

NEVER PEDESTRIAN

harrysoflondon.com

480 Stores Customers Love Most

11.01.2019

Newsweek

CAN YOU TRUST YOUR TOASTER?

We are surrounded by billions of devices connected day and night to the internet



$8.99
44
0 733616 4
08321

ORLANE

PARIS

EXTRAORDINAIRE.
YOUTH IS BACK.



firmer skin
97%

wrinkles fade
88%

moisturized skin
97%

radiant skin
97%

* Results from self-evaluation tests on 40 women after 28 days.

PATENTED

Available at neimanmarcus.com and bergdorfgoodman.com

Newsweek

NOVEMBER 01, 2019 _ VOL.173 _ NO.13



FEATURES

SMILE!
In a world of limitless options, sometimes it can feel impossible to find a company that does two simple things: helps you and makes you happy.

COVER CREDIT
Illustration by **Britt Spencer** for *Newsweek*;
Toaster by Ballyscanlon/Getty;
Toast by Jeffrey Coolidge/Getty

For more headlines, go to
NEWSWEEK.COM

ROOTSTOCKS/GETTY

16

Guess Who's Listening

We're surrounded by devices connected to the internet. Most of them are easy to hack.

BY ADAM PIORE

28

America's Best Customer Service

Ready, set shop! We've rounded up nearly 500 stores that consumers love most.

Newsweek

NOVEMBER 01, 2019 _ VOL.173 _ NO.13

DEPARTMENTS

In Focus

06 **London**
The Queen's Speech

08 **Beirut**
A Close Call

Vienna
Broken Record

Port-au-Prince, Haiti
Cry From the Heart



PUPPET MASTERS
From the very first season of *Sesame Street* in 1969, children have loved learning and laughing along with Big Bird, Bert and Ernie.

Periscope

10 **Manmade Viruses: The Next Terrorist Threat?**
The Dark Side of Synthetic Biology

13 **Talking Points**
Kathryn Morgan, Trevor Noah and Ronan Farrow

Horizons

42 **By The Numbers**
Sesame Street

Culture

44 **Taking on Political Correctness 101**
Meghan Daum's New Book

48 **Parting Shot**
Willem Dafoe

P.10

NEWSWEEK (ISSN0028-9604) is published weekly except one week in January, February, March, April, May, June, July, August, September, October, November and December due to combined issues. Newsweek is published by Newsweek LLC, 33 Whitehall St., 8th Floor, New York, NY 10004. Periodical postage is paid at New York, NY and additional mailing offices. **POSTMASTER:** Send change of address to Newsweek, 33 Whitehall St., 8th Floor, New York, NY 10004. For Article Reprints, Permissions and Licensing **NewsweekReprints.com** PARS International (212) 221-9595 x210 **Newsweek@parsintl.com**

GLOBAL EDITOR-IN-CHIEF _ **Nancy Cooper**
CREATIVE DIRECTOR _ **Michael Goesele**
EDITORIAL DIRECTOR _ **Hank Gilman**
DIGITAL DIRECTOR _ **Laura Davis**
US NEWS DIRECTOR _ **Juliana Pignataro**
MANAGING EDITOR _ **Melissa Jewsbury**
SPECIAL PROJECTS EDITOR _ **Fred Guterl**
EDITOR AT LARGE _ **Diane Harris**

EDITORIAL

Senior Editors _ **Peter Carbonara, Meredith Wolf Schizer, Tara Francis Chan**
Deputy Editor _ **Christopher Groux** (Gaming)
Associate Editors _ **James Etherington-Smith, Hannah Osborne** (Science), **Dom Passantino, Harriet Sinclair** (Politics)
London Sub-Editor _ **Hannah Partos**
Copy Chief _ **Elizabeth Rhodes Ernst**
Contributing Editor, Opinion _ **Lee Habeeb**
Editorial Assistant _ **Emmy Espinal**

CREATIVE

Director of Photography _ **Diane Rice**
Contributing Art Director _ **Michael Bessire**
Associate Art Director _ **Paul Naughton**
Digital Imaging Specialist _ **Katy Lyness**
Art Assistant _ **Elizaveta Galkina**

WRITERS

David Brennan, Nina Burleigh, Dan Cancian, Brendan Cole, Shane Croucher, Chantal Da Silva, Sam Earle, Benjamin Fearnow, Kashmira Gander, Ari Georgiou, Nicole Goodkind, Katherine Hignett, Jessica Kwong, James LaPorta, Cristina Maza, Tom O'Connor, Ewan Palmer, Callum Paton, Tom Porter, Bill Powell, Roberto Saviano*, Marc Vargas, Janice Williams, Christina Zhao (**Contributing*)

VIDEO

Video Production Manager _ **Jessica Durham**
London Video News Editor _ **Daniel Orton**
Bangalore Video News Editor _ **Nandini Krishnamoorthy**
Senior Video Producers _ **Sho Murakoshi**
Video Producers - **Chiara Brambilla, Rufaro Ndoro, Frances Rankin, N. Ravichandran, Holly Snelling**
Motion Graphics Producers _ **Simon Vella**

PUBLISHED BY
Newsweek LLC

Chief Executive Officer _ **Dev Pragad**
Chief Content Officer _ **Dayan Candappa**
Chief Operating Officer _ **Alvaro Palacios**
Chief Revenue Officer _ **James Green**
General Manager EMEA / SVP Finance _ **Amit Shah**
Chief Technology Officer _ **Michael Lukac**
General Counsel _ **Rosie Mckimmie**
VP, HR Business Partner _ **Leiann Kaytmaz**
VP Ad Sales, North America _ **Shaun Hekking**
SVP Global Creative Director _ **Robert Lee**
Director, Content Strategy _ **Nalin Kaul**
Deputy News Director + Senior Digital Strategist _ **Adam Silvers**
Global Executive Producer _ **Alfred Joyner**
Global Head of Programmatic + Partnerships _ **Jeremy Makin**
SVP, Product + Business Intelligence _ **Luciano Costa**
Senior Manager, Events + Partnerships _ **Maria Vultaggio**
Senior Sales Director _ **Chantal Mamboury**
Head of Subscription Operations _ **Samantha Rhodes**
Newsstand Manager _ **Kim Sermon**

FROM TOP: PHOTO5963/GETTY; PASIEKA/GETTY; PHOTO5963/GETTY; COURTESY OF SESAME WORKSHOP

★★★★★

“Journalism I don’t see elsewhere until later, if at all.”

NEWSWEEK.COM/TRY













SAVE 79%

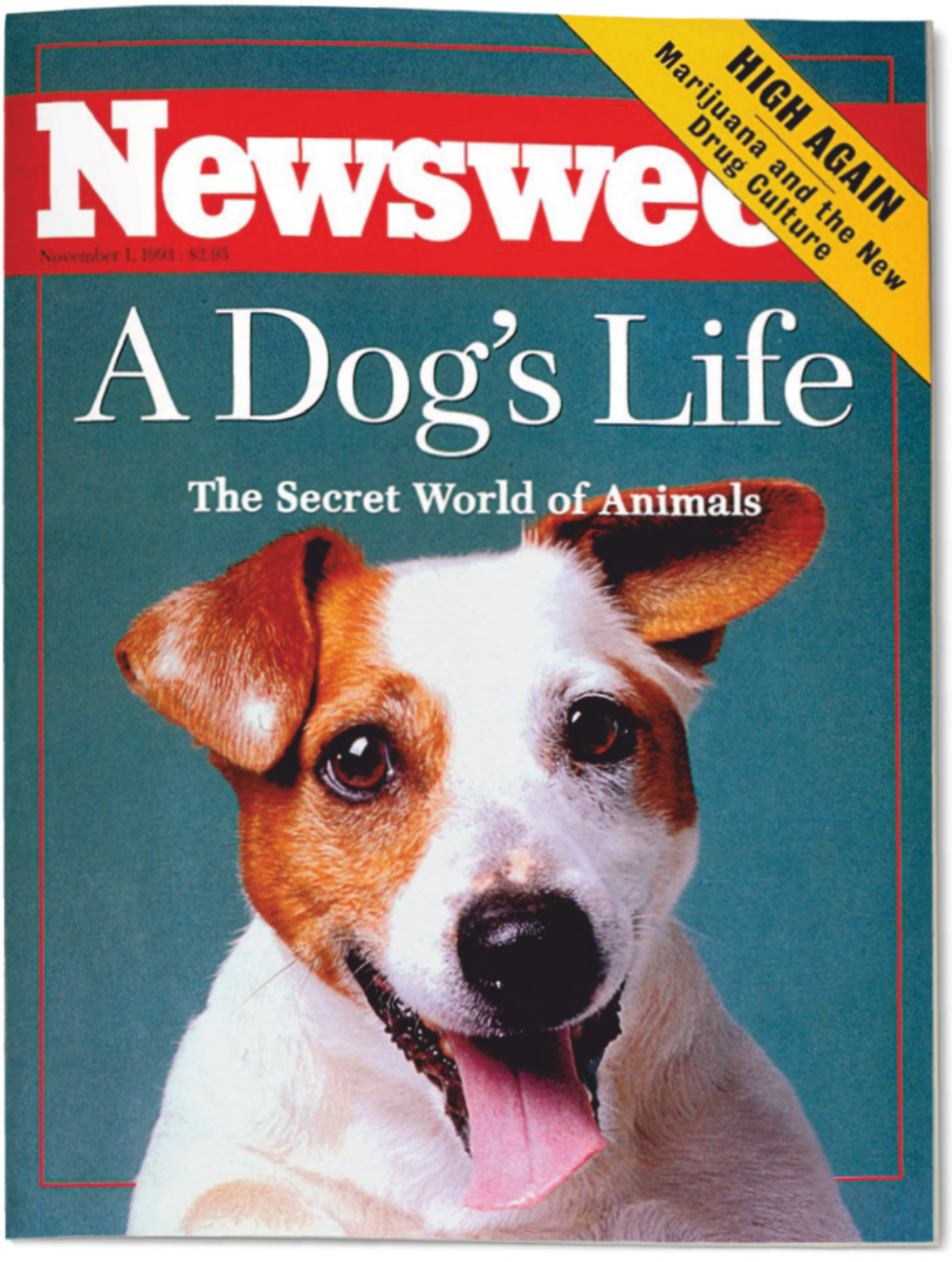
Subscribe

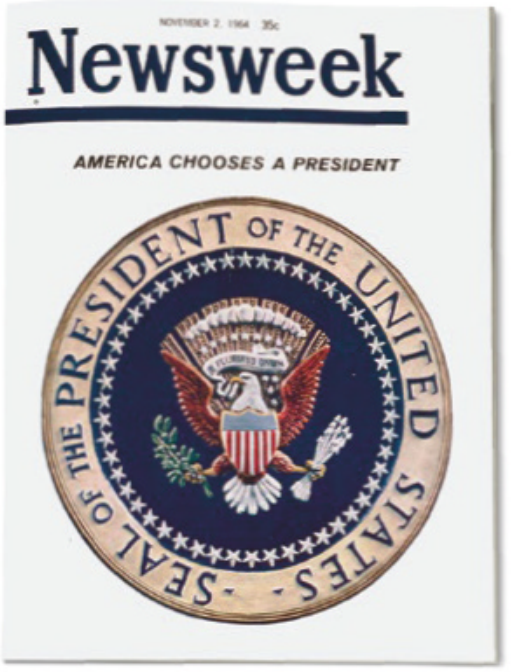
FROM $1.72 PER WEEK

The Archives

1993

"Do dogs lead textured lives full of love, jealousy, passion and fear?" *Newsweek* asked. "According to best-selling author Elizabeth Marshall Thomas, they sure do," For her book, *The Hidden Life of Dogs*. Thomas rigorously studied her 11 dogs for three decades. *Newsweek* said the book boasted "a remarkable level of intimacy for a work of science." and provided significant insight into "the secret world of animals"—they "fall in love, get married, and live in complex societies." Their lives are "rich in intellectual pursuits, packed with emotion." This in mind, we can all feel better about a dog's unbridled joy.





1964

Newsweek reported on the "consensus that President Lyndon B. Johnson and the Democrats were poised for a landslide victory" over Barry Goldwater. After "the most bizarre and apparently lopsided presidential campaign in U.S. history," Johnson's win propelled him into his highly controversial presidency.



2004

"The shortage has put millions into a panic," *Newsweek* reported after a plant shut down, shrinking the U.S flu vaccine supply by nearly half. While "spotty supply is the immediate problem, caring for our country's public health is the bigger issue." It still is. Disjointed manufacturing processes have left millions short of vaccines this year.

CLOCKWISE FROM LEFT: HOWARD BERMAN; FRED WARD/BLACK STAR; CRAIG CUTLER

FOR ALL THE MOMENTS WE STAND UP

Since 2008, *Major League Baseball*® has supported Stand Up To Cancer in its mission to fund groundbreaking research and get treatments to patients faster than ever before. Join us as we stand united to show our support for loved ones affected by cancer.

Visit **StandUpToCancer.org/MLB**



CANDICE PATTON
Stand Up To Cancer Ambassador

STAND UP TO CANCER®

Stand Up To Cancer is a division of the Entertainment Industry Foundation (EIF), a 501(c)(3) charitable organization.

Major League Baseball trademarks and copyrights are used with permission of Major League Baseball. Visit MLB.com

Photo By
ANDREW ECCLES

In Focus _ THE NEWS IN PICTURES





LONDON

The Queen's Speech

Queen Elizabeth II sits alongside Prince Charles at the State Opening of Parliament on October 14. In her speech, which covered the government's agenda for the coming year, the queen touched on Brexit and the bond between the four nations that make up the United Kingdom. She also mentioned climate change and how the U.K. will continue to "play a leading role in global affairs."

TOBY MELVILLE

TOBY MELVILLE/AFP/GE



BEIRUT

A Close Call

A demonstrator walks past burning tires during protests on October 17 against Lebanon's plan to tax calls made on WhatsApp, FaceTime and other apps. Hours later the government reversed course on the 20 cent daily fee. But in the midst of an economic crisis with the government declaring a state of "economic emergency" and public debts totaling 150 percent of gross domestic product, uncertainty remains.

→ ANWAR AMRO

VIENNA

Broken Record

Kenya's Eliud Kipchoge crosses the finish line on October 12 to become the first person to break the two-hour barrier for a marathon-distance run—a feat he compared to reaching the moon. The run, which was not an official marathon, was perfectly engineered and included a pace-setting laser projected from a car that was followed by pacesetters running in an aerodynamic "V" formation. Kipchoge's final time was 1hr 59min 40.2sec.

→ ALEX HALADA

PORT-AU-PRINCE, HAITI

Cry From the Heart

A girl cries during her father's funeral on October 16. The city has been paralyzed by anti-corruption protests for more than six weeks with mounting calls for President Jovenel Moise to resign. Tens of thousands of people have flooded the streets and 18 people have died in violent clashes. On top of a fuel shortage, Haitians are also struggling with a lack of access to safe water and food. Half of the country's population lives below the poverty line.

→ CHANDAN KHANNA







CLOCKWISE FROM LEFT: ANWAR AMRO/AFP/GETTY; ALEX HALADA/AFP/GETTY; CHANDAN KHANNA/AFP/GETTY



SCIENCE

Are Manmade Viruses the Next Big Terrorist Threat?

There's a dark side to the promise of synthetic biology, says a leading futurist who is sounding an alarm over its potential use to create weapons of mass destruction



TIM BIRD/GETTY; TOP RIGHT: RICHIE DOWNS/MSNBC/NBCU PHOTO BANK/NBCUNIVERSAL/GETTY

"I don't need lessons from you on courage." »P.13



A DEVASTATING STRING OF MASS SHOOTINGS HAS left the country reeling this year. But an even greater threat may be looming in the near future, one with the potential to cause far more widespread injury and loss of life: synthetically modified diseases designed to infect human beings on a global scale.

That's the danger that best-selling author and futurist Rob Reid predicts could arise from the field of synthetic biology, which combines biology and engineering to create artificial biological systems, from genetically-modified crops to custom viruses.

