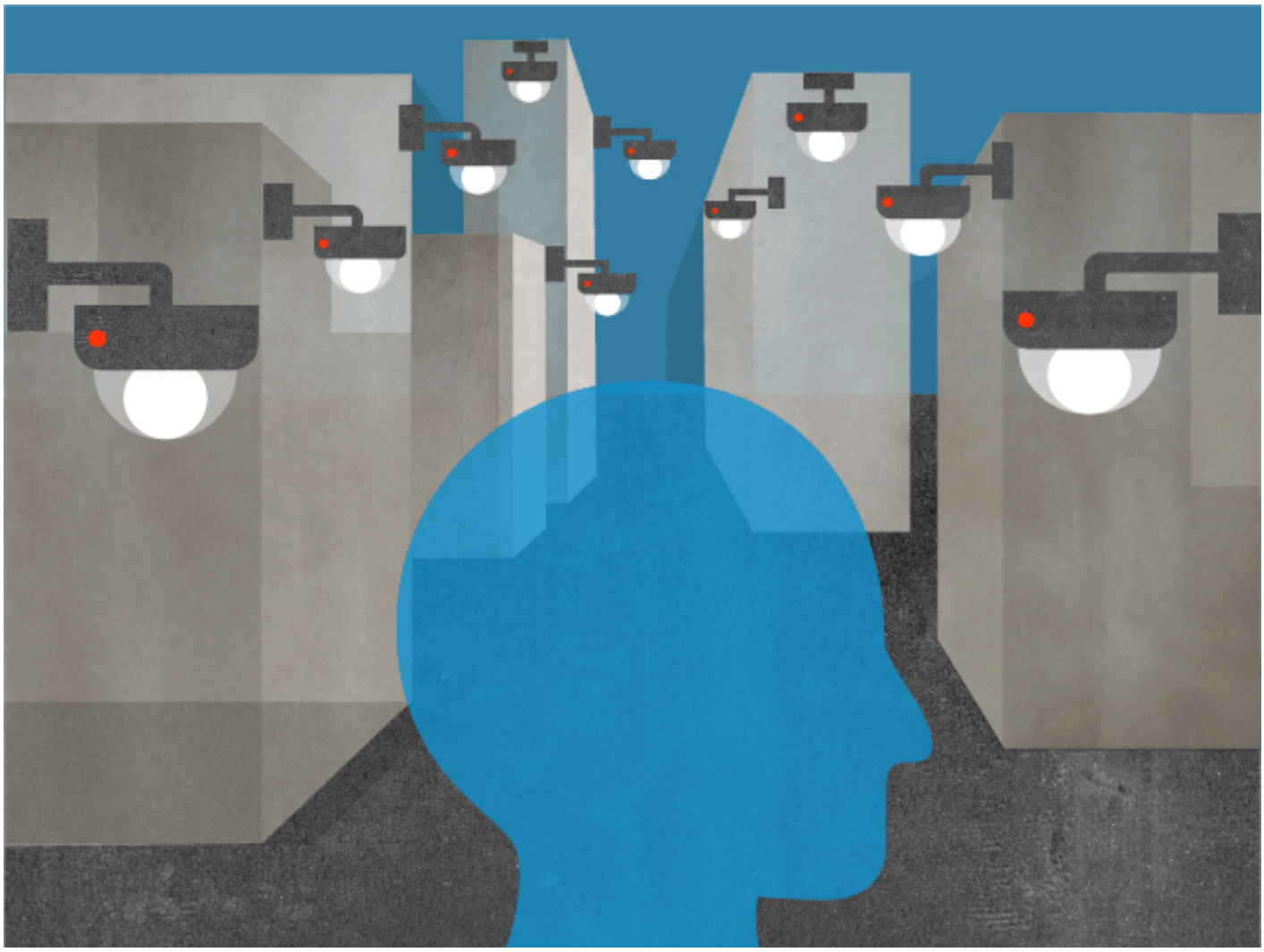
THE NEW YORKER

SHOULD WE BE WORRIED ABOUT COMPUTERIZED FACIAL RECOGNITION?

The technology could revolutionize policing, medicine, even agriculture—but its applications can easily be weaponized.

By David Owen



Many U.S. cities won't disclose their police departments' surveillance methods. Illustration by Chad Hagen

Stephen Lawlor and David Hunt have witnessed a lot of bullying. Among the principal victims, in their experience, are young, first-time mothers, who are sometimes so intimidated that they're unable to eat. Isolating their tormentors in a separate group isn't a solution, Hunt told me: "They just knock the crap out of each other."

