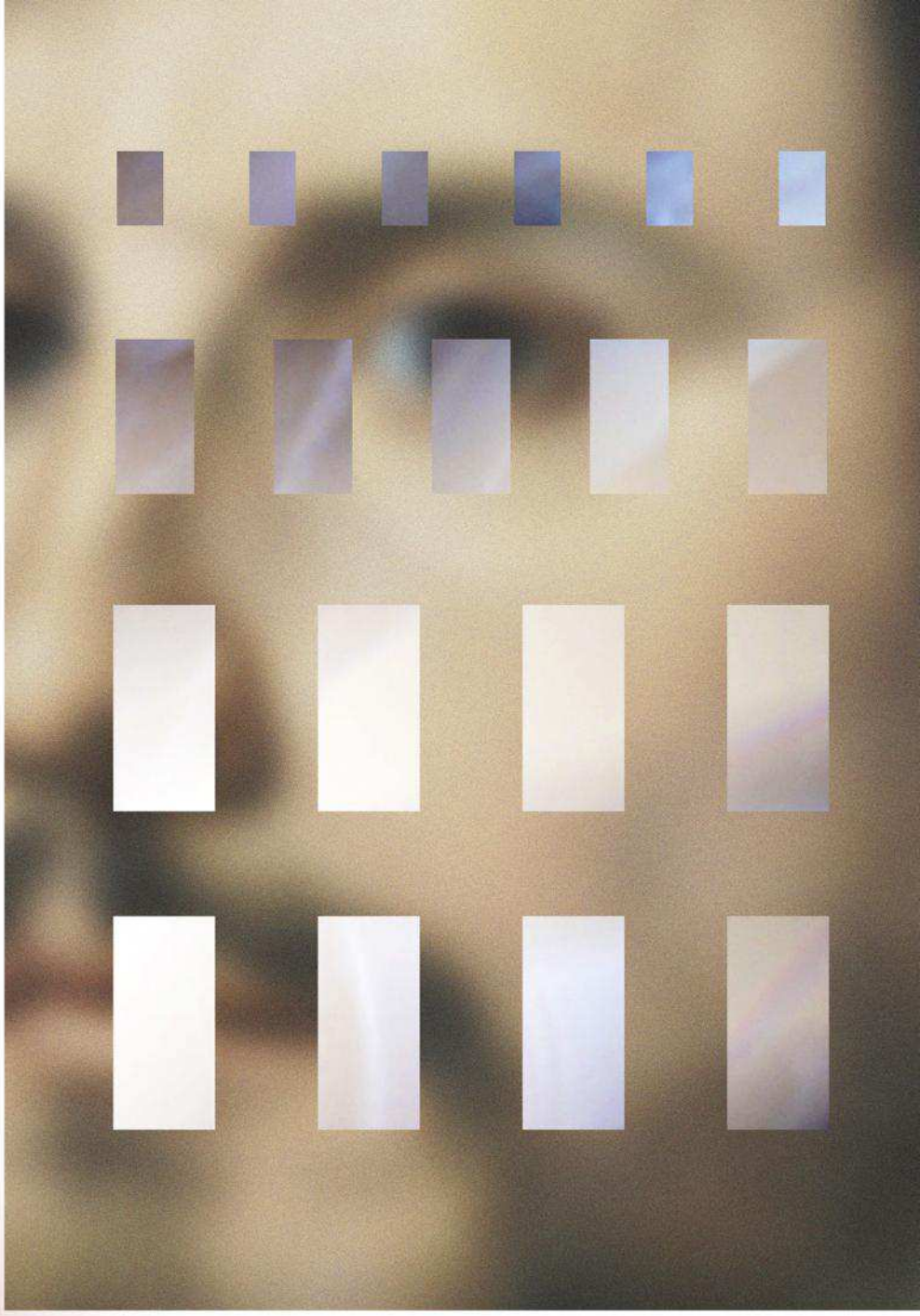
In August 2013, Carolyn drove six hours from Kentucky, where she lives, to Springfield, Illinois, where she had booked a room

AMANDA SCHAFFER *(@abschaffer) is a science writer based in Brooklyn, New York.*

at the Holiday Inn Express. That evening, she and seven other volunteers, who had come from all over the country, gathered with Halford in one of the hotel rooms, where they sat on chairs, the couch, and the bed. "People were excited," Carolyn recalls. Halford arrived with a box, which contained a tray and small vials, and began "mixing what appeared to be components of the vaccine right there," Carolyn says. When her turn came, he took a sample of blood, then swabbed her calf with alcohol and drew a circle on the skin with a black felt-tip pen. Within the circle, he injected the mixture. A bump appeared, followed later by a welt.

In subsequent months, the volunteers gathered in Springfield twice more for injections. The Halfords invited them to their home for dinner. "We were telling Bill and his wife our stories, and they listened," Carolyn says. "They are good people."

As a seasoned researcher, Halford was certainly aware that his behavior violated ethical norms, and probably federal regulations as well. The Food and Drug Administration requires that researchers get permission before using an unapproved drug or agent on people in the United States, according to Hank Greely, an expert in biomedical ethics at Stanford Law School. Halford had not said a word to the agency about his plans, nor did he intend to say anything publicly. That "would be suicide," he told participants in an email obtained by Kaiser Health News. Still, he believed that his brazen behavior would advance the cause of his vaccine; and in one sense, he was right.