Synthetic biologists have been modifying the DNA of pathogens with alarming speed and efficacy over the last decade, Reid notes, opening up a new frontier in virology, public health and global security. "I'm a big SynBio fan," says Reid, who believes in the promising applications of DNA modification, such as solutions for climate change and breakthroughs in life extension. "But there's a dark side to it."

In the wrong hands, he warns, this technology could create a weapon with the potential to inflict catastrophic damage on an unprecedented scale. And unlike recent acts of localized terror, such as the 2014 downing of Malaysia Airlines Flight 370 and this summer's shooting at a local Walmart in El Paso—events that killed or injured dozens or hundreds of victims at a time—a synthetic biological agent has the potential to travel around the world, putting billions of people at serious risk.

A PROLIFERATING THREAT

Reid's prediction, laid out in a TED talk earlier this year, isn't just the stuff of speculative sci-fi. Synthetic biology has already waded into impressive—and controversial—territory.

In 2011, for instance, virologists in both Holland and Wisconsin successfully altered the DNA of the deadly H5N1 virus (commonly known as "bird flu") to make the naturally-occurring virus, which under normal conditions isn't easily spread from person to person, more transmissible. Their goal was to proactively study an extreme version of the virus, in case one emerged from nature organically in the future. At the time, microbial geneticist Paul Keim, then chair of the U.S. National Science Advisory Board for Biosecurity, said, "I can't think of another pathogenic organism that is as scary as this one."

Since then, the development of a game-changing power tool for DNA editing called CRISPR makes it possible to carry out this kind of gene modification more easily, and far more cheaply, by hundreds of people, with less oversight than a well-regulated laboratory. "Radically powerful editing that the entire field of biology would have found impossible 10 years ago can now be done by a couple smart grad students" in a tiny room, Reid says.

And the technology is proliferating in a way that even nuclear weapons haven't, Reid adds—with more decentralization and far less oversight.

Now consider the form of these technological breakthroughs. The genome for a flu virus is roughly 10,000 letters long, a sequence that could fit on a handful of pages. The code the Dutch scientists developed for their beefed-up H5N1 virus is even smaller than that—and could fit on a Post-it Note.

The nightmare scenario that Reid envisions goes something like this:

In the next few years, an ambitious virologist uses widely-available gene-editing technology to create a supervirus—a pathogen 10 times as contagious as chicken pox and 10 times as deadly as the Ebola virus, but with an incubation period of, say, 10 months. Based on that programming, the entire world could be infected with the designer virus before the first person even shows symptoms.

Then, a hacker gains access to the scientist's computer and steals the genetic code. This lethal smidgen of data—a blueprint for a biological weapon—ends up floating around the internet, being swapped on torrent sites (a form of peer-to-peer file transfers) or sold on the dark web. Eventually, it could wind up in the hands of a rogue state, malicious actor or biological terrorist, who might use that code to manufacture a pathogen that could infect millions of people—in effect, turning our own bodies into tools for mass terror.

As of now, successfully manufac-

BY

JORDAN HARBINGER

@JordanHarbinger

turing a virus based on that code would be difficult. But, as Reid points out, it's only a matter of time—perhaps 10 or 20 years—before DNA synthesizers become widespread in college and even high school biolabs, allowing virtually anyone to weaponize these blueprints.

"WHOLESALE MILITARIZATION"

The implications of these risks, scientists and experts say, are massive and urgent.

The creation of highly contagious viruses has left the world vulnerable to "the hostile misuse of the life sciences," argued researchers at the Disarmament Research Centre at the University of Bradford in West Yorkshire, England in an article published on the U.S. National Institutes of Health's National Center for Biotechnology Information website. The worst case scenario, according to the researchers: the "wholesale militarization of the life sciences."

That militarization seems more likely now than ever, according to Reid. As he points out, the U.S. is already struggling to keep up with staggering breaches of cybersecurity, such as the theft by Chinese hackers of technical documents related to the Lockheed Martin F-35 aircraft program.

"If the United States military couldn't keep the plans of its F-35 program a secret," asks Reid, "then how in the world is a grad student, who can very easily create a pathogen for a homework assignment, going to keep all bad actors from getting access to this stuff?"

Top U.S. officials have confirmed that the intersection of cyber-espionage and synthetic biology creates an unprecedented risk.

"Cyber threats pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors," noted Dan Coats, then director of national intelligence, in testimony before the Senate Select Committee on Intelligence in 2017.

"The first person to do something awful with synthetic biology might not even be born yet."

The threats, added Coats, who left the position in August, will only magnify as the country continues to rely on "potentially vulnerable automated systems"—technology that "increases the likely physical, economic, and psychological consequences of cyber attack and exploitation events."

PREVENTING DISASTER

What synthetic biology experts are now asking is: What can we do to prevent this kind of doomsday scenario from happening?

One option is to ban synthetic biology altogether.

But, as Reid points out, an outright ban would be highly difficult, given that people can create pathogens in a lab the size of an RV, just as illicit drug manufacturers do today. Abandoning the field would also allow states like Russia, China, or North Korea to pursue the technology unchallenged, with potentially nefarious applications.

Instead, Reid suggests, we need to engineer a situation in which humanity enjoys the massive upsides of synthetic biology while avoiding cataclysmic destruction.

Two initiatives, he says, would help protect against that outcome.

The first is a massively distributed pathogen detector network—a system that would sequence the fragments of DNA cycling through our air and alert us to dangerous pathogens in the atmosphere on an ongoing basis.

If the U.S. devoted federal funding to a program like this, it could make sophisticated pathogen detectors as ubiquitous as smart phones are today over the coming decades. The program would pay for itself simply in the early detection of the common flu virus, Reid says.

The second approach is a disruptive extension to our country's biomanufacturing infrastructure.

In the event that a rogue actor releases a dangerous pathogen, scientists won't have months to study the virus, develop a vaccine and ship it to various cities from a handful of centralized locations, as they do today. Instead, Reid recommends that we adopt 3D printing technology to manufacture vaccines in pharmacies and doctor's offices, creating tens of thousands of distribution points around the country. This model would get vaccines into patients' hands much more rapidly, potentially saving countless lives.

To capitalize on these solutions, we have to begin investing in them now, Reid warns—before a synthetic supervirus arrives in the next 15 to 20 years.

"The Columbine kid isn't going to release this deadly pathogen tomorrow," Reid says. "The first person to do something awful with synthetic biology—and there *will* be such a person someday—might not even be born yet."

In other words, time is still on our side—for now.

→ **Jordan Harbinger** *is the host of The Jordan Harbinger Show, where he deconstructs the playbooks of the world's most successful authors, entrepreneurs and artists. A recent episode featured an interview with Rob Reid.*

Talking Points

CNN

"I don't need lessons from you on courage, political or personal."

—SOUTH BEND, INDIANA, MAYOR PETE BUTTIGIEG TO BETO O'ROURKE

EW

"POWERFUL INTERESTS SAYING THEY ARE GOING TO WIPE YOU OUT IS NOT A FUN EXPERIENCE."

—AUTHOR RONAN FARROW



Ronan Farrow

"I earned my spurs on the battlefield. Donald Trump earned his spurs in a letter from a doctor."

—FORMER DEFENSE SECRETARY JAMES MATTIS AT ALFRED E. SMITH MEMORIAL FOUNDATION DINNER

"If you would have told me then that I would be where I am now, I would have said you were insane. I would never have dreamt how much I could have accomplished."

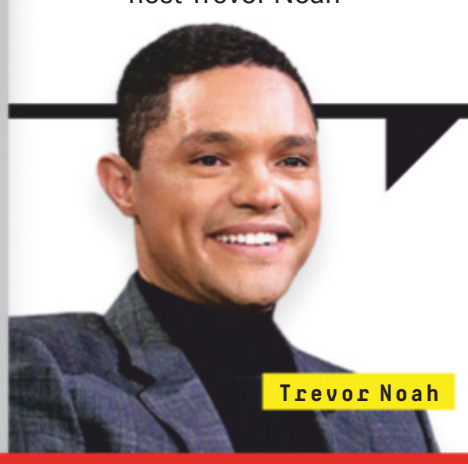
—MIAMI CITY BALLET SOLOIST KATHRYN MORGAN



Kathryn Morgan

"WE NEED TRUMP ON TWITTER. IT'S THE ONLY WAY WE CAN MONITOR WHAT HE'S UP TO!"

—The Daily Show host Trevor Noah



Trevor Noah

"They've got a lot of sand over there... There's a lot of sand they can play with."

—PRESIDENT DONALD TRUMP ON KURDS IN SYRIA

abc

"WAS IT POOR JUDGMENT TO BE IN THE MIDDLE OF SOMETHING THAT IS A SWAMP IN MANY WAYS? YEAH."

—Hunter Biden

FROM LEFT: PAULA LOBO/ABC/GETTY; JARED SISKIN/PATRICK MCMULLAN/GETTY; ANDREW LIPOVSKY/NBCUNIVERSAL/GETTY

CHINA AND THE WORLD

A new white paper makes clear China's relationship with the rest of the world in the new era



Chinese UN peacekeepers take part in a military parade in Beijing on October 1, as part of the celebrations of the 70th anniversary of the founding of the People's Republic of China XINHUA

A common consensus in the world today is that China's development is linked to the change in the international structure and will have a profound and far-reaching influence on the world order. In many people's eyes, China has already become a superpower, second only to the U.S., and is having growing impact on the world.

In this context, a white paper titled "China and the World in the New Era," published by the State Council Information Office on September 27, ahead of the grand celebrations marking the 70th anniversary of the founding of the People's Republic of China (PRC) on October 1, makes clear what role the country wants to play in the world and what it expects from the rest of the world.

Xu Lin, deputy head of the Publicity Department of the Communist Party of China (CPC) Central Committee and minister of the State Council Information Office, said the white paper systematically introduces China's development achievement, path and direction and details the relations between China and the rest of the world to help the international community better understand China's development.

Responding to Misunderstandings

Particularly in recent years, as China's national strength has grown rapidly and its way of dealing with international affairs has become more active, a sense of fear has grown in some countries, both big and small. Some are afraid that China may become a regional or even global dominant force, pressuring other countries to follow its model, rules and standards.

Over more than a year, the trade friction between China and the U.S. has spilled over to other sectors, and the two countries' relations are becoming more complicated. The international community has growing worries that the "trade and technology wars" and the possible economic "decoupling" between the world's two largest economies will disrupt the global supply chain or even the whole global system.

China has continually responded to these fears by publicizing its policies on bilateral and multilateral occasions. There are also an increasing number of Chinese officials, experts and scholars who express China's stand through international media outlets. However, misunderstandings continue to grow, and China still has a lot to do to increase mutual trust and clear doubts.

This is not the first time China has published a white paper on its relations with the world. "China's Peaceful Development Road," published on December 22, 2005, stressed that peaceful development is the inevitable path to China's modernization, and it will make more contributions to the lofty cause of peace and development of humanity.

On September 6, 2011, "China's Peaceful Development"



By An Gang

The author is an op-ed contributor to *Beijing Review* and a researcher with the Pangoal Institution

was published, which pointed out that China has broken away from the traditional pattern where a rising power was bound to seek hegemony, demonstrating instead that peaceful development is China's new development path as the largest developing country in the world. The highlight of the white paper was that it defined China's core interests, which include state sovereignty, national security, territorial integrity and national reunification; China's political system established by its Constitution and overall social stability; and the basic safeguards for ensuring sustainable economic and social development.

The latest white paper explains an already strong China's promise to the world and its stance in a more confident and constructive manner. It reflects China's willingness to promote reform of the current global system and international order.

A New Reality

In the new era, the guideline for dealing with the relations between China and the rest of the world is "Xi Jinping Thought on Diplomacy," which was developed from inheriting the excellent traditions of Chinese civilization, absorbing the experiences of China's diplomatic initiatives since the founding of the PRC and studying the development trends of the contemporary world and the opportunities and challenges China has faced.

Based on the vision of a community with a shared future for humanity, "Xi Jinping Thought on Diplomacy" is underpinned by multiple concepts such as a new model of international relations, a new model of economic globalization and a new type of partnership. It also highlights the principle of extensive consultation, joint contribution and shared benefits, and a new security concept featuring mutual trust, mutual benefit, equality and coordination. It provides new-type international public goods such as the Belt and Road Initiative and the Asian Infrastructure Investment Bank. Its aim is to safeguard the international system centered around the United Nations, improve global governance through reform rather than reinventing the wheel, and build a more fair and reasonable international order.

On the same day the white paper was published, Chinese State Councilor and Foreign Minister Wang Yi spoke at the annual general debate of the U.N. General Assembly, where he said over the past 70 years since the founding of the PRC, China has constantly integrated with and made contributions to the world. Entering the new era, the Chinese people are more confident in and capable of realizing national renewal and are more prepared to make contributions to humanity than at any other time in history.

China will prove to the world through its engagement in peaceful development and global governance that it will not find its place in the world through power transfer, hegemony, competition or geopolitical expansion.

Comments to yanwei@bjreview.com

HIGHLIGHTS OF THE WHITE PAPER

China Has Found a Development Path Suited to Its Actual Conditions

China has made tremendous achievements over the past 70 years since the founding of the People's Republic of China. Its successes have been achieved through the hard work of generations of Chinese people under the leadership of the Communist Party of China. Also, China is developing through interaction with the world.

China's Development Is an Opportunity for the World

The causes of the "China threat" theory include cognitive misunderstanding, deep-rooted prejudice, a psychological imbalance brought about by the prospect of falling power and deliberate distortions by vested interests. China's pursuit of peaceful development is not diplomatic rhetoric, an act of expediency or a strategic ambiguity. Rather, it showcases China's confidence in theory and readiness for practice, and represents China's unswerving strategic choice and solemn commitment. China will never pursue hegemony or expansion, nor will it seek to create spheres of influence no matter how the international situation changes or how China develops.

It is both unrealistic and harmful to regard China's economic development as a "threat" or a "challenge" and try to squeeze China out of the globval industrial chain, supply chain and value chain so as to "detach" China from the world economy.

A Prosperous and Beautiful World Is the Common Aspiration of All Peoples

The world is undergoing the greatest changes in a century, and one of the most notable changes is that the rise of China and other emerging markets and developing countries is fundamentally altering the international structures of power. China's proposal to build a global community with a shared future pursues the goal of universal harmony and the principles of cooperation and mutual benefit, while opposing the law of the jungle, power politics and hegemonism. Meanwhile, it looks beyond zero-sum games to the idea of blazing a new path of development based on win-win cooperation, joint contribution and shared benefits, and offering a new option to the international community.

China Contributes to a Better World

China will do well only when the world does well, and vice versa. The country will continue to forge ahead on its socialist path. Seeking a better life for the Chinese people has always been China's primary goal. China believes that the global trend toward multipolarity and democratic international relations is irresistible, and it hopes the world will uphold multilateralism, ensure equity and justice and turn the proposals for the transformation of the global governance system into consensus and concerted actions.

As for China-U.S. relations, cooperation is the only correct choice for the two countries. The U.S. should treat bilateral relations from a broad and rational perspective. China has no intention of challenging the U.S. or replacing it. The U.S. will be unable to force China's hand, and even less likely to halt China's development. China is ready to work with the U.S. to jointly advance China-U.S. relations focusing on coordination, cooperation and stability.