The bullies and victims we were discussing are cows. Lawlor milks about three hundred Holsteins on a farm in County Meath, Ireland, an hour northwest of Dublin. The farm has been in his family for four generations; his calf barn, which is long and narrow and made of primeval-looking gray stone, was a horse stable in his grandfather's time. He, Hunt, and I were standing in a more recent structure a few feet away, a hangar-size cowshed with a corrugated-metal roof. Directly in front of us, a cow that weighed maybe seventeen hundred pounds was using her anvil-shaped head to push a smaller cow away from a pile of bright-green grass, which had been cut that morning and heaped on the floor. For Lawlor, this was an act with economic consequences. A mature lactating Holstein will eat well over a hundred pounds of grass and other feed in a day, and produce about nine gallons of milk. Immature cows yield less to begin with, and their output falls further if they have trouble reaching their food.

It was partly in the hope of resolving this issue that Lawlor had engaged Hunt's company, Cainthus, an artificial-intelligence startup based in Dublin. Hunt, the company's president, describes its specialty as "facial recognition for cows"; it uses surveillance cameras, computer vision, and predictive imaging to track animals and analyze their behavior. Not long before my visit, a crew had installed cameras on slender aluminum beams several feet above Lawlor's feed areas and water troughs. (The installers had learned from experience to mount the cameras higher than cows can reach with their tongues.) Price competition has put pressure on farmers in many countries to enlarge their herds and increase their output, even as their children are deciding they'd rather work for Google. Lawlor's next big farm-equipment purchase, he said, is likely to be a robot.

Cainthus's chief financial officer is David Hunt's fraternal twin, Ross. They're thirty-six years old. They grew up in a tiny farming community in Connemara, near the country's west coast, and for a long time they were the only people they knew whose family owned a personal computer. After college, they held jobs in business and finance. When they were in their late twenties, they went to work for their father's grain company (first Ross, then David) and, with their father's encouragement, quickly took it over. They

replaced its ancient trading software with a cloud-based system that they designed, and they proved that speculating in grain futures, which the company's traders had always believed to be a source of profit, was a consistent money loser. In two and a half years, the company's annual revenue roughly doubled. Then they got bored and left (first David, then Ross). They attended a Silicon Valley incubator started by Peter Diamandis and Ray Kurzweil, and founded Cainthus in 2016, with a third partner, Robin Johnston, who had grown up around dairy farms in Canada and later helped to develop computer-vision systems. The company's name comes from the word for the corner of an eye, "canthus"; the added "i" creates a mild internal pun on the abbreviation of "artificial intelligence." Ross said, "If you want to Google well, invent your name."

"Agriculture is the least digitized industry in the world right now," David told me. He and his brother believe that artificial intelligence can reduce the environmental impact of food production, by making it more efficient, and can also make it more humane. Cainthus's first outside investor was Aidan Connolly, the director of innovation at Alltech, an American agricultural-technology company, who told me that he believes Cainthus "will change the world." One way it will do that, he said, is by enabling farmers with large herds to know as much about the behavior of individual cows as farmers with small herds do. In January, the global food conglomerate Cargill became a significant minority shareholder in Cainthus, and also a development partner. During the week I was in Ireland, Cainthus was installing five dairy-farm systems in addition to Lawlor's: three in Canada and two in Italy.

The Hunts' long-term ambitions don't necessarily end at agriculture. "Anytime I talk about doing something with bovines, I'm painfully aware of how transferrable that is," David said. Working with animals gives Cainthus a research advantage over facial-recognition companies focussing on people, he said, because cows don't hide behind hats, sunglasses, or clothes, and they don't object if you spy on them, and you can interfere at will with their behavior. ("Don't mess with the mammal whose fight-or-flight response involves lawyers," he said.) "A number of years from now, we will have a difficult decision to make," he continued. "All the core competencies we've built up on cows—at what point do we transition them to humans?" The company's goals involve not merely identifying individuals but closely analyzing their behavior. Potential applications, in his view, include helping professional athletes train more effectively and diagnosing illnesses before their sufferers notice symptoms, but it's easy to imagine less

benign uses. “If you put it in the wrong hands, facial-recognition technology is a dangerous tool,” he said. “If you don’t feel incredibly threatened the first time you hear about it, you don’t understand what it is.”