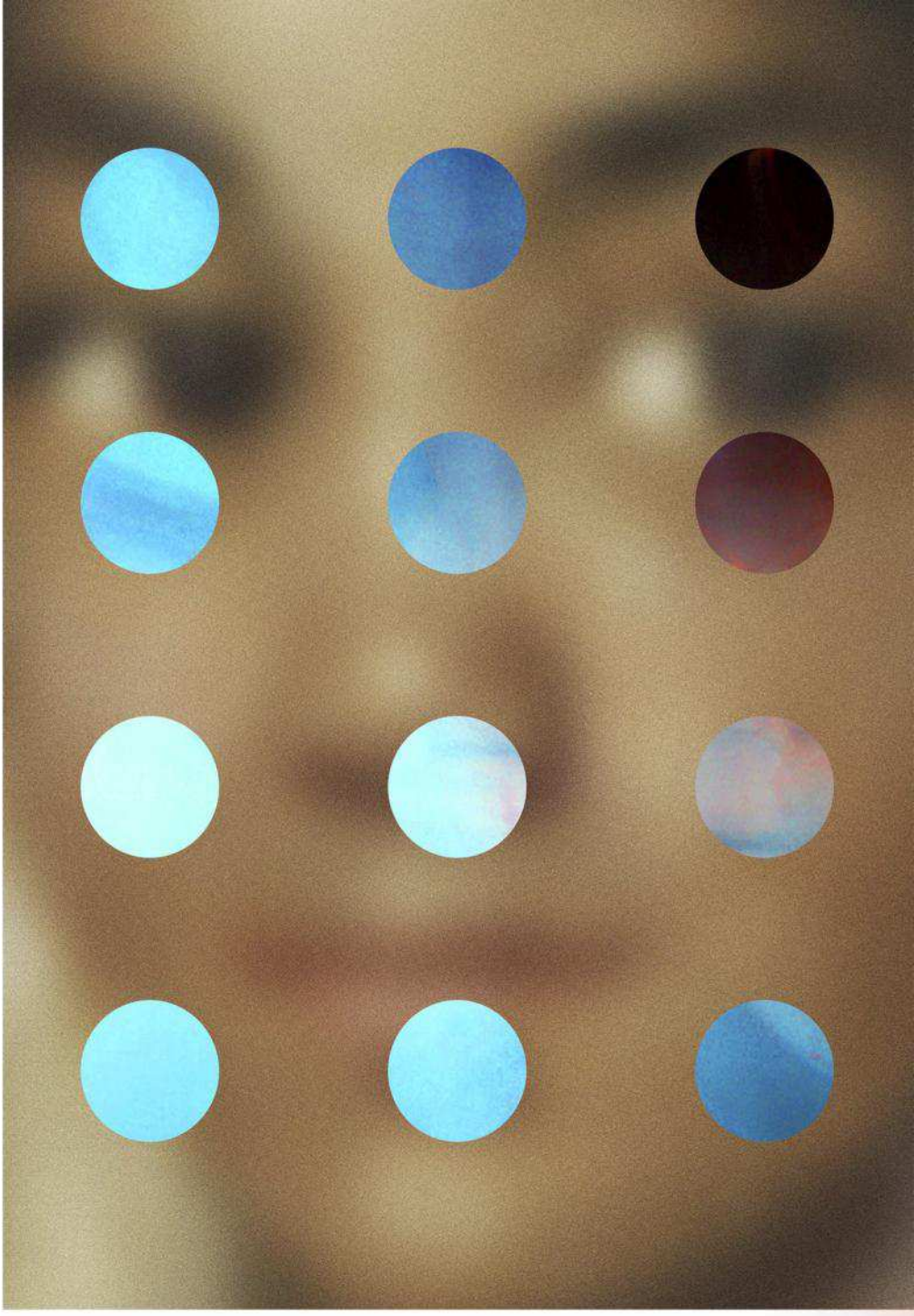


A

AGUSTIN FERNANDEZ is a Hollywood film executive—*Badge of Honor*, a Martin Sheen drama, is his best known movie. Brash and gregarious with a bald head and, sometimes, a trim goatee, he splits his time between New York and Los Angeles. He also has an outsized fear of herpes. Years ago he started dating a woman with the virus. And at first he thought, "OK, what's the big deal, you get a rash." But over time he saw how she suffered during outbreaks and began to fear that he would become infected. "It just completely consumed me," he says.

Fernandez threw himself into online research and, like Carolyn, soon came across Halford's work. "I just made it my mission to meet him," Fernandez says. Eventually, Fernandez persuaded Halford to fly to New York and join him for dinner at Frankies 570 Spuntino Italian restaurant. They talked for hours. "Bill probably still thought I was a crazy guy," Fernandez says. "I was just on a very selfish mission." Still, they met again in Chicago. Halford confided to Fernandez that he'd secretly tested the vaccine in humans and that a participant named Carolyn had not experienced herpes outbreaks since the injections and had even stopped taking antiviral medications. "I thought I'd found the holy grail," Fernandez says.

To Fernandez, the next step seemed obvious: Start a company. Fernandez didn't know much about scientific research, but he did know how to intrigue investors.



He figured a herpes vaccine would be an easy sell, and more gratifying than raising money for a Hollywood movie. "It's not like, 'This is so great, Steven Seagal is going to punch a mummy in the face!' This is like, 'We can really change the world.' "

In 2015 Halford and Fernandez founded Rational Vaccines. Fernandez provided most of the initial money and then reached out to friends and family, raising a total of around $700,000. Halford cared mainly about intellectual control; he would oversee the science. The company also licensed a patent for Halford's work from Southern Illinois University, where Halford remained a professor.

Halford started making plans for a clinical trial overseas, outside the jurisdiction of the FDA—a not uncommon strategy. He never seriously considered submitting plans to the agency, which would have required him to manufacture the vaccine in a standardized manner and comply with the FDA's oversight and requirements. "It takes years and years," Melanie says—years that Halford did not anticipate having.

Pharmacological testing of any kind involves risks, and the standards for vaccine safety have evolved over time. Edward Jenner, the late-18th-century English scientist, demonstrated that he could protect an 8-year-old boy from smallpox by exposing him to a related virus called cowpox. It wasn't until the 1950s, however, when the American virologist Jonas Salk developed a polio vaccine, that the modern era of mass inoculation began. Polio had left thousands of children paralyzed, and Salk's vaccine is rightly viewed as a triumph of 20th-century science. At the same time, problems at one of the first production labs led to vaccine contamination that paralyzed 164 children and killed 10 others, a tragedy that might have been averted with better safety testing.

Improved oversight of drug development arrived in 1962 with the modernization of the FDA. In the wake of the thalidomide scandal, in which a drug to treat morning sickness was found to cause birth defects, the agency began requiring companies to complete three phases of clinical testing, demonstrating the safety and efficacy of their products. Scrutiny of vaccines increased too. In the early days, researchers typically tested vaccines on a few thousand people at a cost of several million dollars. Now they are expected to conduct trials with tens of thousands of subjects, with expenses in the hundreds of millions. Regulators also have strict requirements for ensuring the purity of products that will be tested in humans and tend to be cautious about side effects. "The bar has gotten much higher," says Paul Offit, director of the Vaccine Education Center at Children's Hospital of Philadelphia.

This can make it hard for small companies to develop vaccines, even when they report promising data. Last fall, Genocea, a small biotech firm, got as far as successful Phase II trial results for a herpes vaccine, but then the company announced that it was halting the effort. It lacked the capital to continue to the next phase of trials, which CEO Chip Clark says would have cost $150 million. (Genocea says it's still looking to partner with a larger pharmaceutical company.) Given the FDA's regulatory standards, some good vaccines surely don't make it to market because the financial burdens are too great.

To Halford, however, any obstacle to his vaccine seemed an injustice. His cancer returned in early 2016, and this time "his doctors were out of good options," Melanie says. Neither radiation nor surgery was feasible, so he was left with chemotherapy.