BY
Adam Piore

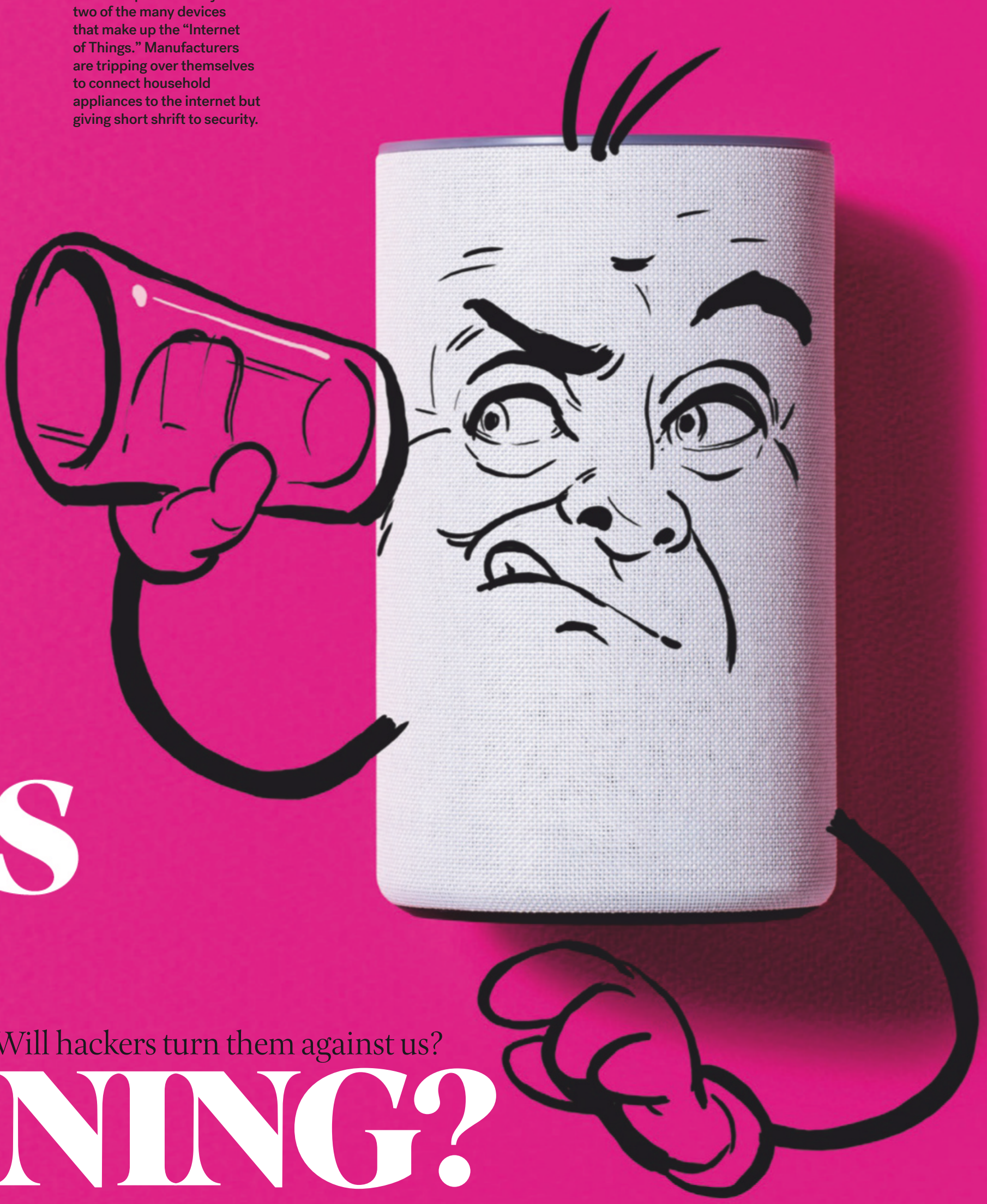
Illustrations by
BRITT SPENCER

Photographs by
YAGI STUDIO

GUES WHO'S LISTE

Billions of devices are now connected to the internet.

HOUSEHOLD SPY
Smartphones and WiFi-enabled speakers are just two of the many devices that make up the "Internet of Things." Manufacturers are tripping over themselves to connect household appliances to the internet but giving short shrift to security.



S

Will hackers turn them against us?

NING?

In 2009, just as consumers had begun to buy wifi-enabled thermostats and front-door cams and other early devices that now make up the "Internet of Things," computer scientist Ang Cui had gotten the idea to scan the Web for "trivially vulnerable" embedded devices.

By trivial, he meant those devices that still carried the usernames and passcodes programmed into them at the factory—obvious usernames like "name" and passcodes like "1234." Many of these codes were published in manuals available freely on the internet and easily scanned automatically with computer programs, so there was no need even to guess.

When he did his scan, Cui found more than one million vulnerable, publicly accessible devices in 144 countries. From this sample, he estimated that about 13 percent of all devices connected to the internet were essentially unlocked doors, waiting for a hacker to walk through. Even more alarming, four months later 96 percent of those devices had the same security holes.

Cui's warning was no less terrifying for its deadpan delivery: "Widely deployed and often misconfigured, embedded network devices constitute highly attractive targets for exploitation."

In the decade since, the number of vulnerable devices connected to the internet has increased sevenfold. The explosion comes from growing demand, fueled by hype, for smart devices. Manufacturers are now tripping over themselves to embed just about every ordinary object, it seems, with tiny computers that happily communicate wirelessly with the world around them. In this "smart" revolution, virtually any device with an on/off switch or up/down button can be controlled remotely with a cellphone or voice sensor. Do you want to turn up the heat, dim the lights and run the dryer without getting up off the sofa—simply by uttering your desire to an Amazon Echo? Do you want your toaster to send a message to the television when the bagel has popped? Do you want your oven to inform you that the casserole has cooked for the prescribed 20 minutes at 350 degrees and is now cooling in the kitchen at 200? The Internet of Things can make all such things happen.

There's a dark side to this wireless-driven revolution in convenience. The danger goes beyond hacking. Unlike the traditional "Internet of Computers," which is confined to a circumscribed digital "virtual" world, the Internet of Things has a direct connection to the physical one. That opens up a disturbing set of questions: What might happen if the computers inside our new-fangled toaster ovens, security cameras or smart cities were turned against us? Can we really trust the Internet of Things? Most cybersecurity experts are unequivocal in their answer to that last question. "No," says Ben Levine, senior director, product management, cryptography at Rambus, a Sunnyvale-based technology company, specializing in the performance and protection of data. "My short answer, right now, is 'no'."

Unlike the "Internet of Computers," which has been created largely by technicians with a background in information technology or computer science, many manufacturers making the devices now lack the expertise necessary to build airtight systems. Some don't realize the importance of doing so. As a result, the possibilities for mischief seem endless—a fact Cui and other cybersecurity mavens have demonstrated on multiple occasions.

UNLOCKED WINDOWS

An estimated 13 percent of all devices connected to the internet still have factory-default passwords, making them vulnerable to hackers. Clockwise from right: Google's Nest thermostat; computer science professor Alvaro Cardenas; a laptop and other WiFi-enabled devices.

CLOCKWISE FROM LEFT: NEIL GODWIN/FUTURE PUBLISHING/GETTY; JOSEPH BRANSTON/T3 MAGAZINE/FUTURE/GETTY; RANDY ANDERSON; PREVIOUS SPREAD: YAGI STUDIO/GETTY







Is your vibrator cheating on you?

SOME OF THE MORE CREATIVE OF THESE EXPLOITS in recent months come from the lab of Alvaro Cardenas, who challenged his students at the University of Texas at Dallas last year to crack a wide array of IoT devices. Among other things, they managed to turn on and hijack a drone and demonstrate they could use it to attack an innocent victim, Kamikaze-style, or to stream video and audio of a neighbor. They hacked into a popular children's toy—a small, talking dinosaur networked to the internet so it could receive updates. Then they demonstrated they could take over the toy and use it to insult the child, instigate inappropriate conversations (using the trusted voice of the toy) or tell the child what to do. They showed they could take control of internet-connected cameras to spy on households. They even identified the existence of "sensitive devices"—vibrators—sometimes used by overseas military personnel to have remote virtual relations with their partners. Not only were they able to obtain private usage information, they warned it was possible to impersonate a "trusted partner" and "commit remote sexual assault."

"The problem at the moment is that there's really no incentive for security. **SECURITY** usually gets in the back burner of these products."



Cardenas reported their findings to device manufacturers and the CERT Coordination Center, a federally funded non-profit R & D group that works with business and government to improve the security of the internet. Then he submitted a paper to IEEE, a professional association for electronic engineering and electrical engineering, which published their findings in a special issue this fall.

"These attacks show how IoT technologies are challenging our cultural assumptions about security and privacy and will hopefully motivate more emphasis on the security and privacy practices of IoT developers and designers," they wrote. (After the paper was published, all the manufacturers responded and attempted to fix the vulnerabilities, except for the drone companies).

& WAYS TO PROTECT YOUR HOME FROM HACKERS

by Kimberly Burke



NOTHING IS 100 percent secure. That's especially true for homes chock full of devices chirping away day and night on the internet. But there are simple steps to minimize the risk of hackers turning homes into surveillance fish-bowls or recruiting appliances for zombie bot armies. It starts with self-awareness: the number one cause of security breaches is human error, usually when someone clicks a malicious link that allows unauthorized access or loads malicious software. Here's what you can do to minimize the risk:

→ **Don't buy unsecured devices.** Sometimes the cool factor can cloud your decision-making. Do your research before you make a purchase. Are there known vulnerabilities with the device that can expose your home network?

→ **Harden your home WiFi router.** Set up a unique username and password. Update the router consistently. Close open ports that are not being used and enable the router's firewall and the devices' firewalls.

→ **Take an inventory** of all your connected devices and associated MAC and IP addresses and write them all down. That way, you can easily identify and remove them from the network in the event one of your devices is breached. If you create a file for this on your computer, make sure you keep it password protected.

→ **Keep your smart home devices separate** from your regular home network by setting up a separate guest network to connect them to.

→ **Check all connected devices** for factory-installed username and passwords. Change them to unique combinations and if they can't be updated, swap them out for a more securable version.

→ **Update all firmware and software** for all devices on a consistent basis. Manufacturers often include "fixes" for vulnerabilities.

→ **Review the settings** on all your connected devices for privacy and data sharing. Are they sharing data with a third party? Do they need to be providing your utility company (or whomever) a constant stream of your data? If not, then turn it off.

→ **Do not click** on any update links provided to you via email from any of the manufacturers. Instead, go to the manufacturer's website and download the update directly. N

KIMBERLY BURKE *is chief operating officer of TecKnow, a firm in Westport, Connecticut that specializes in smart-device home networks.*

Force multiplier

BY THE END OF 2018, MORE THAN 23 BILLION IOT devices had been installed globally. Many consumers buying these smart devices currently don't bother to hook them up to their WiFi, which means they're essentially offline and out of reach of hackers. But that may change as manufacturers continue to tout the benefits of connectivity. And the number of devices is expected to more than triple, to 75 billion, by 2025.

The sheer number of vulnerable devices gives hackers powerful leverage. The Mirai attack of 2016, which may have been inspired by Cui's original paper, illustrates how dangerous the threat has grown. Paras Jha, a quiet, socially awkward college dropout from New Jersey, ran a lucrative business renting space on his own private computer server to fellow aficionados of the video-game Minecraft, so they could play privately with their friends. It sounds pleasant, but the business is cutthroat. A common tactic of Jha and his rivals was to hack into the home computers of unsuspecting people,





"But there's a lot of **VC MONEY**, and they want to very quickly roll out a thing that has an IoT feature that they think the market might like."

FROM LEFT: PHILIPPE HUGUEN/AFP/GETTY; GEORG WENDT/PICTURE ALLIANCE/GETTY

ZOMBIE ARMY
The Mirai attack of 2016 showed how vulnerable the Internet of Things can be to hacking. It started as a Distributed Denial of Service attack on small-time servers used for playing the video game Minecraft (above), and escalated to an attack on OVH, a big French internet company (left). By some estimates, hackers managed to build an army of 600,000 zombie devices.

hijack them with malware and instruct them to send torrents of unwanted messages and data to the machines of their rivals, overwhelming them and hopefully shutting them down—known as a Distributed Denial of Service Attack (DDoS). Unsuspecting customers, frustrated by the "unreliable" service, were then easy targets for poaching.

In 2016, Jha and two Minecraft friends he'd met online decided to do his rivals one better. They hacked not only desktop computers but also the myriad security cameras, wireless routers, digital video recorders, household appliances and other IoT devices. Like Cui before him, Jha and his friends wrote a program that scanned the internet to locate vulnerable devices. But unlike Cui, they actually planted malware on the machine and took control of them. Leveraged by the proliferation of smart devices, Jha's zombie bot army grew faster than he could have imagined--by the end of the first day, he had appropriated 65,000 devices; by some estimates his zombie army reached 600,000.

The attack, nicknamed "Mirai" ("the future") after a Japanese television series, was so powerful that Jha wasn't content with taking down his small-fry Minecraft rivals. He also trained the new weapon on the huge French telecom provider OVH, which hosted a popular tool that his rivals relied on to defend themselves against his attacks. Eventually, the cops took notice. Jha was fined $8.6 million and 2,500 hours of community service working for the FBI.

Cui, now the 36-year-old founder and CEO of Red Balloon Security, often gives talks at hacker conferences wearing a tee-shirt, a bead necklace, and a man bun and makes a good living advising companies how to protect themselves in a hostile cyber-world. He continues to marvel at how little has been done to patch not just the vulnerability

his paper identified but also many others that he believes could arguably cause even more damage. While the security firms serving large well-financed companies like those targeted in the Mirai attacks have come up with new ways to defend client servers against DDoS attacks, many manufacturers of IoT devices are doing little if anything to protect the rest of us from cyber mischief—not just zombie device conscription, but also spying, sabotage and exploits that security experts argue should raise profound privacy and safety concerns.

What accounts for the neglect, Cui believes, is a gold-rush mentality to grab market share in the burgeoning IoT device business. Over the last five years, the hype over IoT has become so hot that many VC-funded startups in the consumer-device field—and even some major manufacturers—are adding internet connectivity, rushing their products to market, and resolving to fix any security flaws later. Some haven't even thought about security at all. "You have to put in the time and resources to care about security," says Cui. "But there's a lot of VC money, and they want to very quickly roll out a thing that has an IoT feature that they think the market might like."

The money is primarily spent to develop new devices. "The problem at the moment is that there's really no incentive for security," Cardenas told Newsweek. "Security usually gets in the back burner of these products." Most consumers aren't aware of the dangers and aren't demanding protection. And the device manufacturers are under no obligation to provide it.



"Someone will **LOSE THEIR LIFE** and then eventually they'll kind of knee jerk into fixing the whole industry. I think that's what it will take to change the mentality of car manufacturers."

In a lab at the Georgia Institute of Technology, Manos Antonakakis, an associate professor in the school of electrical and computer engineering, and research scientist Omar Alrawi, have also been probing the gaping security vulnerabilities of the emerging IoT. Antonakakis notes that while there's a class of well-known vendors that "at least try to get the security right in some cases," even large manufacturers are under pressure to rush new IoT products onto the current market. "It takes a lot of quality assurance and testing, and penetration analysis and vulnerability analysis to get it right," he says. But the rush to market "comes into violent disagreements with proven security practices."

Many of the largest tech companies have invested heavily in tapping into the market for "smart home" devices , one of the fastest growing areas for IoT devices. Amazon is among those dominating the market for smart hubs, along with Google, which purchased the digital thermostat maker Nest in 2014 for $3.2 billion. Google has since expanded it to become a digital hub that also includes smoke detectors and security systems like smart doorbells and locks. Samsung

ONLINE BREAK-INS
Hackers could break into one device on a car or in a home and from there gain access to an entire network. Clockwise from right: many toys are now linked to the internet; IoT devices in Jeep Cherokees have been hacked; the Department of Justice indicted seven hackers from Iran in 2016.

CLOCKWISE FROM LEFT: DANIEL ACKER/BLOOMBERG/GETTY; ALEX WONG/GETTY; ROBYN BECK/AFP/GETTY



has the SmartThings hub, which it acquired in 2014 for $200 million, and now connects to air conditioners, washers and TVs. Apple has a home kit which can control any number of devices through voice commands delivered in range of its HomePod.

Gaping vulnerabilities

ONCE THESE SYSTEMS ARE INSTALLED, DEVICES from a growing number of companies can be added to the home network, including those made by well-known home appliance manufacturers like GE, Bosch and Honeywell. Belkin makes a line of connected appliances that includes a Crock-Pot WeMo Smart Slow Cooker, smart Mr. Coffee maker and a smart home humidifier. There's a lot of money to be made. All told by the end of 2019, more than $490 billion in profits will have been earned on the nearly 2 billion consumer devices sold over the previous 12 months, according to the property management consulting firm iProperty Management.

To try to draw attention to the dangers—and the things consumers should be asking questions about when buying new IoT products—Antonakakis and Alrawi, in collaboration with researchers at the





University of North Carolina at Chapel Hill, have developed a rating system and begun evaluating the security of a wide array of IoT devices. And surprisingly they found gaping vulnerabilities in devices and systems produced by even some of the most tech-savvy companies.

The vulnerability of IoT devices goes well beyond holes in password protection, the vulnerability exposed by the Mirai attack, they argue. IoT devices can also be accessed and taken over directly through the home network they are connected to, and that home network is only as strong as its weakest link. That means that even if each device comes with a unique password and username, it's not necessarily secure. Once hackers find a way onto the home network through one vulnerable device, the path is often wide open to the rest of the network.

To secure an IoT device, they argue, manufacturers need to patch vulnerabilities in four different areas : direct access to the device itself, the mobile app used to run it, the way it communicates with its home network and, in many cases, the cloud-based server that manufacturers use to push out updates, collect user data, or provide new services.

Getting all that right is not easy. For a vendor to secure all four parts, Alrawi notes, it needs a good mobile-app developing team "that knows secure development," a "system team that does very good embedded system development and secure development" and cloud experts who can design a secure cloud "backend" that allows the device to be managed without exposing it to additional risk. Finally, the device manufacturers need somebody who has network knowledge on how to build efficient and secure internet protocols and what protocols to avoid.

"They have to balance all this with usability," he says "So you can see that this is already getting really hard to manage just mentally. When a startup team that comes up with this great idea wants to push a product to market, they're usually a small team that doesn't have all this expertise. But even with big vendors, some of these problems are really hard to pin down and manage."

Indeed, while Antonakakis, Alrawi and their team give relatively high marks for device security to the mainstream products like the Amazon Echo and the Belkin Netcam, they gave them Cs, Ds, and Fs for network security—a measure of how protected these devices are from intruders who manage to access the home wireless network through other vulnerable devices. And while a number of devices associated with Google's Nest smart home products (like thermostats, smoke detectors, smart locks and doorbells) receive As and Bs for device and network security, they got Cs and Ds for mobile and cloud protections—meaning a resourceful hacker intent on say, unlocking the front door, could still access a home.

The cloud category is the most worrisome. Since many of these services are cloud based and connected to central company servers, if a determined, well-financed hacker—say, China, North Korea or Russia—were to use the same kind of



AN ABSOLUTE MESS. David Kennedy, CEO of TrustedSec, a consulting firm, told Congress: "We're going into this very blind, without a lot of security discussions around what the impacts are going to be to our lives, and to our safety."

Q&A

OUR PRIVACY NIGHTMARE AND WHAT CAN BE DONE ABOUT IT.

THE INTERNET OF THINGS (IoT) is not just a security problem. It's also a privacy nightmare. Few people in Washington know more about the issue than Marc Rotenberg, a Georgetown Law Professor who serves as president and executive director of the Electronic Privacy Information Center (EPIC). In 1994, he founded the Washington D.C.-based organization to fight to protect individual privacy and civil liberties on the burgeoning computer network. At the time banks and other large commercial interests just beginning to establish an online presence. Today there's a lot more to worry about. Newsweek's Adam Piore spoke with Rotenberg about what the emerging world of networked devices means for our privacy -- and what protections, if any, exist to protect it. Edited excerpts:

Q Big Tech already collects a lot of data on their customers. What's to stop IoT manufacturers from collecting even more?
A In the absence of a privacy law, like the GDPR in Europe, American consumers who have purchased devices, door locks and thermostats are basically allowing these companies to collect and use their personal data.

Q Should we be concerned?
A It's been very interesting to watch the public response to recent news about Amazon's Ring, the Internet-connected doorbell. We've learned recently that Amazon has actually entered into arrangements with 400 police departments across the country that give police access to the video feed from the Internet-connected device on the front of the home. Most people who bought that product didn't know that that was a possibility and had no idea that was going on. When you have a video camera on the front of someone's home sending a feed to the police, who is most likely to appear in the feed? It's not some bad guy, it's actually going to be the residents. It's not just the privacy risk, it's also the risk of surveillance by law enforcement.

Q Any other examples?
A We've raised concerns about Google's Nest thermostat. There was actually an audio mic that could hear people, which created some Alexa-like functionality. Apparently they're now exploring adding facial recognition to the home thermostat. A device that most people understand in a pretty straightforward way, once connected to the Internet, creates some real risks. This isn't just something consumers need to worry about. The largest drone manufacturer in the world is DJI, a Chinese firm. The Department of Defense, after some testing, figured out that the manufacturer of the device could obtain remote access to the [drone's] imagery and audio. So the DOD suspended the purchase of so-called over-the-counter drones partly out of concern that the device was, itself, keeping information and transferring it to a third party.

Q What needs to be done?
A Much of our work has been to try to get Congress and the agencies to focus on these risks, because they're going to increase rapidly. But it's not just about

FROM LEFT: MCKINLEY WILEY; BOGDANDREAVA/GETTY

18+

WHAT IS AVAXHOME?

AVAXHOME-

the biggest Internet portal, providing you various content: brand new books, trending movies, fresh magazines, hot games, recent software, latest music releases.

Unlimited satisfaction one low price
Cheap constant access to piping hot media
Protect your downloadings from Big brother
Safer, than torrent-trackers

18 years of seamless operation and our users' satisfaction

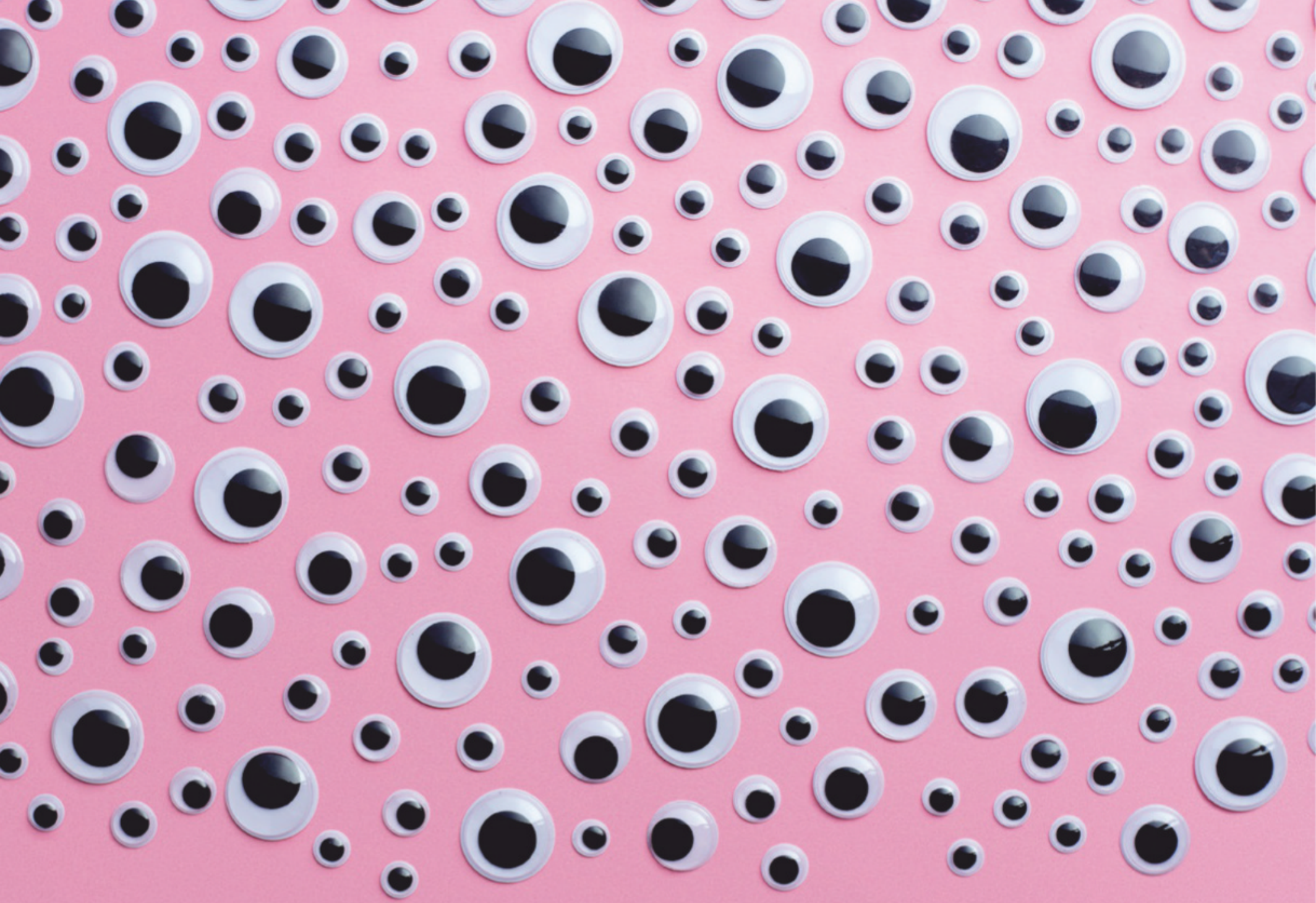
All languages
Brand new content
One site



AVXLIVE.ICU

AvaxHome - Your End Place

We have everything for all of your needs. Just open https://avxlive.icu



privacy, it's [also] about public safety. If you have door locks that are connected to the Internet, someone else [can] hack your front door and go into your home. If you had a comprehensive privacy law, then any company that was collecting personally identifiable data would be limited in how it could collect the data, and how it could use the data. We need federal legislation to limit the collection and use of personal data. We need to adopt robust security standards to ensure that Internet-connected devices can't be hacked by others. We need to minimize data collections. And we need to make meaningful decisions about the risks associated with Internet-connected devices, involving automobiles, drones, and door locks. Even thermostats.

Q What are the prospects for that kind of regulation?

A The good news is that privacy, unlike a lot of other issues in

"If you have door locks that are connected to the Internet, someone else [can] **HACK YOUR** front door."

Washington, is nonpartisan. So you do see Republicans and Democrats working together on legislation. There are about a dozen bills that have been introduced so far. But there hasn't been much movement. Part of the problem here is that we don't have strong advocacy for privacy within the Congress. And the Federal Trade Commission, which holds itself out as a privacy agency, really has not done enough to inform the Congress about the privacy risks from some of these devices.

Q Why isn't the market providing a solution, or a service, that shields people from this exposure? Seems like it would be a selling point.

A It's very difficult for people to evaluate the privacy risks. The technology rapidly changes and most of the companies are actually making their money off the data, not off the product. The business model makes it unlikely that consumers will be able to make meaningful choices.

Q What has to happen for Congress or the Federal Trade Commission to step up and take care of this problem?

A There has to be a willingness to recognize that market based solutions are not working. That's typically the argument that's made against legislation—"let's find a market-based solution." But if consumers can't meaningfully evaluate the risks, then it's unlikely that they're going to provide incentives in the market that are going to produce better products.

Q What will it take to create the sense of urgency needed to enact protections?

A It's going to require more people understanding the risk of Internet-connected devices. It may take a few well-publicized episodes. I also have said that, in the United States, in addition to privacy legislation, we need a new agency that's tasked with addressing these emerging challenges. In Europe, where you have data protection agencies, one of the issues that they are studying and proposing regulations for is precisely the Internet of Things.

sophisticated exploits they have used to bypass security on the traditional internet of computers, there's no telling what they might do.

"You're talking about getting access to potentially millions of people's homes, and when that happens, think about all of the microphones and cameras and actuators that you have around your house, and multiply that out by all the people who use these things," Cui says.

"Many consumers don't fully understand the risks associated with installing some of these devices in their homes," adds Alrawi.

Until they do, the situation is unlikely to change. Many experts wonder how big a price we will have to pay before that happens. "It's a mess," says David Kennedy, a cybersecurity expert who designs security for a wide array of manufacturers and has testified before Congress on the IoT. "An absolute mess. We're going into this very blind, without a lot of security discussions around what the impacts are going to be to our lives and to our safety."

Kennedy, whose current title is CEO of the company TrustedSec, has hacked into his share of devices over the years to make a point, including smart TVs, thermostats, smart fridges, robotic house cleaners and controllers that are connected to the energy grid. But Kennedy's biggest concern at the moment is in the area of automotive safety.

There have already been some cautionary tales. In 2015, Fiat Chrysler had to issue a safety recall affecting 1.4 million vehicles in the United States so it could patch software vulnerabilities, after two security researchers hacked into the internet-connected entertainment system of a Jeep Cherokee carrying a magazine reporter, took control of the vehicle, blasted the radio and AC, then brought traffic to a standstill in the middle of a freeway.

The problem, says Kennedy, is that most cars have scores of different pieces of technology in them, many of which are connected directly to the internet to allow them to transmit data needed for preventive maintenance. But the manufacture of these different IoT devices is often subcontracted out to scores of different contractors, which makes it logistically difficult to provide security updates and patches when new security vulnerabilities are discovered. (He pointed to Tesla as the major exception because, he argues, it is "a software manufacturer first and car manufacturer second," and thus knows how to build secure systems.)

The idea of regularly pushing out preventive security updates to patch newly discovered vulnerabilities in IoT-networked cars—a standard practice for products like Microsoft windows and the Apple iPhone—is new and has not yet been incorporated into the automotive industry. "I can't talk about which car manufacturers I've done assessment work for, but I can tell you that I've worked for a number of them, and security practices need a lot of work," he says. "They're not pushing patches out to the cars, which makes them extremely vulnerable to specific attacks—everything from eavesdropping in your car to driving them off the road."

The nightmare scenario is a mass fleet takeover, where a bad actor hacks different cars across the world to cause mass mayhem. "That's definitely something that's possible now with these

RISK REDUCTION
Lawmakers are wading into the murky waters of IoT regulation. Top right: a prototype of a Byton M-Byte electric SUV; Bottom right: Dave Limp of Amazon devices introduces the Echo Dot in 2018; Below: FBI Director Christopher Wray, CIA Director Gina Haspel and other officials testify before a Senate Intelligence Committee hearing on cybersecurity and other threats.

FROM TOP: ANDREJ SOKOLOW/PICTURE ALLIANCE/GETTY; GRANT HINDSLEY/AFP/GETTY; WIN MCNAMEE/GETTY

"Many consumers don't fully understand the risks associated with installing some of **THESE DEVICES** in their homes."









interconnected cars, no question about it," Kennedy says. "Someone will lose their life and then eventually they'll kind of knee jerk into fixing the whole industry. I think that's what it will take to change the mentality of car manufacturers."

Lawmakers in some jurisdictions are beginning to wade into the murky waters of IoT regulation. In January, California will become the first state to implement an IoT security law. The bill, passed in 2018 with a January 2020 deadline, will require companies that make connected devices to equip them with "reasonable security features," explicitly requiring that each device come with either a unique passcode or require the user to generate one before using the IoT device for the first time—taking aim at patching the vulnerability exploited so successfully in the Mirai exploit and the copycat attacks that have followed. Beyond that, however, the law seems to have been written to be purposely vague, allowing room for further state guidance in the future.

Cybersecurity experts have called on the Federal government in the U.S. to step in to regulate the industry. The U.S. House of Representatives last March introduced a bill, for the third session in a row, that would require the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce to develop recommended standards for IoT devices, and would assign the Office of Management and Budget (OMB) the task of issuing guidance to agencies that aligns with NIST's requirements. The law would also require NIST to offer guidance on vulnerability disclosure and report on IoT cybersecurity threats.

Two and half years ago, NIST started a program to look at the issue and this past summer solicited public comment on a voluntary set of minimum "baseline" security functions that any internet capable device should offer, whether it is intended for consumers, businesses or federal agencies, says Katerina "Kat" Megas NIST program manager, Cybersecurity for Internet of Things.