Each month he received several days of grueling treatment, which left him nauseated and exhausted. Then he plunged into work again, conducting research and planning for a clinical trial on the Caribbean island of Saint Kitts, before starting the chemo cycle over again.

Halford began to recruit participants for the clinical trial through his personal blog. The desperation he found in the potential volunteers echoed the urgency of his own prognosis, and he was more responsive to their queries than many of their own doctors had been. A woman named Beth Erkelens, who lives in Colorado, learned about Halford's work from a Google search that led to his blog. She called him about the clinical trial, and they talked, she says, "for like an hour." At the time, Erkelens felt desperate. She was 45 years old and, for years, experienced nearly constant itching, as well as about 12 full-blown outbreaks a year. She felt she had nothing to lose and was swayed by Halford's bold assurances, as well as his promise that Rational Vaccines would reimburse her for airfare and hotel for three trips to Saint Kitts. "It was his confidence that drew everyone in," she says.

So when Halford sent Erkelens an informed-consent document laying out the potential risks of participation and noting that the trial would not include FDA oversight, she signed it without hesitation.

I

IN JUNE 2016, Erkelens arrived on the tiny island of Saint Kitts, which was quiet in the summer. Rational Vaccines had set up shop in a house high above a turquoise bay. One room became a makeshift medical office. There, Erkelens' blood was drawn and her temperature taken. Then, as Halford looked on, a physician administered the injection. "We all had high hopes," she recalls.

Initially, Erkelens' only reaction was a walloping welt, which she had been told to expect and which seemed more of a curiosity to her than anything else. It was also a kind of badge. Before coming to Saint Kitts, Erkelens had avoided talking about her woes, except with potential partners. But on the island it was easy to spot other Americans who had also flown down for the clinical trial. "How do you miss another person with a giant red mark on the back of their leg when there's no one else around?" In many ways, the trip felt like a group vacation.

Erkelens spent about five days on the island and recalls afternoons lounging on the beach, drinking beers at the bar, and exploring the island, where vervet monkeys ambled down from the hills. In the evenings, Fernandez sometimes paid for seafood dinners and drinks out of his own pocket. Participants had been flying to the island since March, receiving injections on a staggered schedule. Fernandez had been there for much of the time. When Erkelens returned home, she was already looking forward to her next island jaunt. She even planned to bring her 11-year-old son to Saint Kitts and stay between her second and third shots so he, too, could enjoy a "big, beachy vacation."

"There were no protections for these people. There was no one watching over the conduct of this trial ... I mean, what was he thinking?"

In July, however, when Erkelens and her son arrived in Saint Kitts for her second shot, things did not go so well. This time she experienced an intense herpes outbreak after the injection, along with severe aches and pains, numbness and tingling in her arms and legs, shooting sensations, and "crazy, crazy shaking." Halford had warned that she might feel flu-like symptoms, but this went far beyond that. By the time her symptoms started setting in, however, the other trial participants and researchers were leaving the island.

A little more than a week later, Erkelens sent frantic messages to Halford telling him how sick she was. "That's when he called me," she says. "He was really angry," insisting, she says, that the symptoms were caused not by the vaccine but by a mosquito-borne virus called chikungunya. But he called back and offered to discuss her symptoms. (Erkelens says she later tested negative for chikungunya.)

In early August, Erkelens called Halford in distress from Saint Kitts, where she had remained for several weeks. Halford was in Portland, Oregon. He had flown there to ask a herpes expert named Terri Warren to join the board of Rational Vaccines. Warren, who was trained as a nurse practitioner and ran a sexual-health clinic in Portland for decades, has served as an investigator on more than 100 clinical trials, mostly involving herpes. She and Halford had worked together previously, but as he sat at her kitchen counter and described the experiment already under way in Saint Kitts, she grew increasingly alarmed. "There were no protections for these people," she says. "There was no one watching over the conduct of this trial."

While US companies frequently pursue clinical research abroad, often to save money, they virtually never do so without oversight from some kind of institutional review board, which tries to ensure that the potential benefits of an experiment outweigh the risk to participants. IRBs review every aspect of a trial: the script researchers use to recruit participants, the entry criteria for the study, the wording of the informed consent document, the protocol for administering the drug or vaccine, rules for record keeping and reporting adverse events. These norms were established in response to historic abuses like the Tuskegee study, in which, over the course of 40 years, researchers observed how syphilis affected African American men without explaining fully what they were researching and failing to treat them even when an effective cure was found. Part of the idea of

having a review board, though, is that even well-meaning researchers can lack perspective on their own work and require a third party to set them straight.

With mounting agitation, Warren grilled Halford on the kinds of issues an IRB might care about: Where did this vaccine come from? Who manufactured it? How was it shipped? How had he made sure that it was free from contaminants? Halford did not have satisfying answers. Warren also wanted to know how he had screened trial participants and was disturbed to learn that he had included people with two different strains of herpes virus, HSV-1 and HSV-2. The vaccine contained a live form of HSV-2, so the risks to individuals who only had HSV-1 were potentially higher. "I mean," Warren told me, "what was he thinking?"

Compounding Warren's concerns was Halford's approach to data collection. He relied on questionnaires that participants filled out regarding their symptoms. Warren felt that the self-reports could potentially be influenced by a desire to please the researchers, especially since personal relationships had developed on an isolated island. "There was a lot of socializing with the investigators and the guy from Hollywood," Warren says. "They'd sit around at the bar and drink and talk, and that's just not appropriate."

And then there was Halford's casual approach to adverse events. When he admitted to Warren that some participants were having bad reactions to the vaccine, she asked, "Well, what are you going to do about that? How are you going to follow them?" His response, she says: "We removed them from the trial." But that solves nothing, Warren told him. It leaves research subjects vulnerable and doesn't answer crucial questions about the vaccine. "That's not how you do it," she told him. "You continue them in the trial and you follow them" because you want to know what the vaccine does.

Throughout the two-and-a-half-hour conversation, Warren felt she made little headway with Halford. "I wouldn't describe him as belligerent, but he was not introspective in any way," she says. "Just defensive." She told him she wanted nothing to do with the clinical trial or the company. (Rational Vaccines declined to comment on Warren's account.)

In early August, when Halford returned to Saint Kitts to oversee another round of injections, he asked Erkelens to meet him, Fernandez, and the doctor who administered the injections at a coffee shop. She still felt acutely ill, and as she approached the meeting with her son in tow, she was anxious that her symptoms would not be taken seriously. She also worried about letting Halford down, knowing how much he'd invested in the vaccine. Almost as soon as the conversation started, Erkelens says, Fernandez reminded her that she had signed a legal document acknowledging that the vaccine carried risks. It seemed her relationship with Rational Vaccines had shifted: "I was no longer their friend," she says. "I was a foe." (Fernandez denies that he brought up the informed-consent document and says that the company's primary concern was to address Erkelens' symptoms.)