Among them, every single device must have a unique number or identifier associated with it that shows up on the network, which would make it easy to locate quickly and unplug the source of any problems that arise—a feature that many IoT devices currently do not offer. Other features would manage access to each device through secure methods of user authentication; protect data by encrypting it; and provide secure updates and log cyber-events so investigators can track how problems develop.

Few experts have illusions these measures will solve the problem soon. The standards would be voluntary. And even if Congress were to enact laws mandating security standards, a profound security vulnerability would remain: users themselves.

"No matter how strong your system is, it's only as strong as your weakest link—and the weakest link is always the human," says Jason Glassberg, cofounder of Casaba Security, a leading cybersecurity firm. "The largest breaches, the largest attacks for the most part have not been because of some super significantly technical attack. It's been because someone's been fooled into giving up their credentials. They've been fooled into clicking on a link which installed malware or asked them to provide their password. And it certainly doesn't change in the Internet of Things world."

Newsweek

AMERICA'S Best CUSTOMER SERVICE COMPANIES



Ready, set, shop! Here are the 480 stores consumers love most

IN THE COURSE OF A DAY, THERE ARE ANY NUMBER OF INTERACTIONS that can darken your mood. One thing that brightens it? Dealing with a company that treats you respectfully, one that prioritizes your needs and knows how much you value your time. They expect to accommodate you—not the other way around. Some companies are particularly good at nurturing their relationships with customers. And even as more and more retail jobs become automated, treating consumers well is still a key factor in business success. For the second year in a row, *Newsweek* partnered with Statista Inc., the respected global data-research firm, to uncover and highlight the Best Customer Service Companies 2020. Our ranking recognizes 480 companies in 160 retail categories. These companies work for *you*. → **NANCY COOPER,** *Global Editor-in-Chief*



METHODOLOGY

→ The 2020 America's Best Customer Service rankings were identified from the results of an independent survey of more than 20,000 U.S. customers who either made purchases, used services or gathered information about products or services in the past three years. Customers evaluated several brands: 115,115 evaluations were collected in total. The awarded brands each received on average close to 100 evaluations from customers.

The survey was conducted on retailers and service providers from 160 categories, providing results for a broad spectrum of customer experiences in traditional retail, online and service segments. For each category, the most relevant brands have been included in the scope of the survey according to their reputation, turnover or market share. In the brick and mortar categories, only retailers and service providers present in at least two census regions have been included in the list. In the online categories, only retailers and service providers present mainly online have been included in the list. For retailers and service providers with online presences and store networks, only the core business was taken into account.

The final assessment and rankings were based on the Net Promoter Score* (50 percent of the final score) and five evaluation criteria (also 50 percent of the final score):

1. **Quality of Communication** Measures whether the contact (via e-mail, telephone or face to face) was friendly or polite.
2. **Professional Competence** Measures the quality of information received and whether questions were answered correctly and in sufficient detail.
3. **Range of Services** Measures whether one's personal expectations and requirements were fulfilled.
4. **Customer Focus** Measures whether a personal concern/requirement was addressed with a tailored/specific solution.
5. **Accessibility** Measures the availability of customer service in a shop or on a helpline.

The top three brands receiving the highest scores for their category were awarded as America's Best Customer Service 2020.

SHOP AT THE TOP

Meet the most loved companies helping us eat, shop, travel and live



01 Disney Cruise Line

This magical company earned the highest rating, A-, of any cruise line this year for reducing its carbon footprint from Friends of the Earth. It also wants to inspire more women to take to the seas and will be gifting new scholarships to students at a maritime academy in The Bahamas.



02 Neiman Marcus

Despite operating for 112 years, it only opened its first New York City flagship this year. Many of their stores use digitized mirrors so customers can record themselves in 360 degrees and "try on" different colors, and now customers can check out from their fitting room.



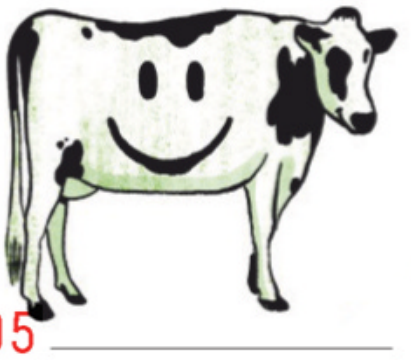
03 The Ritz-Carlton

Its spirit began in Boston's luxurious Ritz-Carlton in 1927, which had a room rate of $15 and kept lights on in vacant rooms during the Great Depression to look successful. For decades, staff have followed the motto, "We are Ladies and Gentlemen serving Ladies and Gentlemen."



04 Edward Jones

A Fortune 500 company founded in 1922 that now has 18,000 financial advisors working for 7 million clients with more than $1.5 trillion in assets under care. Last year, the company's contributions to the Alzheimer's Association topped $6 million alone, following $4.8 million in 2017.



05 Chick-fil-A

Despite its commitment to still closing every Sunday, it has, for four years, beaten out every fast food establishment in the American Customer Satisfaction Index restaurant report. Part of their success is that franchisees are carefully chosen and are usually limited to a single store.



06 L.L.Bean

Hikes, camping trips, free concerts and maker nights: this is how the outdoor goods company is leading the way for building unique experiences for customers. And despite having scaled back its much-loved lifetime return policy, the 107-year-old retailer still allows returns within the first year.



07 Nat'l Storage Affiliates

Real estate investment trust focused on self-storage properties. It operates and holds ownership interests in 729 self storage properties in 35 states and Puerto Rico, amounting to 46 million rentable square feet. All their properties are set to receive energy efficient LED lighting.



08 Embassy Suites

Guests can expect free breakfasts and evening drinks and snacks everyday, while the Make it Right promise means staff will fix anything that's gone wrong at your stay in any of their 245 locations. They also partner with Clean the World to recycle leftover soap and hygiene products.



09 Publix

The world's largest employee-owned company, this supermarket chain has had the same slogan for 60 years: "Where shopping is a pleasure." Its stores provide free medications and gift card incentives for getting the flu shot and are now rolling out wheelchair-friendly shopping carts.



10 Beau-coup

Named for the French phrase *merci beaucoup*. Online retailer providing favors for every type of party you can think of: weddings, baby showers or bridal parties. It was dreamt up on the back of a napkin by Polly Liu on the way back from her honeymoon in 2001.

Illustrations by ALEX FINE

BRICK & MORTAR



CATERING, RESTAURANTS & LEISURE

CATEGORY	BRAND	SCORE
Bagel and Sandwich Chains	Jersey Mike's Subs	8.32
	Jason's Deli	8.22
	Potbelly Sandwich Shop	8.22
Buffet Restaurants	Souplantation	8.03
	Hoss's Steak and Sea House	7.80
	Pizza Ranch	7.70
Casual Dining Restaurant Chains	Bonefish Grill	8.68
	LongHorn Steakhouse	8.49
	Texas Roadhouse	8.48
Coffeehouse Chains	Tim Hortons	8.29
	Starbucks	8.22
	Dunkin' Donuts	7.99
Doughnut Chains	Hurts Donut	8.56
	Krispy Kreme	8.33
	Jack's Donuts	8.28
Fast-Casual Restaurant Chains	Panera Bread	8.16
	Chuys	8.13
	Chipotle	8.08
Fast-Food Restaurant Chains	Chick-fil-A	9.08
	In-N-Out Burger	8.83
	Whataburger	8.81
Ice Cream & Frozen Yogurt Stores	Marble Slab Creamery	8.57
	Menchie's Frozen Yogurt	8.42
	Ben & Jerry's	8.36
Movie Theaters	Marcus Theatres	8.45
	Cinemark	7.97
	Regal Cinemas	7.94
Pizza Chains	Hungry Howie's	8.66
	Papa Murphy's	8.66
	Marco's Pizza	8.31
Upscale Chain Restaurants	The Capital Grille	8.82
	Del Frisco's Double Eagle Steak House	8.67
	Morton's The Steakhouse	8.64

CLOTHING

CATEGORY	BRAND	SCORE
Apparel	Hollister	8.38
	American Eagle Outfitters	8.07
	GAP	8.05
Baby & Children's Products	Justice	8.73
	Carter's	8.55
	Janie and Jack	8.51

Bridal Fashion	Lovely	7.85
	Fabulous Frocks	7.84
	Winnie Couture	7.65
Department Stores	Nordstrom	8.87
	Dillard's	8.75
	Bloomingdale's	8.66
Fashion Jewelry & Accessories Retailer	Alex and Ani	8.68
	Fossil	8.01
	Icing	7.98
Footwear	Vans	8.43
	Crocs	8.31
	DSW	8.25
High Jewelry Retailer	Jared	8.55
	Tiffany & Co.	8.53
	Kay Jewelers	8.24
Jewelry Retailer	James Avery	8.71
	Swarovski	8.29
	Pandora	8.22
Lingerie	Soma	8.26
	La Perla	8.21
	Victoria's Secret	8.16
Luxury Fashion & Accessories	Neiman Marcus	9.11
	Hugo Boss	8.58
	Versace	8.54
Outdoor & Athletic Apparel	Eddie Bauer	8.90
	The North Face	8.52
	Under Armour	8.49
Plus-Size Fashion	Torrid	8.64
	DXL	8.40
	Catherines	8.31
Premium Apparel	JoS. A. Bank	8.85
	Ralph Lauren	8.58
	Tommy Hilfiger	8.56
Second-Hand Clothing & Products	Once Upon A Child	7.94
	Red, White & Blue Thrift Stores	7.85
	Goodwill	7.46
Sporting Goods Retailer	Scheels	8.31
	Academy Sports + Outdoors	8.28
	Finish Line	7.80
Women's Apparel	J.Jill	8.88
	Chico's	8.72
	Ann Taylor	8.10

FOOD, HEALTH & BEAUTY

CATEGORY	BRAND	SCORE
Chocolate & Candy Stores	See's Candies	8.79
	Godiva	8.76
	Lindt	8.42
Convenience Stores	QuikTrip	8.46
	Wawa	8.41
	Sheetz	8.26
Eyewear Retailers	Warby Parker	8.33
	MyEyeDr.	7.96
	Eyeglass World	7.82
Hearing Care	Hearing Tracker	7.74
	HearUSA	7.72
	Miracle-Ear	7.52
Perfume & Cosmetics	Sephora	8.55
	M·A·C	8.54
	Bath and Body Works	8.49
Pharmacies & Drugstores	Good Neighbor Pharmacy	8.39
	Giant Eagle Pharmacy	8.19
	Health Mart Pharmacy	8.12
Supermarkets	Publix	9.01
	Wegmans	8.99
	Trader Joe's	8.95

Superstores & Warehouse Club Stores	Costco	8.75
	Meijer	8.48
	BJ's	8.24

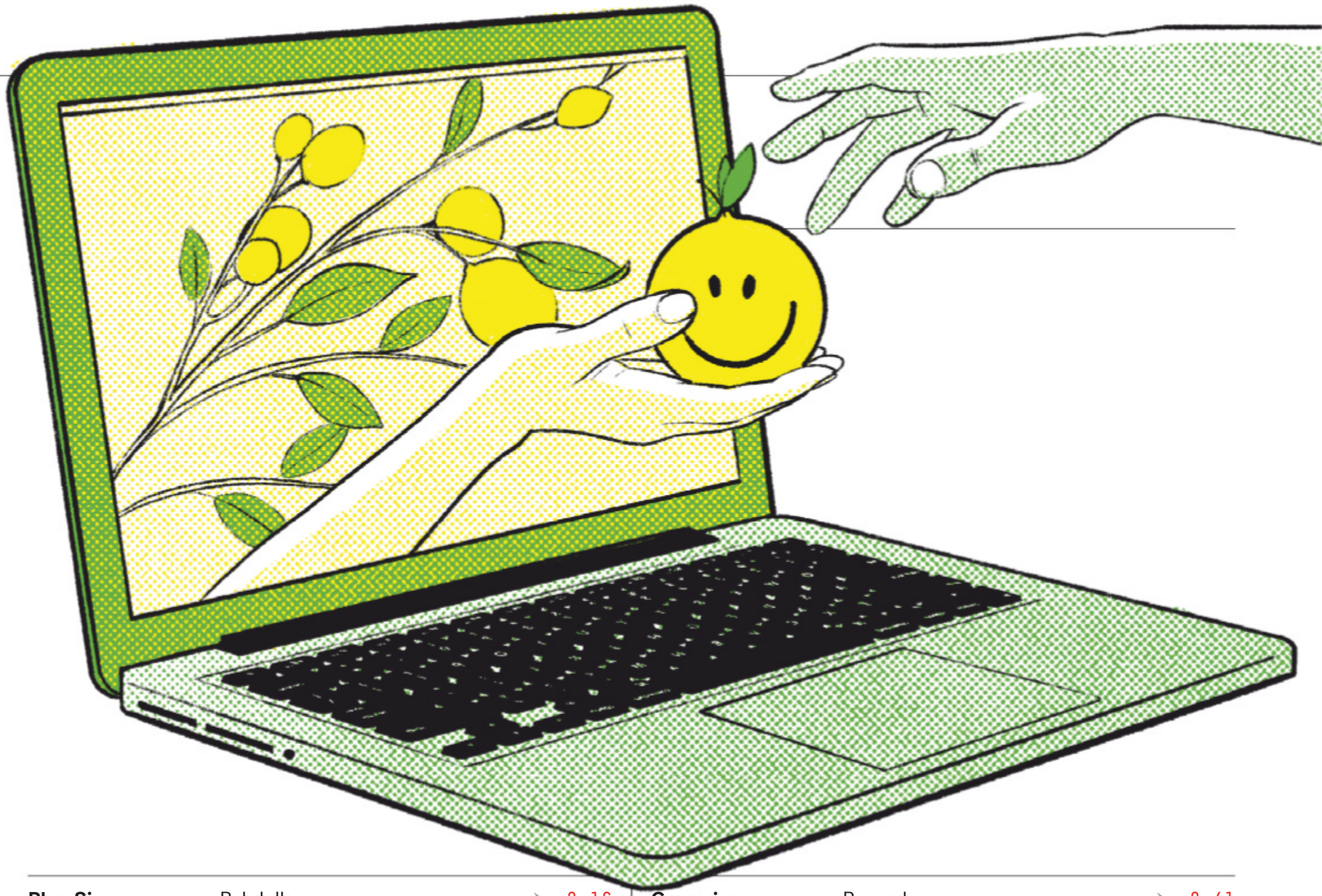
HOME GOODS

CATEGORY	BRAND	SCORE
Arts & Crafts	Blick	8.40
	Hobby Lobby	8.32
	Jo-Ann	8.16
Bookstores	Barnes & Noble	8.55
	Half Price Books	8.15
	Books-A-Million	8.01
Furniture Retail	Rooms To Go	8.58
	La-Z-Boy	8.53
	Bob's Discount Furniture	8.19
Home Goods & Decor	The Container Store	8.36
	Bed Bath & Beyond	8.31
	Pier 1 Imports	8.28
Home Improvement Stores	True Value Hardware	8.29
	Ace Hardware	8.25
	Lowe's	8.20
Outdoor Sporting Goods	L.L.Bean	9.07
	REI	8.98
	Bass Pro Shops	8.70
Pet Care	Petsense	8.99
	Pet Supplies Plus	8.41
	Pet Supermarket	8.39
Premium Furniture Retail	Ballard Designs	8.31
	Crate&Barrel	8.00
	Pottery Barn	7.98
Toys	Disney Store	8.35
	LEGO	8.22
	American Girl	8.17

ONLINE RETAILERS

CLOTHING

CATEGORY	BRAND	SCORE
Apparel	Everlane	8.42
	Lands' End	8.41
	Hanes	8.27
Baby & Children's Products	Burt's Bees Baby	8.35
	aden & anais	8.27
	The Honest Company	8.19
Footwear	Scarpetta Shoes	8.22
	Zappos	8.17
	6pm.com	7.87
Jewelers	Etsy	8.57
	Ross-Simons	8.13
	Allurez	7.88
Luxury Fashion Accessories	kate spade	8.43
	Moda Operandi	8.33
	Bergdorf Goodman	8.22
Members-Only Sales	HauteLook	7.75
	Zulily	7.73
	RueLaLa	7.70
Men's Accessories	Beau Ties	7.69
	Bowtie.com	7.59
	Tiemart	7.56
Occupational Clothing	UniFirst	8.14
	Dickies	8.12
	USA Scrub	7.98