Halford was not well. "He looked like he might throw up or pass out," Erkelens says. At one point, she says, he shot her a sympathetic look and brought her and her son outside, where they could talk alone. As they walked along the road, in the direction of Erkelens' hotel, Halford told her that he wanted to draw her blood again and try to understand why she'd become so ill; she could decide if she wanted the third injection. He had "a very big heart," says Erkelens, who agreed to provide another blood sample. But she was afraid to continue with the vaccine. "I'm convinced the third shot would have killed me," she says. "I felt like I was 100 years old."

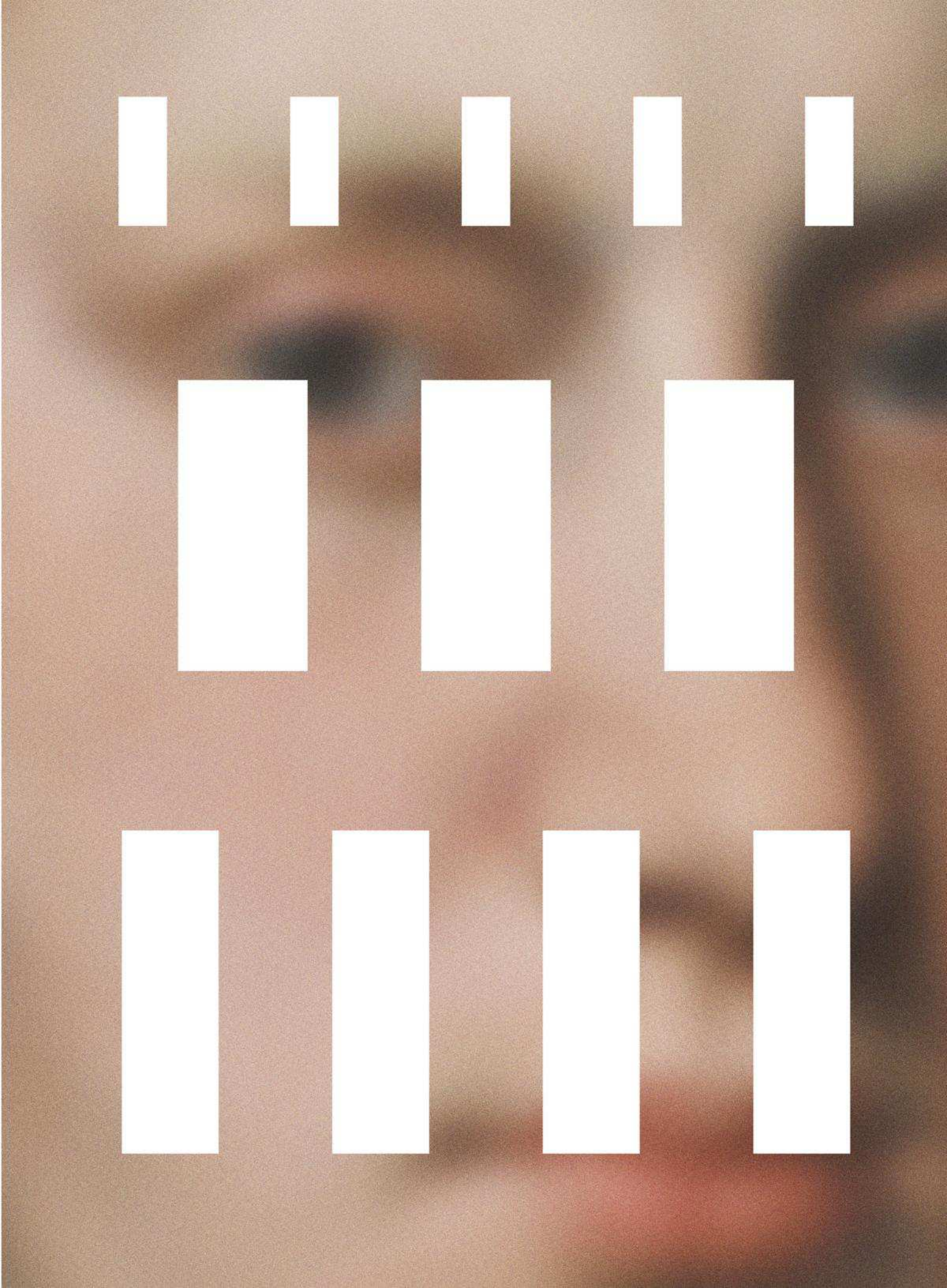
H

HALFORD'S CANCER WAS taking an increasing toll. When Melanie picked him up at the airport in August, at the end of the clinical trial, he was seeing double and couldn't drive. She later learned that he had a seizure in Saint Kitts but kept it from her, not wanting her to worry.

Racing against time, Halford wrote up the results of the Saint Kitts trial. He reported that 17 out of 20 subjects completed the three-injection series and described, on average, a "3.1-fold reduction in their frequency of herpes-symptomatic days." For one participant, Halford also presented blood test results, which seemed to indicate a greater range of antibodies to the herpes virus after the vaccine than before. Nowhere in the manuscript did Halford provide data on the three participants who did not complete the trial, nor did he refer to adverse events beyond welts at the injection site.

When Halford submitted the manuscript to a peer-reviewed journal called *Future Virology*, the response was scorching. In reviews later obtained and posted online by Kaiser Health News, one scientist argued that "neither safety nor efficacy has been demonstrated by the data presented" and described the paper as "partly a vision, partly science, and partly wishful thinking." The reviewers also came down hard on the lack of documented oversight: "Who is giving the immunizations in Saint Kitts and who is following them medically when they return to the US? Where is the clinical protocol based? Is this an end run around the FDA?" The manuscript was rejected.

If Halford failed to win approval from academic peers, he struck gold with investors. Earlier that year, Fernandez says, an angel investor named Paul Bohm, who had cofounded a hackerspace called Metalab and had Silicon Valley ties, reached out to Rational Vaccines and offered to put the company in touch with venture capitalists. Drawing on these connections, Fernandez spent months



pitching the research. In April 2017, at a symposium at Southern Illinois University, Halford stood in an auditorium and described the long arc of his research. A former managing director of Credit Suisse named Bart Madden was in the audience, and he was enthralled. "He's got a patch on his eye, he can't hear out of one ear, he's all messed up, but he gets up there for 20 minutes," Madden says. "I felt like I was watching history being made, just like the smallpox cure with [Edward] Jenner." Madden later invested $750,000, Fernandez told me. (Bohm did not respond to requests for an interview, and Madden declined to confirm or comment on the size of his investment.)

Madden, who retired from Credit Suisse in 2003, is an author and policy adviser to the conservative-libertarian Heartland Institute. He focuses on market-based solutions to public policy issues. In 2010 he wrote a book called *Free to Choose Medicine*, which argues that the FDA's risk-averse approach to drug approval gets in the way of innovation and keeps life-saving medicines off the market. He first heard about Halford in early 2017, when a documentary filmmaker contacted him for an interview about Halford's research and free-to-choose medicine. In Madden's eyes, Halford embodied the part of the brilliant outsider tangling with the scientific establishment.

Madden also took note that Peter Thiel, the legendary early investor in Face-

"I had to take a chance Dr. Bill was dying. Nobody wanted to speak up, so I was like, 'I'll do it.'"

book, was also interested in Rational Vaccines. Thiel is known for contrariness and taking arms against regulation and norms. A libertarian, he has criticized the FDA, calling the agency too restrictive and questioning whether an innovation like the polio vaccine could be achieved today.

"It caught my attention that Peter Thiel had done an incredible amount of due diligence on this," Madden says. (Fernandez says he was first introduced to Jason Camm, the chief medical officer of Thiel Capital, by Paul Bohm, in early 2017. Camm was present at the April symposium, according to Fernandez, but Thiel was not.)

Madden also was moved by the testimony of a trial participant named Rich Mancuso, who attended the symposium. Mancuso has red hair and a puckish smile. He was working as an exterminator in New Jersey when he first met Halford online. He had been infected with herpes for more than 20 years, and though the symptoms waxed and waned, he experienced outbreaks as often as twice a month on his genitals and face. Mancuso told Madden about the humiliation of living with inflamed facial sores and the financial toll of paying for antiviral medicines. Dating was nearly impossible, and one rejection in particular brought him to the verge of suicide. Since receiving three shots of Halford's vaccine, however, he had intervals of several months without the blistering sores. In gratitude, Mancuso chose to speak publicly to make his support more credible. "I had to take a chance," he told me. "Dr. Bill was dying. Nobody wanted to speak up, so I was like, 'I'll do it.'"

With strong interest from investors—and at least one public success story—the company's fortunes appeared to be ascendant. Halford's health, however, was spiraling downward. By May 2017, it was no longer possible for him to work. And by early June, it was clear that he was close to death.

Halford had a jade necklace that he wore at all times, "like a talisman, to remind him to seize the day," Melanie says. He got it a couple of years after his diagnosis, on a family trip to New Zealand. On June 22, he placed the necklace on his nightstand; when Melanie saw it there, she realized it was his way of saying, "I'm giving this up now."

I

IN AUGUST, two months after Halford's death, the company received a total of $7 million from investors, Fernandez says, including $4 million from Thiel funds. At nearly the same time, however, Kaiser Health News broke the story that Halford had carried out a clinical trial with no guidance from the FDA or an institutional review board. The dean of Southern Illinois University's School of Medicine had once referred to Halford as a "genius," and the school had promoted his vaccine work on its website. But when details of the Saint Kitts research emerged, the university quickly distanced itself, saying that the institution was unaware of the trial's oversight issues until after the work was done.

The university has acknowledged that there were serious problems with Halford's work, and its medical school has halted all herpes simplex virus research. A spokesperson confirmed that "the government is conducting an investigation, and we are fully cooperating."

Rational Vaccines is trying to weather the storm. As CEO, Fernandez is now charting a new course for the company, leaning on a recently hired chief technical officer as well as his investors. Madden says he first learned of the hotel-room injections and lack of oversight in Saint Kitts from news reports and admits he is troubled by what he heard. At the same time, "I don't want to give opinions about this scientist that I revere," he says, referring to Halford. "Was it done the right way? No." But he said that now the company would comply with "the highest standards of gathering data." Fernandez says Thiel Capital is also encouraging Rational Vaccines to conduct Phase I trials to follow FDA protocols. Camm, the chief medical officer at Thiel Capital, is "really one of the driving forces behind this whole thing," Fernandez says. "If it were up to him, we'd be at the FDA already. I'm the one saying, 'Let me get all the ducks in a row.'" (Neither Camm nor Thiel responded to numerous requests for interviews.)

The US market is lucrative and large, and "if you want to sell a treatment in the US, you have to play by US rules," says Greely, of Stanford Law School. "I don't care how libertarian you are."

That doesn't mean that the company will have an easy time with the FDA, which will likely ask to see all the data from Saint Kitts, as well as the lab notes for the animal studies. "The FDA will go back and look at the records, and if they're not in order, they can't be used," says Robert Califf, a former commissioner of the agency. Still, if the company can convince the agency that the vaccine looks promising in animals—and that it is prepared to follow the rules—the agency is likely to allow further research. The FDA's goal is not to punish, Califf says, speaking generally. "If there's a good product and a bad company, the role of the FDA is to help get the good product through the system." (The FDA declined to comment.)

Of course, more often than not, products that seem exciting in preclinical work fail in subsequent rounds of testing. Plenty of potential herpes vaccines, both preventive and therapeutic, have disappointed researchers in late-stage animal testing or in clinical trials over the years. "I think collectively we've all thrown the kitchen sink" at herpes efforts, says Clark, of Genocea. "It's a hard virus, it really is."

F

FOR MONTHS AFTER she received the injections in Saint Kitts, Erkelens struggled to take her son to school, then often lay in bed for the rest of the day, unable to move. She continues to experience relentless tremors and intermittent nerve pain. "Nobody knows what's going on," she says.

Trial participants who felt better after the vaccination have a different concern: future access to the vaccine, both for themselves and others who are suffering. Rich Mancuso says he has not had an outbreak in more than a year but worries that if his symptoms do return, he won't be able to get a booster shot—an option that Halford discussed with him. Carolyn says her symptoms disappeared for more than two years but "slowly started creeping back." Now she gets occasional nerve pain, lasting a few minutes. "Most of the time it's bearable, but I have been woken up in the middle of the night a few times as it got severe."

Erkelens has hired a lawyer and is suing Rational Vaccines in state court for negligence and lack of informed consent. (Her lawyer argues that the document she signed before the trial did not fully represent the risks of the vaccine.) One other trial participant and one person who received hotel-room injections from Halford in 2013 have also filed suit against the company. (Rational Vaccines declined to comment on any legal proceedings.)