Plus-Size Fashion	Rebdolls	→	8.16
	Roaman's	→	8.15
	Woman Within	→	8.04
Women's Apparel	Nico Nico	→	7.45
	Venus	→	7.44
	ModCloth	→	7.22

FOOD, HEALTH & BEAUTY

CATEGORY	BRAND		SCORE
Adult Beverages	Total Wine & More	→	8.75
	Quality Liquor Store	→	8.39
	Wine.com	→	7.74
Contact Lenses	1-800 Contacts	→	8.21
	LensDirect.com	→	8.20
	Contacts Direct	→	7.71
Eyewear Retailers	Zenni Optical	→	8.26
	Coastal	→	8.09
	Glasses.com	→	7.70
Groceries	Peapod	→	8.41
	AmazonFresh	→	8.38
	Boxed	→	8.05
Meal Kit Services	HelloFresh	→	8.20
	Home Chef	→	8.14
	Sun Basket	→	8.13
Medical Supplies	Edgepark Medical Supplies	→	7.97
	Medical Supply Depot	→	7.83
	East Coast Medical Supply	→	7.69
Perfume & Cosmetics	Lancôme	→	8.91
	Clinique	→	8.79
	Estée Lauder	→	8.60
Restaurant Delivery Services	Postmates	→	7.77
	DoorDash	→	7.74
	Uber Eats	→	7.72
Shopping TV Channels	QVC	→	8.61
	Home Shopping Network	→	8.32
	EVINE Live	→	7.83

Subscription Boxes (Clothing & Other)	Le Tote	8.37
	Dollar Shave Club	8.35
	Society Socks	8.27
Subscription Boxes (Makeup & Cosmetics)	Birchbox	8.18
	Play! by Sephora	8.17
	FabFitFun	8.08
Vegan & Vegetarian Products	Vegancuts	8.43
	VeganEssentials	8.35
	The Green Life	7.93

HOME GOODS

CATEGORY	BRAND	SCORE
Booksellers	Amazon	8.66
	Powells	8.21
	ThriftBooks	8.10
Consumer Electronics	Apple	8.65
	HP	8.55
	Samsung	8.34
Flower Retailer	ProFlowers	8.17
	Send Flowers	8.06
	Florists	7.98
Home Furnishings	Magnolia	7.88
	The Company Store	7.61
	Caitlin Wilson	7.54
Lighting	Lumens	7.96
	Lamps USA	7.77
	Shades of Light	7.76
Office Supplies	Quill	7.98
	OfficeSupply.com	7.91
	Concord Supplies	7.51
Online Home Stores	Wayfair	8.33
	Fingerhut	8.14
	Hayneedle	8.11



Second-Hand Products	eBay	8.13
	Poshmark	8.05
	Gazelle	7.96

ONLINE SERVICES & DIGITAL PRODUCTS

CATEGORY	BRAND	SCORE
Book Printing Services	KDP Print	7.91
	Blurb	7.47
	DiggyPod	7.27
Business Printing Services	GotPrint	8.57
	Overnight Prints	8.38
	Vistaprint	8.25
Cloud Storage and Cloud Computing Services	Google Drive	8.27
	iCloud	8.18
	MediaFire	8.18

Email Services	Gmail	8.26
	Inbox.com	7.53
	Microsoft Outlook	7.49
Employment Search Engines	Indeed	7.82
	LinkedIn	7.55
	Glassdoor	7.43
Internet Service Providers	Cox	7.32
	xfinity	7.05
	Spectrum	7.04
Language E-Learning Platform	italki	8.30
	Duolingo	8.06
	Rosetta Stone	7.90
Mobile Carriers & Telecommunications	Consumer Cellular	8.69
	T-Mobile	7.93
	Verizon Wireless	7.77
Music Streaming Services	Spotify	8.76
	Pandora	8.54
	SiriusXM	8.44
Online Dating Sites	ChristianCafe.com	7.63
	Elite Singles	7.08
	Bumble	6.89
Pay-Per-View Services & Video-On-Demand	Netflix	8.48
	Amazon Video	8.32
	Hulu	8.11
Price-Comparison Websites	Shopzilla	7.91
	Google Shopping	7.83
	Shopping.com	7.79
Ticketing Services	Vivid Seats	8.02
	Fandango	7.73
	StubHub	7.72
Wedding Registries	Wayfair	7.99
	The Knot	7.62
	MyRegistry.com	7.49

SPORTS & LEISURE

CATEGORY	BRAND	SCORE
Bicycles	Western Bike Works	8.84
	Jenson USA	8.67
	Bike Nashbar	8.48
Costumes & Accessories	Halloween Express	8.11
	Buy Costumes	7.77
	Costume SuperCenter	7.69
Electronic Cigarettes	VaporDNA	8.25
	180 Smoke	8.03
	VaporBeast	7.99
Fishing Equipment & Clothing	Tackle Warehouse	8.33
	Fishing Tackle Unlimited	7.84
	Outlet Bait & Tackle	7.71
Hobby Store, Model Making	Free Time Hobbies	8.05
	Gundam Planet	7.88
	Horizon Hobby	7.84



Hunting Gear & Equipment	MidwayUSA	8.62
	Sportsman's Guide	8.21
	Cheaper Than Dirt	8.19
Musical Equipment	Sweetwater	8.59
	American Musical Supply	8.35
	World Music Supply	8.04
Party Supplies	Beau-coup	9.00
	Koyal Wholesale	8.09
	Oriental Trading Company	7.98
Pet Food & Pet-Related Products	Chewy	8.88
	1800Petsupplies.com	8.49
	Coupaw.com	8.44
Photo and Video Equipment	B&H	8.50
	Canon	8.22
	Adorama	8.15
Sports & Fitness Nutrition	Vitacost	8.96
	Optimum Nutrition	8.46
	Puritan's Pride	8.19

TRANSPORTATION

CATEGORY	BRAND	SCORE
Auto Parts Retailer	RockAuto	8.38
	Auto Parts Warehouse	7.56
	1A Auto	7.41
Automotive Marketplace	CarGurus	7.80
	Autotrader	7.48
	TrueCar	7.38
Motorcycle Parts & Accessories	MotoSport	8.65
	J&P Cycles	8.35
	Revzilla	8.04
Tire & Wheel Manufacturers	Tirebuyer	8.87
	Tire Rack	8.02
	Discount Tire Direct	8.00

SERVICES

BEAUTY & WELLNESS

CATEGORY	BRAND	SCORE
Fitness Centers	YMCA of the USA	8.38
	Planet Fitness	7.89
	LA Fitness	7.75
Hair Salons	Fiesta Salon	8.00
	Hair Cuttery	7.78
	Famous Hair	7.41
Nutrition & Weight-Loss Programs	WW (Weight Watchers Reimagined)	8.18
	Beachbody	7.83
	Herbalife	7.64
Spas, Wellness & Beauty	bliss spa	8.08
	Elements Massage	8.05
	Hand & Stone Massage & Facial Spa	7.90

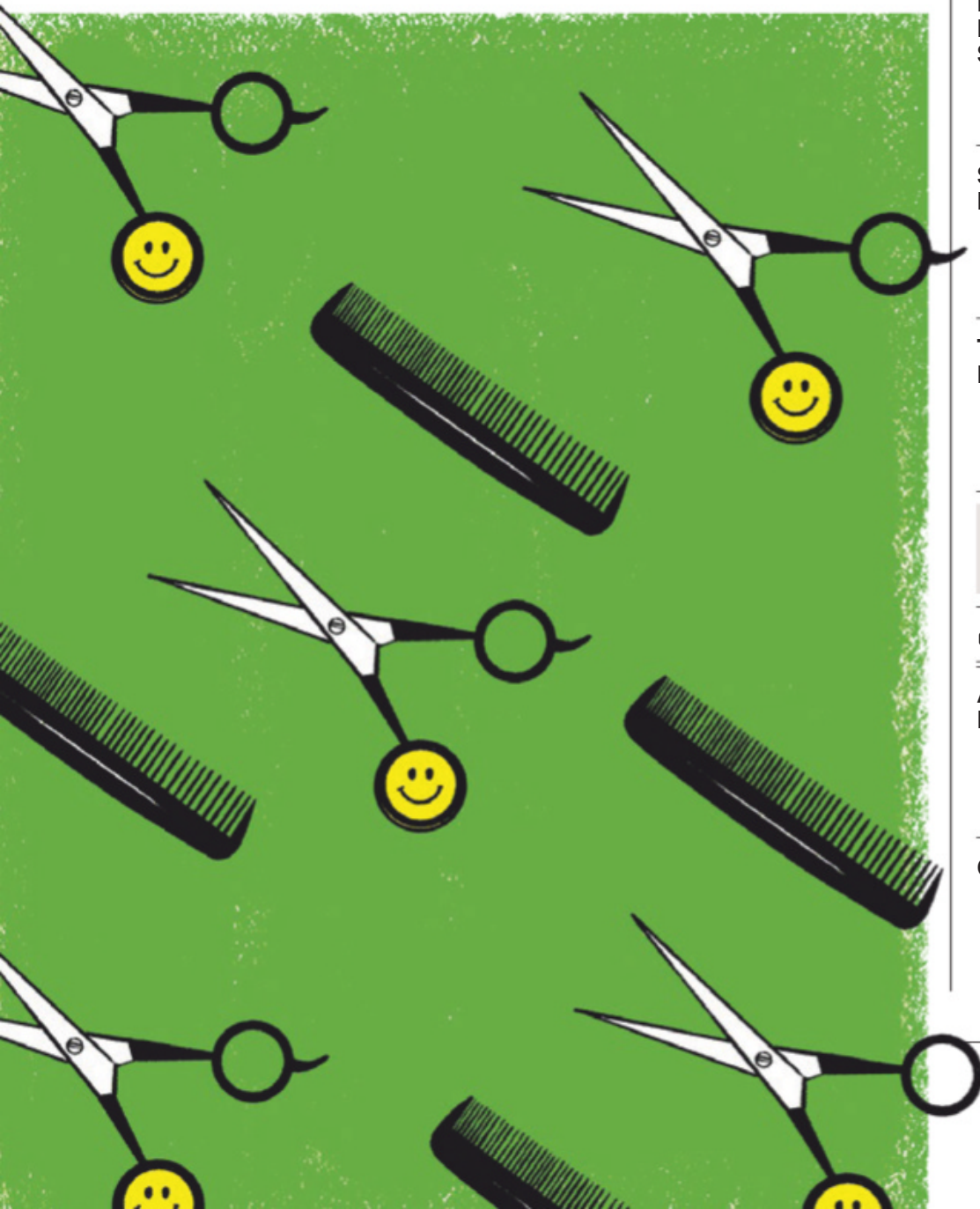
EMPLOYMENT, EDUCATION & CHILD CARE

CATEGORY	BRAND	SCORE
Child Care Services	Montessori Kids Universe	7.90
	KidsPark	7.46
	College Nannies, Sitters, and Tutors	6.81
Language Schools	OHC	8.20
	Kaplan International	7.84
	The Language Company	7.75
Nanny & Au Pair Agencies	Nanny Connections	7.89
	UrbanSitter	7.48
	Nanny Poppinz	7.33

Temporary Employment Agency	Apprentice Personnel	7.50
	Randstad	7.30
	Frontline Source Group	7.03
Tutoring Services	Kumon	7.65
	Huntington Learning Center	7.60
	Grade Power Learning	7.46

INSURANCE

CATEGORY	BRAND	SCORE
Accidental Death & Dismemberment Insurance	MetLife	8.09
	Fidelity Life	7.57
	Mutual of Omaha	7.24
Auto Insurance	USAA	8.88
	Safeco: A Liberty Mutual Company	8.25
	State Farm	8.23
Disability Insurance	MetLife	7.41
	Mutual of Omaha	7.33
	MassMutual	7.26
General Liability Insurance	State Farm	8.53
	USAA	8.30
	The Hartford	8.09
Health Insurance	Humana	8.14
	Aetna	7.87
	Blue Cross Blue Shield	7.70
Homeowners Insurance	USAA	8.99
	The Hartford	8.72
	Auto-Owners	8.53
Life Insurance	MetLife	8.18
	New York Life Insurance Company	7.98
	Prudential	7.93
Retirement Planning Solutions	AXA	8.92
	USAA	8.89
	Vanguard	8.64
Supplemental Insurance	UnitedHealthcare	8.37
	Blue Cross Blue Shield	8.15
	Humana	8.04
Travel Insurance	Nationwide	8.36
	Travel Insured International	8.16
	Generali Travel Insurance	8.11



PERSONAL, HOME CARE & MAINTENANCE

CATEGORY	BRAND	SCORE
Automotive Repair	Meineke	8.95
	O'Reilly Auto Parts	8.32
	Goodyear Auto Service Centers	8.31
Car Washes	Super Wash	7.74
	Goo-Goo	7.66
	Mister Car Wash	7.54

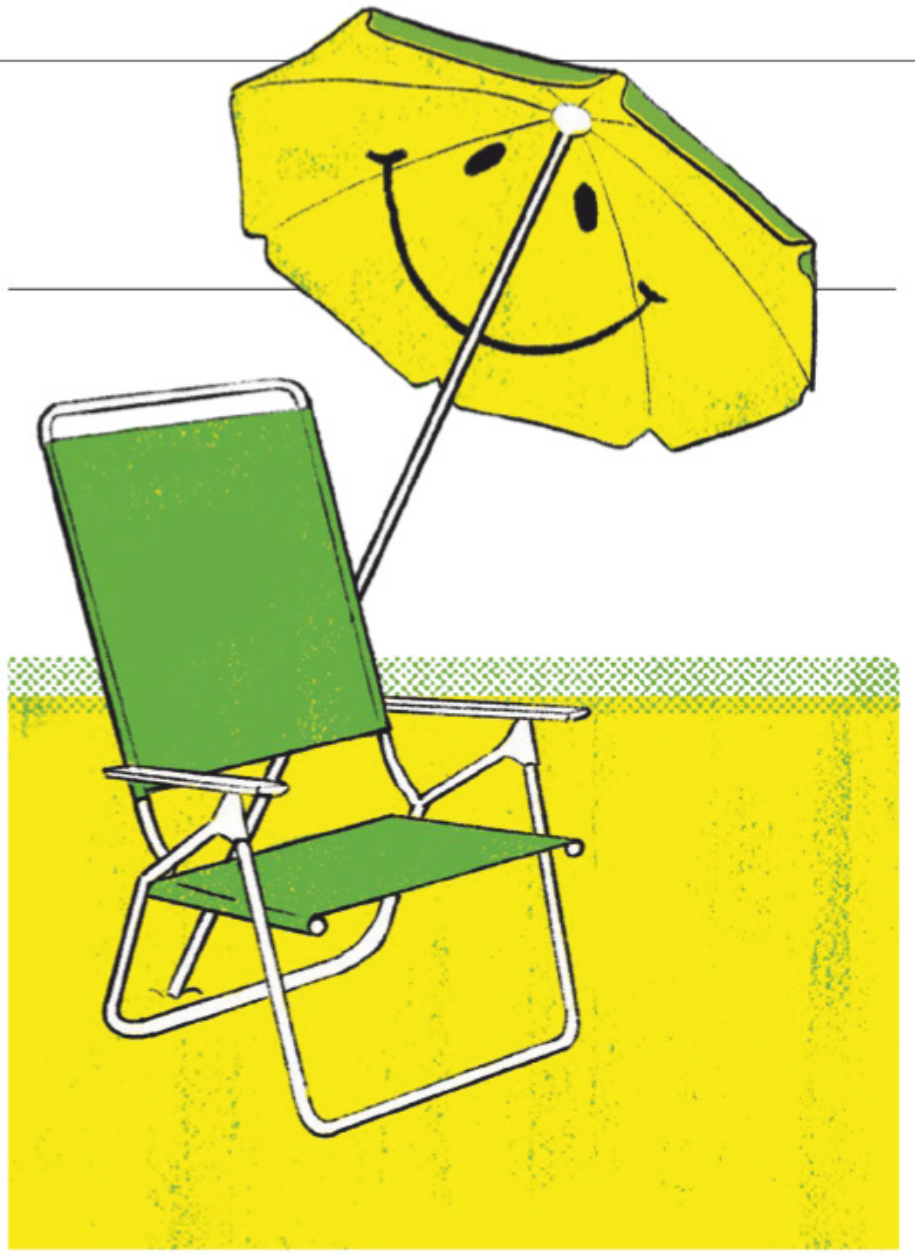
Dry-Cleaning Services	Tide Dry Cleaners	7.83
	Martinizing Dry Cleaning	7.26
	Dryclean USA	7.25
Handyman Referral Services & Home Repairs	Mr. Rooter Plumbing	7.76
	Handyman Matters	7.74
	Handy	7.33
Home-Care Services For Seniors & Disabled	Comfort Keepers	7.99
	Senior Helpers	7.90
	Visiting Angels	7.77
Home Security	Protect America	7.95
	SimpliSafe	7.87
	ADT	7.71
House Cleaning & Maid Services	The Maids	8.05
	Housekeeper	7.64
	Maid Brigade	7.53
Storage Centers	National Storage Affiliates	9.02
	Life Storage	7.89
	SecurCare Self Storage	7.63