Before Halford died, Erkelens says, he called her "over and over and over" to see how she was doing. Halford always tried to understand the pain of the participants in his study; his empathy was part of what drew them to him. Yet it was perhaps his own suffering that made him blind to the larger implications of his actions. In what felt like the final insult, Erkelens said she had to reveal her identity in order to proceed with the lawsuit. It was an agonizing choice. Herpes had always felt like a mark of dishonor, and now it threatened to stain her public reputation as well. In the days after she filed the lawsuit, she set the wheels in motion to change her name.

COLOPHON

MELTDOWNS THAT HELPED GET THIS ISSUE OUT:

Alfredo sauce disasters; scuppered peace talks between the cat and the dog; Sam Nunberg; furniture I was charged for months ago yet somehow is still back-ordered; the BART conductor thanking everybody for their "forbearance"; catharsis cafés; my dad smoking marijuana for the first time and throwing up in my bed; my brother's fiancée asking whether I understood the meaning of "cocktail attire"; too much natural light in the LA office; wedding-planning insanity; three kids in the backseat on the way to Grandma's house; angst over an invasive mystery rash that just won't go away; the Cambridge Analytica datastrophe; poorly crafted procedural flowcharts; when #daisysaysnope; the SodaStream explosion that disabled my Bodum electric burr grinder—my most bougie gadgets are out to kill each other; getting my face melted repeatedly at MMJ OBH4 in the DR; semi-nightly overthinks/spirals of self-hatred; five freelance 1040 tax forms all hitting my mailbox at once; JURY DUTY.

WIRED is a registered trademark of Advance Magazine Publishers Inc. Copyright ©2018 Condé Nast. All rights reserved. Printed in the USA. Volume 26, No. 5. WIRED (ISSN 1059–1028) is published monthly 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. Robert A. Sauerberg, Jr., President and Chief Executive Officer; David E. Geithner, Chief Financial Officer; Pamela Drucker Mann, Chief Revenue & Marketing 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.

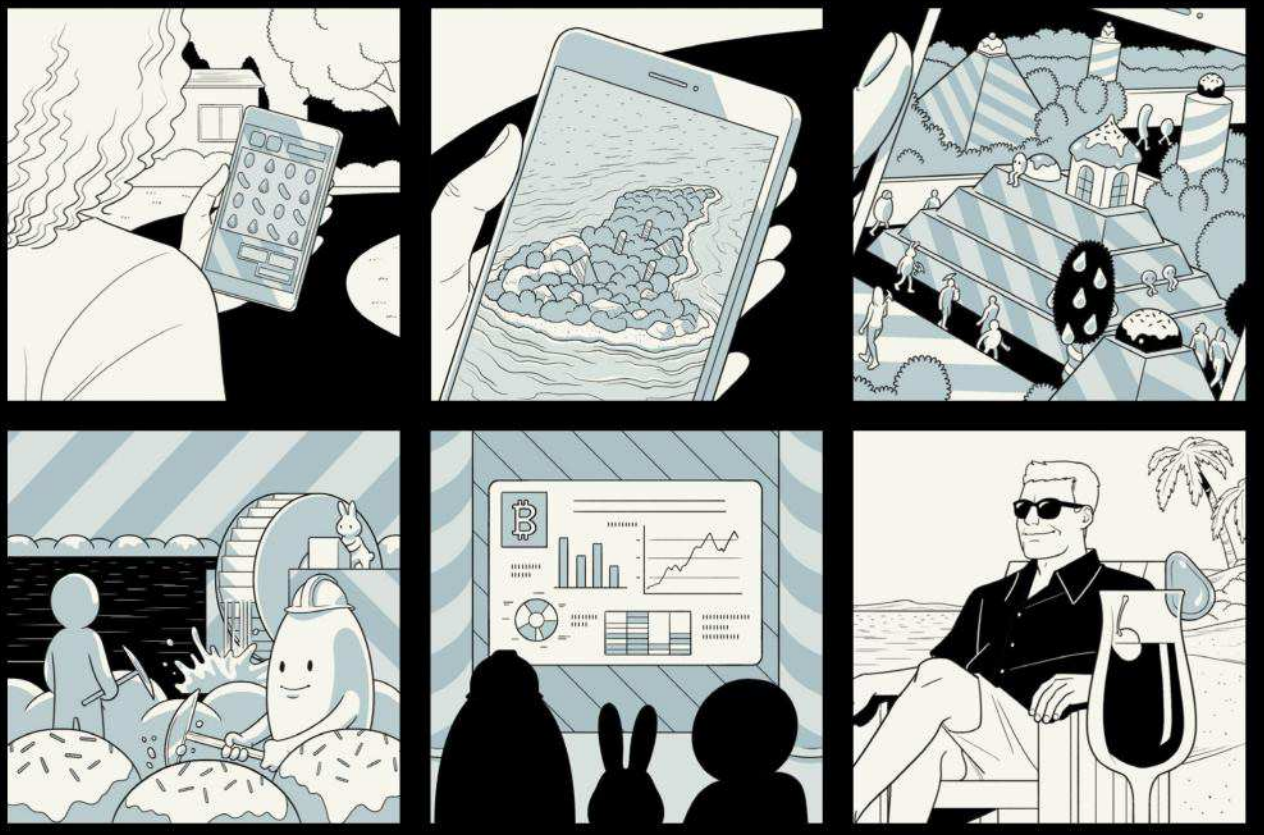
POSTMASTER: Send all UAA to CFS (see DMM 707.4.12.5); NONPOSTAL AND MILITARY FACILITIES: Send address corrections to WIRED, PO Box 37706, Boone, IA 50037-0662. For subscriptions, address changes, adjustments, or back issue inquiries: Please write to WIRED, PO Box 37706, Boone, IA 50037-0662, call (800) 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 www.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 37706, 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.

SIX BY SIX: STORIES BY WIRED READERS

Each month, we publish a six-word story—and it could be written by you. Submit your six words on Twitter, Facebook, or Instagram, along with #WIREDBACKPAGE. We'll pick one story to illustrate here. **Your next assignment: In six words, write a story about the high-tech future of the pot industry.**

#WIREDBACKPAGE



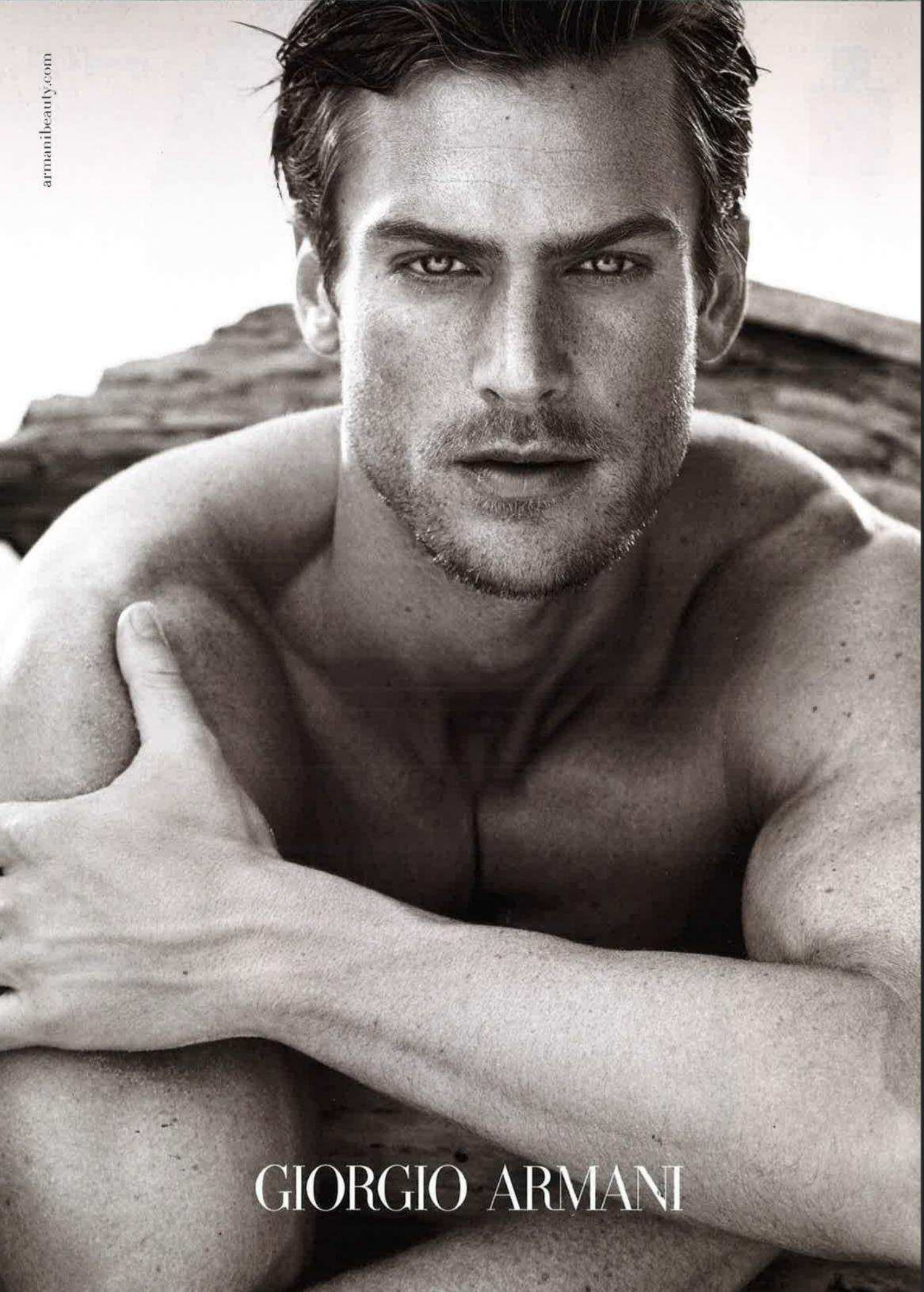
AN EPIC HACKER CAPER:

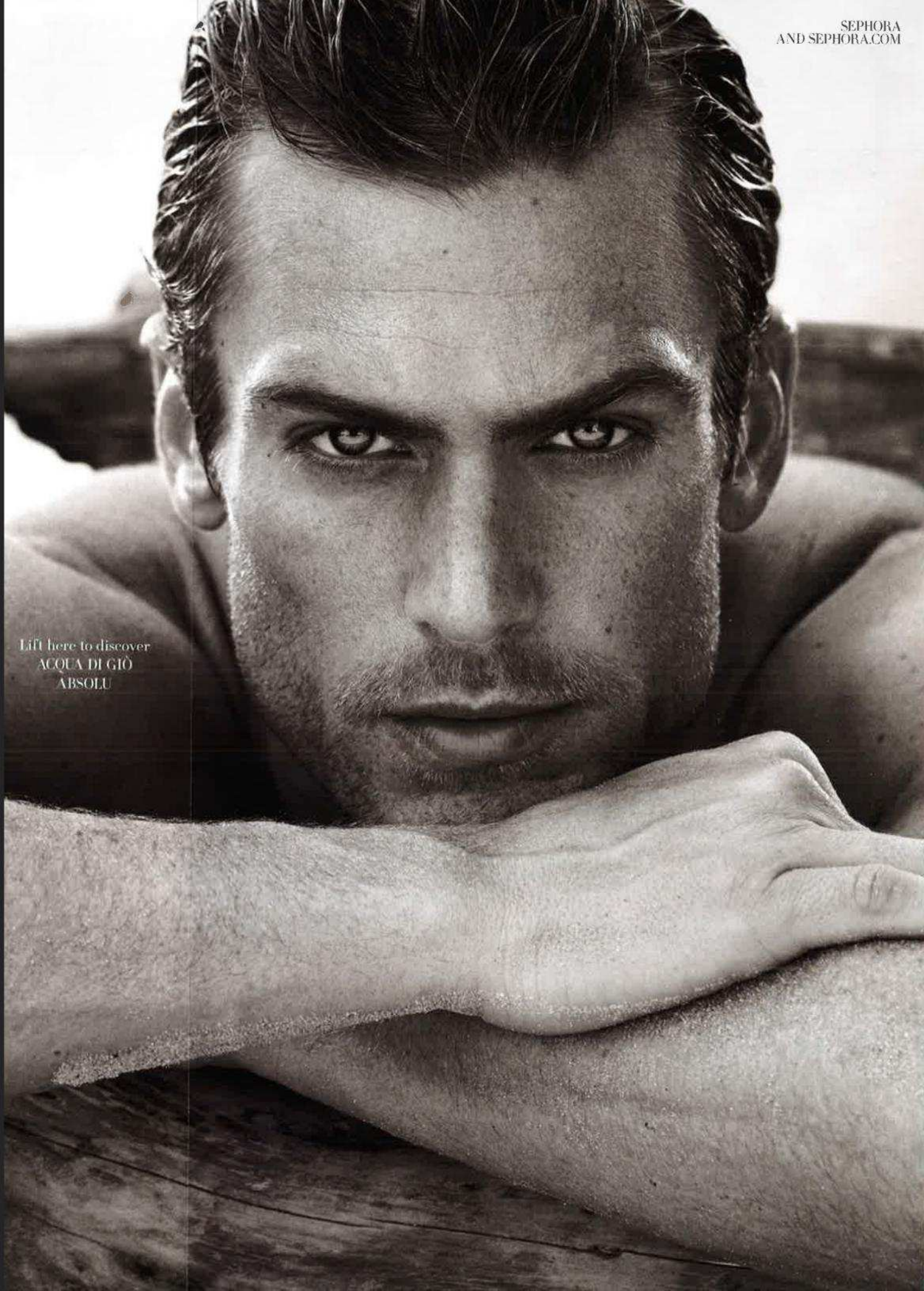
CANDY CRUSH WAS ACTUALLY MINING BITCOIN.