REAL ESTATE & BANKING

CATEGORY	BRAND	SCORE
Asset Management	Vanguard	8.46
	Fidelity Investments	8.14
	JPMorgan Chase	8.07
Commercial Banks	PNC Bank	8.97
	TD Bank	8.77
	U.S. Bank	8.75
Crowdfunding Platforms	Indiegogo	7.86
	Kickstarter	7.78
	Republic	7.63
Online Banking	Discover Bank	8.24
	Charles Schwab Bank	8.19
	Ally	8.18
Payment Services	Zelle	8.84
	PayPal	8.22
	Amazon Pay	8.18
Real Estate Agencies	Keller Williams Realty	7.96
	RE/MAX	7.90
	ERA	7.85
Real Estate Database	RE/MAX	8.29
	Realtor.com	7.80
	Zillow	7.61
Trading & Brokerage Services	Edward Jones	9.09
	Vanguard	8.94
	Fidelity Investments	8.71

TRAVEL & TRANSPORTATION

CATEGORY	BRAND	SCORE
Airlines	Alaska Airlines	8.48
	Hawaiian Airlines	8.26
	Delta	7.95
Amusement Park Experience	Disney Parks & Resorts	8.88
	Busch Gardens Theme Parks	8.81
	LEGOLAND	8.64
Apartment Hotels, Extended Stays	Staybridge Suites	8.61
	Homewood Suites by Hilton	8.32
	Residence Inn by Marriott	8.27
Budget Hotel (1 to 2 stars)	Microtel	8.20
	La Quinta Inn & Suites	8.06
	Comfort Inn	7.94
Bus Carriers	Amtrak	7.52
	Trailways	7.06
	Megabus	7.05
Car Rental	Enterprise Rent-A-Car	8.36
	National Car Rental	8.23
	Thrifty	8.19



Carsharing	Maven	8.30
	Enterprise CarShare	7.72
	Car2go	7.72
Cruise Operators	Disney Cruise Line	9.29
	Celebrity Cruises	8.79
	Royal Caribbean International	8.65
Economy Hotel (3 stars)	Embassy Suites	9.01
	Hampton by Hilton	8.80
	Courtyard by Marriott	8.71
Flights, Hotels & Holiday Deals Search Engines	TripAdvisor	8.52
	trivago	8.14
	Kayak	8.00
Gas Stations	QuikTrip	8.35
	Marathon	8.18
	Valero	8.17
Low-Cost Airlines	Southwest Airlines	8.82
	JetBlue	8.55
	Allegiant Air	7.46
Luxury Hotel (5 stars)	The Ritz-Carlton	9.10
	JW Marriott	8.84
	InterContinental Hotel	8.73
Moving Services	U-Haul	8.01
	Allied Van Lines	7.27
	Two Men And A Truck	7.11
Music Festival	New Orleans Jazz & Heritage Festival	8.40
	EDC Las Vegas	8.22
	Essence Festival	7.93
Premium Hotel (4 stars)	Westin	8.95
	Hyatt	8.84
	Hilton	8.80
Ridesharing, Taxi	Lyft	8.12
	Uber	7.97
	RideYellow	7.12
Shipping & Delivery Services	UPS	8.30
	FedEx	8.23
	USPS	8.00
Spa Resort & Retreat	The Spa at Spruce Point Inn	8.85
	The Lodge at Woodloch	8.84
	LakeHouse Spa at Lake Austin Spa Resort	8.37
Travel Agencies	Expedia	7.89
	Travelocity	7.73
	Hotwire	7.35
Travel Management	BCD Travel	7.36
	Liberty Travel	7.36
	Carlson Wagonlit Travel	6.94
Vacation Rental	VRBO	8.22
	Airbnb	8.16
	Hotels.com	7.99

statista publishes worldwide established rankings and company listings with high profile media partners. This research and analysis service is based on the success of statista.com. The leading data and business intelligence portal provides statistics, business relevant data, and various market and consumer studies/surveys.

BY THE NUMBERS

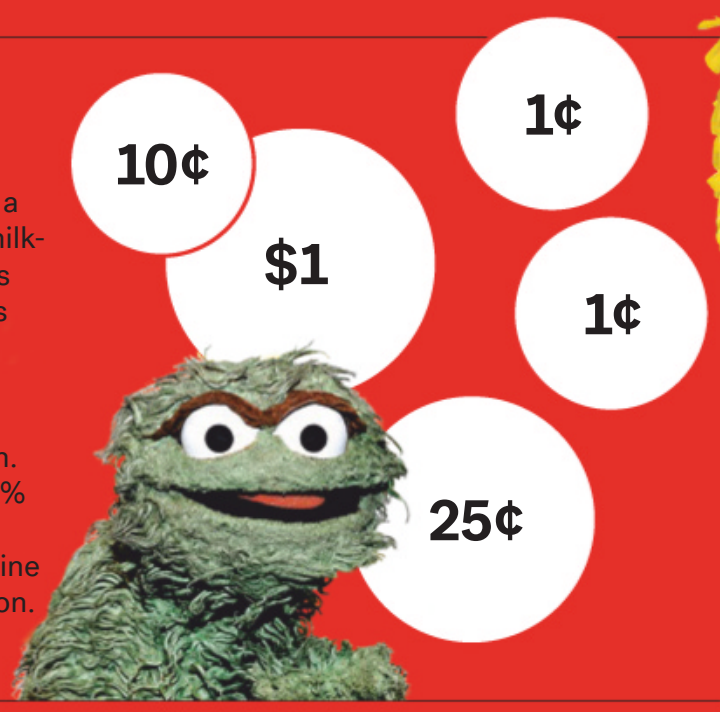
Sesame Street

Sesame Street is celebrating a big anniversary this month, brought to you by the numbers "5" and "0." Since the first episode aired on November 10, 1969, the show's reach has grown exponentially: *Sesame Street* is now watched by 150 million children in 150 countries and heard in 70 different languages. Here are some highlights from the past 50 years. —*Lauren Barrett, Maya Page*



$1.37

How much a birdseed milkshake costs at Hooper's Store, vs. 20 cents in the show's first season. That a 600% increase, roughly in line with inflation.



4,526 → The number of episodes aired over 49 seasons since *Sesame Street* first debuted (not including specials). The 50th season starts this month, airing on HBO and PBS Kids.

86 million

The number of adults who watched Sesame Street as children

8 feet 2 inches
Big Bird's height

3½

The perennial age of beloved pre-schooler Elmo, who joined the cast in 1984.

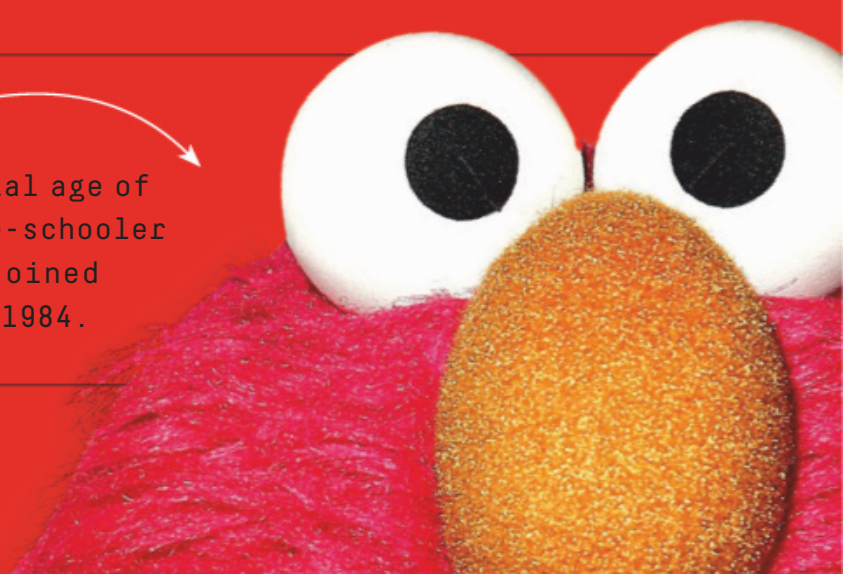
$135,2

Sesame Workshop's total operati

650

The number of celebrities who have visited *Sesame Street*. Carol Burnett and James Earl Jones were the first; Whoopi Goldberg has appeared most (seven times).

200



SOURCES: SESAME WORKSHOP, MUPPET WIKI, CENTER FOR UNIVERSAL EDUCATION AT BROOKINGS, PBS, LIBRARY OF CONGRESS

CLOCKWISE FROM LEFT: EUGENE GOLOGURSKY/GETTY; DOUGLAS GORENSTEIN/NBCUNIVERSAL/GETTY; LLOYD BISHOP/NBCUNIVERSAL/GETTY; RICH SCHULTZ/GETTY; DEBORAH FEINGOLD/GETTY; PHOTO12/UNIVERSAL IMAGES GROUP/GETTY; PAM FRANCIS/LIAISON/GETTY; PHOTO12/UNIVERSAL IMAGES GROUP/GETTY; PAUL ZIMMERMAN/GETTY; REVIERFOTO/GETTY

234,000

ng revenues in 2018



1,830,653 B.C.

The year that Count Von Count was born.

1,602,385

The number of Tickle Me Elmo dolls sold between fall 2017 and the end of last year. During the height of the Tickle Me Elmo craze in 1996, the dolls sold for thousands on the secondary market.





The year Big Bird and Carroll Spinney, the actor who played the character from 1969 through 2018 (as well as Oscar the Grouch), were declared Living Legends by the Library of Congress.

16%

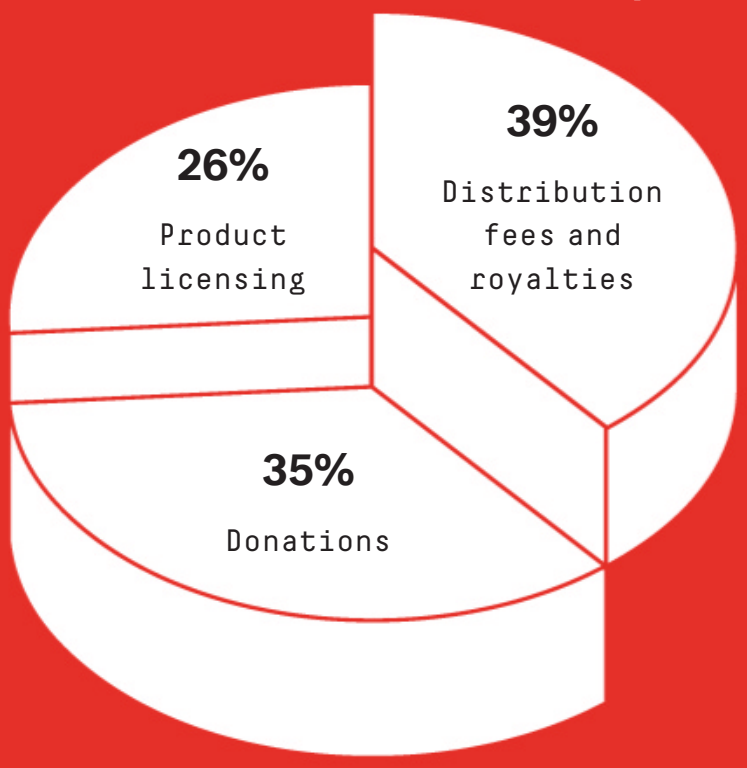


The percentage of the global population of children aged 7 or younger who watch *Sesame Street*.

14 PERCENTAGE POINTS

The average gain in literacy, numeracy and other types of learning among children in 15 countries who watched *Sesame Street* regularly compared with kids who didn't.

How *Sesame Street* makes money:





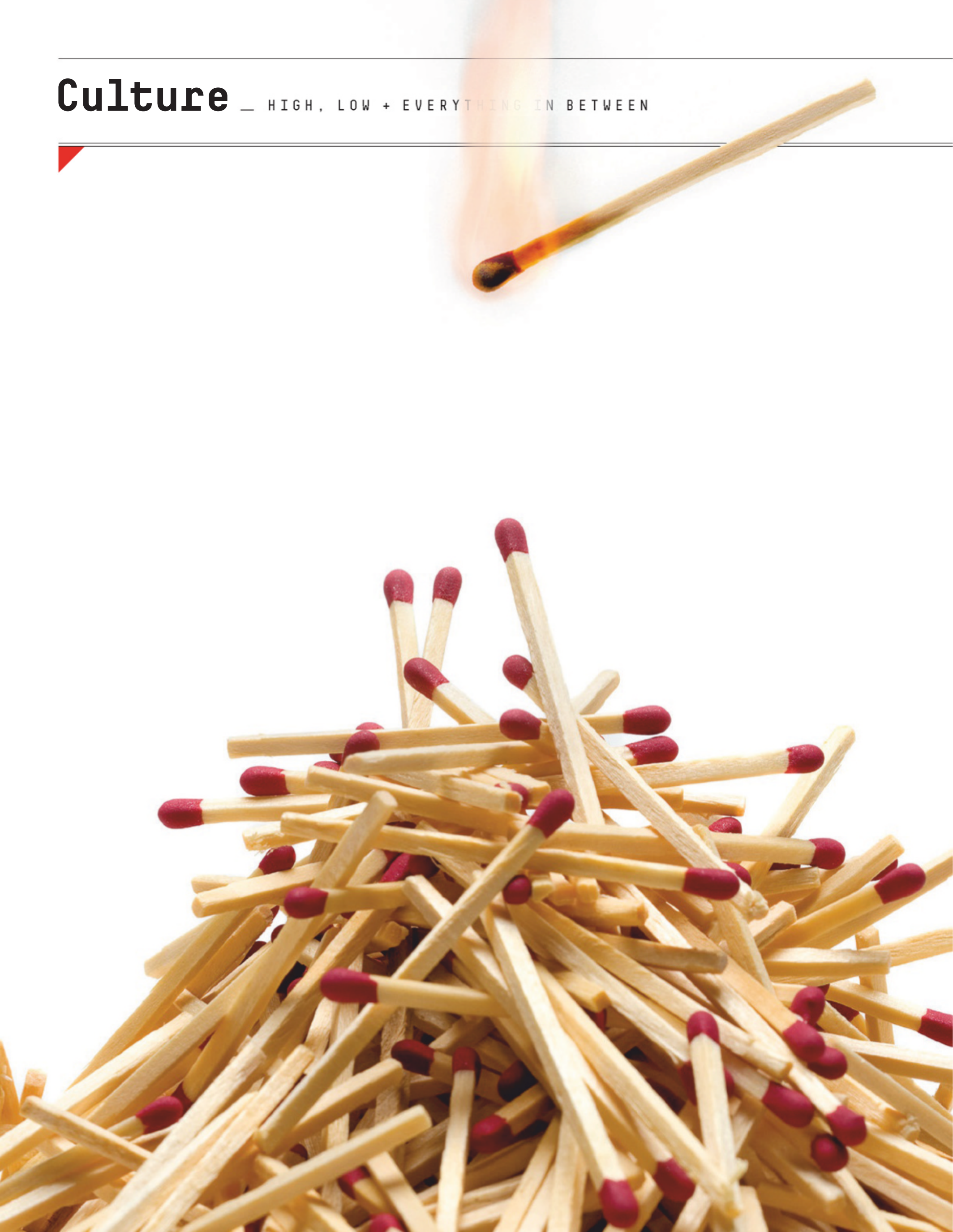
Four

The number of First Ladies who have visited *Sesame Street*: Michelle Obama, Hillary Clinton, Barbara Bush and Laura Bush

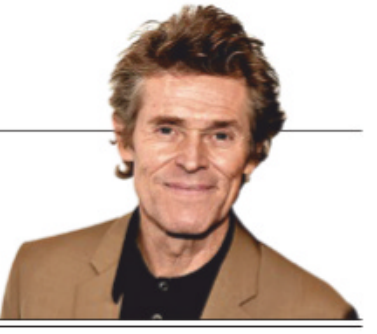


One → The number of *Sesame Street* characters who've testified before Congress (Elmo appeared in 2002 to advocate for music programs in schools). Also the number who have campaigned for president: Big Bird briefly ran in the 1976 election, which Jimmy Carter won.

Culture _ HIGH, LOW + EVERYTHING IN BETWEEN



STRANDED IN THE 1890S
Willem Dafoe on his new film, *The Lighthouse* » P.48



IDEAS

Taking on Political Correctness 101

In her new book, journalist/teacher/flamethrower Meghan Daum declares war on the thought police

BY

NINA BURLEIGH
@ninaburleigh

BELIEVE IT OR NOT: SOME ACADEMICS AND writers, who wouldn't be caught dead in Donald Trump's MAGA hats, have started complaining about language policing and other forms of intellectual bullying on the left. So says Meghan Daum in her new book, *The Problem With Everything: My Journey Through the New Culture Wars*, which will be published this month by Gallery Books.

Daum, 49, an author, journalist and sometimes teacher at Columbia University, has a deep distrust of dogma. Since 2016, she writes, she has distracted herself from her personal woes—divorce, the upheavals of middle age—by clicking onto social media. That's where she witnessed angry lefties swarm individuals who expressed opinions that deviated from a rigid set of rules related to how we talk about race and gender.

She watched with growing fascination as the Trump election, a profound challenge to progressive ideals, did not bring the opposition together, but splintered it, with the movement eating its own. "Almost immediately, the resistance became not just a front line against Trumpism but its own scorching battleground," she writes. "There was no amount of outrage that couldn't be outdone, no wokeness woke enough. Apparently any admission of complexity was a threat to the cause. Nuance was a luxury we could no longer afford."

What started out as a book about Hillary Clinton and feminism morphed into a meditation on the phenomenon. In a series of tart, funny chapters, she takes on pussy hats as needlessly offensive and alienating to potentially pro-female men and women, goes after the "weaponized victimhood" of the #MeToo movement, and suggests that the Trump administration's abuses at the Mexico border are horrible but not equivalent to the Holocaust.

Yes, she is controversial.

Daum devotes much of the book to critiquing the latest wave of feminism and her own relationship to the millennial and 20-somethings of the #MeToo movement. She regrets intersectional feminism, a mainstreamed, once academic theory that makes a kind of victimhood power hierarchy based on layers of marginalized status including being gay, female or a racial or ethnic minority. She rejects college rape statistics and suggests that manipulative and even lying young women do exist—and that some college men get a raw deal in campus "kangaroo courts." She recounts the ugly food fight between younger and older women over an anonymous sexual misconduct allegation against comedian Aziz Ansari that older women regarded as a mere bad date.



GARY S CHAPMAN/GETTY; TOP RIGHT: THEO WARGO/GETTY; THEO WARGO/FILM AT LINCOLN CENTER/GETTY

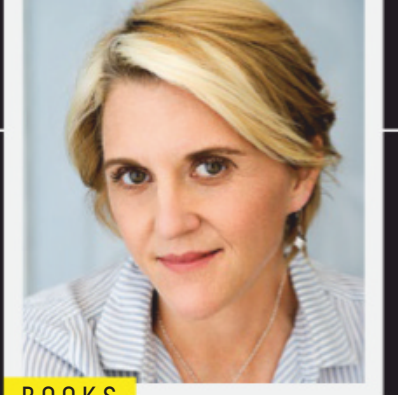
Throughout the book, her theme is: Buck up, kids. "Perhaps the starkest difference between Generation X and the generations that are now or were recently in college lies in the soul of our self-definition," she writes. "We were obsessed with being tough. They are obsessed with being fair. Just as "life in the big city" loomed large in our imaginations, life in a better world looms in theirs."

In one chapter, she describes how she showed a class of writing students in Iowa a clip of the late Christopher Hitchens, defending a notorious article he wrote about how women can't be funny, proclaiming that all female comedians are either Jewish or lesbians. As her students flinched and grimaced, Daum thought back to her own student days and a college film class in the 1980s that included an in-class screening of the Pier Paolo Pasolini film *The 120 Days of Sodom*. The film realistically depicts visceral and disgusting forms of torture. Daum and her Vassar classmates suffered through it, "gagging together even as we struggled to take notes in the dark. As I remember it, the collective gagging caused us to laugh, and from this combination arose a solidarity that rendered the whole experience too absurd to be traumatic, at least as far as I was concerned."

She concedes that "weaponized victimhood" offends her because she came of age at a time when young women equated feminism with being tough, and when they still routinely encountered—and laughed off—gross examples of male chauvinism. She suggests that the AIDS epidemic and accompanying panic gave her generation an existential grit that younger women lack.

"As we got older, the toughness instinct built up in us like muscle mass. When we got dumped by romantic partners, Job One was to keep it together and not cry until we were safely alone. When we got harassed at work, we would no sooner call human resources than call our parents. When we got mugged on the subway, we'd be terrified and shaken. But we'd also know that this was part of the cost of doing business."

Daum's writing is brave and engaging; she does some hard thinking about our times and demands that we do too. Crucially, her insistence on nuance distinguishes her from people on both sides of Trump-era America: She is entirely willing to admit that she doesn't know if she's right. N



BOOKS

Meghan Daum Q&A: I'm a Free Agent!

A lot of the excesses you describe are in the academic, media and publishing world where you teach and write. Did you ever worry about how these views might affect your career?
I didn't worry because I'm not beholden to any single institution. I'm a free agent. Furthermore, I've taken a counterintuitive approach to my writing for decades. I've gotten angry letters from readers since I started publishing in my twenties. But I've also always known that for every person who bothers to tell me how upset they are with what I wrote, there are probably hundreds who are grateful. To me, if you're not going to write in a way that challenges people's assumptions, what's the point of doing the job?

You have witnessed how language policing works on some major campuses. What's the most memorable example you have personally witnessed or heard about?
I think the most serious example of the last few years is probably the case of Oberlin students (and a few professors and administrators) fomenting a major racial uproar over a relatively minor incident that occurred at a local, family-owned bakery near the campus. The reputational damage to the bakery was so extreme that the bakery eventually won $44 million in a defamation lawsuit against Oberlin. The initial incident happened in 2016 (the day after Trump was elected) and the jury verdict happened last summer. That might suggest that public patience for this kind of thing is starting to wane.

Are more intellectuals like you going public?
I like to call us cognitive dissidents. We're owning the cognitive dissonance that happens when you try to stay intellectually honest amid all the groupthink. From there, we're starting to speak up more, even if it means getting cast out of certain media tribes. It's crucial that smart, thoughtful people are willing to take risks and engage in these conversations that have been deemed off-limits. Because if we don't do it there are plenty of stupid, thoughtless people who are happy to do the job for us. *-N.B.*



FROM TOP: COURTESY OF GALLERY BOOKS; NIKAMATA/GETTY

UNDER THE HIGH PATRONAGE OF HSH PRINCE ALBERT II OF MONACO

THE UNITED TALENTS OF

ONLYWATCH

CREATE BEAUTY TO DO GOOD

9 NOVEMBER 2019 - 2PM, GENEVA

A BIENNIAL CHARITY AUCTION OF UNIQUE TIMEPIECES
FOR RESEARCH ON DUCHENNE MUSCULAR DYSTROPHY

AKRIVIA GENEVE · ANDERSEN GENEVE · ARMIN STROM · ARNOLD & SON 1764 · ARTYA · ATELIERS DEMONACO

AUDEMARS PIGUET · Bell & Ross TIME INSTRUMENTS · BLANCPAIN · BOUCHERON · BOVET 1822 Engineering Brilliance · Breguet Depuis 1775

CARL F. BUCHERER LUCERNE 1888 · CHANEL · CHRISTOPHE CLARET · CYRUS GENÈVE · CZAPEK GENÈVE · DE BETHUNE

DEWITT · FABERGÉ · FERDINAND BERTHOUD 1753 · F.P. JOURNE Invenit et Fecit · FREDERIQUE CONSTANT GENEVE · GIRARD-PERREGAUX

GRÖNEFELD · H. Moser & Cie. VERY RARE · HERMÈS PARIS · HUBLOT · JACOB & CO · JAEGER-LECOULTRE

JAQUET DROZ · KONSTANTIN CHAYKIN · L'EPEE 1839 · LOUIS MOINET 1806 · LOUIS VUITTON · MAURICE LACROIX

MB&F · MONTBLANC · MORITZ GROSSMANN · PATEK PHILIPPE GENEVE · PIAGET · REBELLION

RICHARD MILLE · RJ · Singer · SPEAKE-MARIN · TRILOBE · TUDOR

ULYSSE NARDIN · URWERK · VOUTILAINEN Artisan d'Horlogerie d'Art · ZENITH

WORLD TOUR EXHIBITION

MONACO, SEP. 25-28 | DUBAI, OCT. 1-3 | PARIS, OCT. 7-8 | LONDON, OCT. 11-13 | NEW YORK, OCT. 16-17
TOKYO, OCT. 23-24 | SINGAPORE, OCT. 25-26 | HONG KONG, OCT. 28-29 | TAIPEI, OCT. 30-NOV. 1 | GENEVA, NOV. 7-9

ONLYWATCH.COM

Organised by

Association Monégasque Contre les Myopathies

Auctioned by

CHRISTIE'S

Illustration by BRITT SPENCER

PARTING SHOT

Willem Dafoe

"IT'S NOT REALLY A HORROR FILM OR A THRILLER. IT DEFIES DESCRIPTION. It's like nothing you have ever seen before and a beautiful character study," says four-time Oscar nominee Willem Dafoe about *The Lighthouse* in a *Newsweek* Conversation produced by Maria Vultaggio. Set in the 1890s and directed by Robert Eggers, *The Lighthouse* is a mesmerizing tale about two lighthouse keepers who get stranded together. The film opened October 18. Dafoe also stars in Edward Norton's *Motherless Brooklyn*, in theaters November 1. Adapted from Jonathan Lethem's novel, it tells the story of private detective Lionel Essrog (Norton), who has Tourette syndrome. He tries to uncover the murder of his friend, Frank Minna (Bruce Willis), but instead uncovers a salacious truth about politician Moses Randolph, loosely based on the real life Robert Moses, the controversial "master builder" of New York City. For his adaptation, Norton created new characters and set the story in the 1950s. "The whole story that alludes to New York politics is invented and has certain resonances with what's going on in the world now," says Dafoe.



"It really defies description. It's like nothing you have ever seen before."

Was shooting *The Lighthouse* in black-and-white limiting?
I don't find those choices restrictive. There are a lot of things you can do visually… you forget it's black-and-white after awhile. It does things that color can't do.

Tell me about *The Lighthouse*.
There's kind of an antagonistic relationship because I'm the old hand bossing around this new guy, played by Robert Pattinson. He isn't quite with the program. And then we're stuck. If there were tensions before, they get much worse.

Were the conditions harsh?
Actors love to complain about the misery they go through in their work, but it's great work if you can get it. A movie like this has harsh conditions, but often I prefer working on location because you start to create a story, a narrative, that's not of your life.

How is Norton's character special?
His weakness is his strength. While he's alienated from people because they don't know how to deal with his behavior, he free-associates in quite an uncontrolled way and he's got crazy OCD. But he can also remember things. He also puts things together in a way that most people can't.

How was shooting in your hometown for *Motherless Brooklyn*?
It's great to sleep in your own bed! I love shooting in New York at night. You really get a feel for the pulse of the city.

80th Anniversary Edition




GAZING OVER THE RAINBOW
"Judy Garland's Dorothy is a part and parcel of the dream that is in the heart and eyes of a believer in fairy tales," wrote Frank S. Nugent in *The New York Times* on August 18, 1939. Decades later in 1996, Roger Ebert added that Garland's performance "is the reason the film was universal." Here, different people from many backgrounds have a compartment of their memory reserved for *The Wizard of Oz*."

THE WIZARD OF OZ

Judy Garland as Dorothy

Studio boss Louis B. Mayer's second choice becomes first in our hearts.

BY 1939 she had four years as a contract player under her belt and was a veteran leading lady at only 16, but the public still saw Judy Garland as a child star. Based on her popular musical comedies with MGM, in which both she and Mickey Rooney acted and danced, Garland had become a household name and one of MGM's brightest stars. Her musical talent made her the first choice of producers Mervyn LeRoy and Arthur Freed for the role of Dorothy, but studio chief Louis B. Mayer's original choice was Shirley Temple.

When Fox refused to loan the Oz-obsessed Temple to MGM—an apocryphal Oz legend has it Jean Harlow's death made impossible a three-actor deal involving the late star, Clark Gable and Temple—the role went to Garland. Perhaps indicative of the studio's initial preference for Temple is the fact that Garland was fitted with a blonde wig before her auburn locks were allowed on-screen by George Cukor, one of *The Wizard of Oz*'s earlier directors. In retrospect, it's impossible to picture anyone but Garland opening Dorothy's doorway to the color-soaked world of Oz.

Carried on the back of Garland's sprightly portrayal, *The Wizard of Oz* went from a phenomenon of children's literature to a sensation that would net Garland an Academy Juvenile Award—which she called a "munchkin" Oscar. More importantly, 50 years after her death, Garland is still recognizable across the globe as our guide through the Land of Oz. It's rare that a lead character can end someone's life in the first act and still be universally adored, but in the 80 years since *The Wizard of Oz*'s release, Dorothy Gale has become our quintessential witch-killer, and Judy Garland our quintessential Dorothy Gale.

And Toto Too

Born in 1933, Terry, who played the role of Toto, was one of *The Wizard of Oz*'s youngest performers—in human years. The German World War I vet who took Terry in had trained military canines during his service, and his innovative hand-signal training system made Terry Hollywood's favorite pooch.

The Wizard of Oz • 25



Meet the Cast

The people who brought the magical Land of Oz to life cemented their place in cinema history.

AT THE EMERALD GATES
Toto, the Tin Man, the Cowardly Lion, Dorothy and the Scarecrow knock on the door to Emerald City, only to be told nobody gets in to see the wizard. Scholars believe that the city was inspired by Judy Garland's...


BIOPIC PREVIEW
Renée Zellweger as Judy Garland in *Judy* (2019).

LIFE OF A LEGEND

Renée Zellweger as Judy

In *Judy*, the acclaimed actor brings Judy Garland back to life for a new generation of fans.

EVERYBODY felt that [Judy Garland] was talking to them personally," Renée Zellweger told *Town and Country* magazine. "That she somehow related to their pain.... The combination of gifts that she was born with are just indescribably important in terms of what she inspires in other artists." And as reviews of *Judy* continue to excite fans and critics, it seems Zellweger has repaid the favor, inhabiting Garland's pain with her own combination of gifts. Zellweger does her own singing for the biopic, in theaters September 27.

The Wizard of Oz • 26

Follow the Yellow Brick Road to
ONNEWSSTANDSNOW.COM