BY @DANIEL_ZAPPALA, VIA TWITTER

HONORABLE MENTIONS: THE WHITE HAT HACKER WENT BLACK. (@SOUPOFBIDET, VIA INSTAGRAM) **// ONE COMMAND LINE, FOURTEEN TRILLION DOLLARS.** (@ITSMECHRISWONG, VIA INSTAGRAM) **// WHY IS MY TOASTER PINGING CHINA?** (@JORDAN9001, VIA TWITTER) **// HE STOLE FACES TO GAIN RECOGNITION.** (@KRAMERICA93, VIA INSTAGRAM) **// SPACEX ROCKETS REDIRECTED TO RED SQUARE.** (@EKEBY, VIA TWITTER) **// STARTS WITH FREE IPHONES. ENDS BADLY.** (@HONORARYWELSHY, VIA TWITTER)

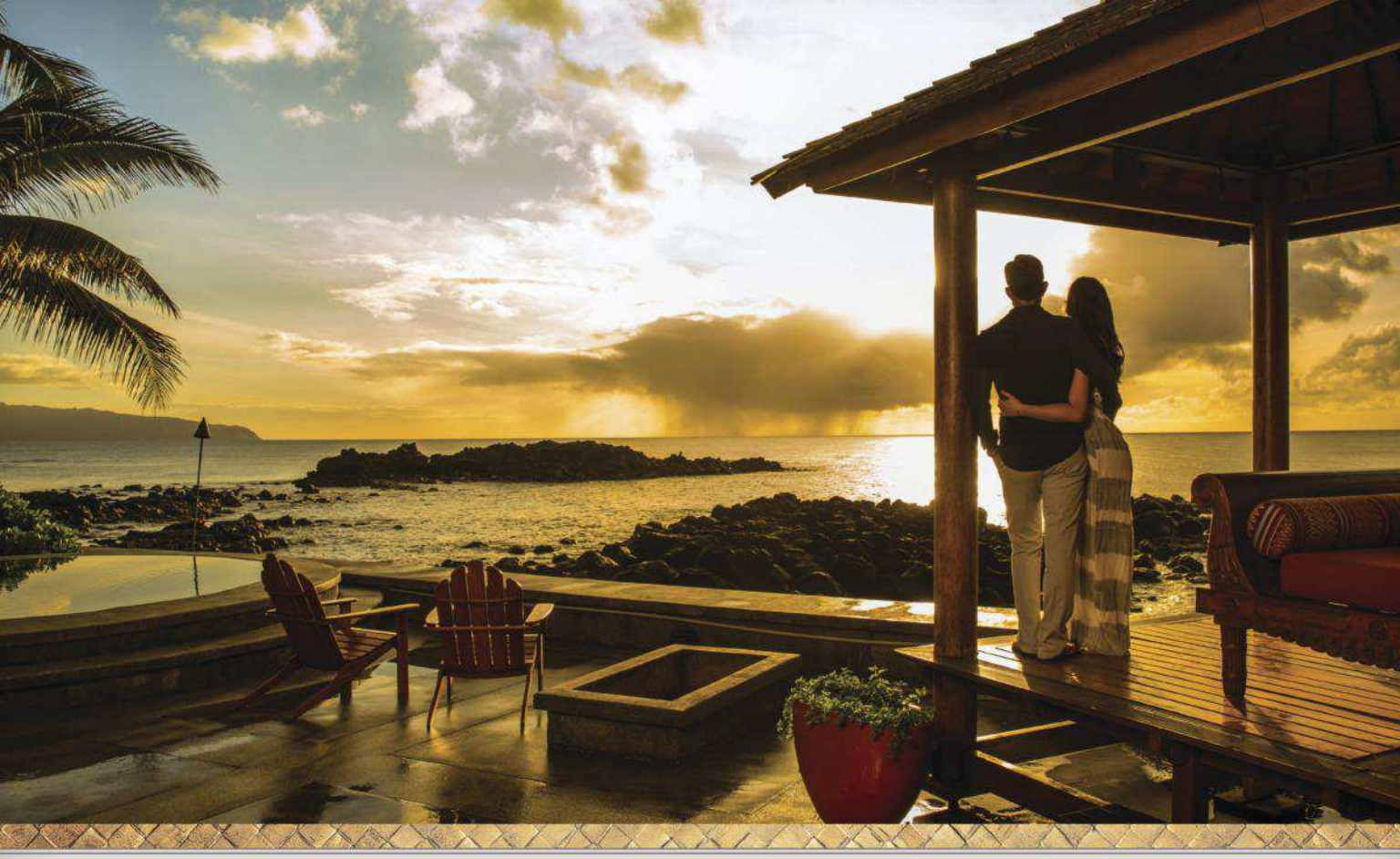
DISCLAIMER: ALL #WIREDBACKPAGE SUBMISSIONS BECOME THE PROPERTY OF WIRED. SUBMISSIONS WILL NOT BE ACKNOWLEDGED OR RETURNED. SUBMISSIONS AND ANY OTHER MATERIALS, INCLUDING YOUR NAME OR SOCIAL MEDIA HANDLE, MAY BE PUBLISHED, ILLUSTRATED, EDITED, OR OTHERWISE USED IN ANY MEDIUM. SUBMISSIONS MUST BE ORIGINAL AND NOT VIOLATE THE RIGHTS OF ANY OTHER PERSON OR ENTITY.


armanibeauty.com
GIORGIO ARMANI



SEPHORA
AND SEPHORA.COM


SEPHORA AND
SEPHORA.COM
ACQUA DI
GIÒ
GIORGIO ARMANI
ABSOLU
THE NEW SENSUALITY



Maui Jim®

Available in prescription.

STYLE SHOWN: CLIFF HOUSE

The view's better from here.

Our lightweight **PolarizedPlus2®** lenses are as flexible as you are, adapting to different light conditions while eliminating glare and enhancing color. Try on a pair and see for yourself. **Color. Clarity. Detail.**

©2018 Maui Jim, Inc.