One afternoon twenty years ago, I was walking on the Upper East Side and barely paying attention to where I was going. Suddenly, I realized that a person who’d just passed me on the sidewalk had seemed kind of familiar. I stopped, thought for a moment, and hollered, “Wilson!” He turned around. It was a guy I’d gone to high school with. He’d never been one of my close friends, I hadn’t seen him in more than twenty years, he’d lost most of his hair and grown a beard, I had no reason to think he’d be in New York, and I’d only glimpsed him as he walked past. Yet somehow I’d known who he was.

Putting names to faces, like formulating conspiracy theories, relies on pattern recognition. Some people are remarkably bad at it, and have trouble recognizing their spouses, their children, and even themselves in photographs. And some people are remarkably good at it. When, in September, Scotland Yard charged two suspects in the poisoning of the former Russian spy Sergei Skripal and his daughter, its investigative team included so-called “super recognizers,” who have a preternatural talent for noticing and remembering facial features and other distinguishing characteristics. Most people fall between those extremes: we’re occasional Wilson-spotters who nevertheless don’t believe our wives when they tell us that the actor who played the con artist in “American Hustle” is the same actor who played the F.B.I. agent in “Public Enemies.”

In the late sixties and early seventies, computer scientists began trying to use a digital form of pattern recognition to identify faces in photographs. The first challenge was programming a computer simply to determine whether a given image contained a face. Harder still, years later, was identifying people in images that weren't composed like mug shots; in one technique, scientists had to create digital three-dimensional models of the human head so that they could "normalize" photographs that hadn't been taken face on. A major advance occurred two decades ago, with the introduction of the first graphics-processing units (G.P.U.s) for desktop computers. The original market was gamers, but the devices were so fast at handling certain kinds of repetitive calculations that artificial-intelligence researchers rapidly made use of them as well.

Almost all current facial-recognition systems employ what are known as artificial neural networks. They aren't programmed, in the old-fashioned sense. If you're using one to recognize faces, you don't write lines of code related to things like hair color and nose length; instead, you "train" the neural network, by repeatedly giving it large numbers of labelled examples and counterexamples—"cow"; "not cow"—which it compares, beginning at the pixel level. This process is guided by humans, who tweak various parameters when the neural networks make mistakes, but to an unnerving degree the algorithms, not their creators, determine which similarities and differences are

significant and which are not. For that reason, neural networks are sometimes referred to as "black boxes."

Recently, I visited the Computer Vision Lab at the University of Massachusetts at Amherst. I found a parking space across from the Computer Science Department, but before I could leave my car I had to download an app and enroll in something called ParkMobile. I made so many mistakes while entering my credit-card number that I kept wishing Google would simply check my face through the windshield and withdraw the stupid three dollars and sixty-three cents from my checking account. Finally, I sorted things out, and found the office of Erik Learned-Miller, one of the lab's two directors. He's in his early fifties, and has worked on computer vision for two decades; he has so much faith in humanity that he shares his passwords with students and doesn't lock his bicycle or his car. We sat in the building's lounge, and he told me that several transformative developments in his field had occurred during the past dozen years. One was the sudden availability of enormous databases of useful images. He said, "Suppose it's the nineteen-eighties and somebody comes to you from the future and says, 'Here's a neural-network design that will work great for face recognition. You just need a million pairs of faces, for training.' And you would say, 'That's great, but I can't get a million pairs of faces.' Well, today you can just scrape them off the Internet."

Another breakthrough was the creation of an economical method of appending the correct identity to each image in a large database. This was made possible, he said, by services like Amazon Mechanical Turk, through which people known as Turkers sign up to perform tiny, repetitive tasks that humans still do better than computers, for as little as a penny a task. (Cainthus uses a somewhat more upscale service: a dedicated team of cow identifiers at CloudFactory, an outsourcing company in Nepal.) Learned-Miller took advantage of these new capabilities in 2007, when he and several collaborators created a database that they called Labeled Faces in the Wild; it became a benchmarking tool for facial-recognition researchers all over the world, including those at Facebook, Google, and the Chinese conglomerate Tencent. An even bigger breakthrough, he said, involved roughly simultaneous improvements in G.P.U.s, computers, and neural networks. All these elements came together in 2012, and later made possible such innovations as Apple's Face ID, Tesla's Autopilot, and so-called "deep learning."

MORE FROM THIS ISSUE
DECEMBER 17, 2018

PROFILES

Julia Louis-Dreyfus Acts Out

By Ariel Levy

DANCING

The Ailey Company's New Artist-in-Residence, Rennie Harris, Stops Short of Salvation

By Joan Acocella

SECOND ACTS DEPT.

Wayne Kramer and the Meaning of Punk

By Nick Paumgarten

SHOUTS &

"The R
Rules if
Dating

By Blythe

A few days after my trip to UMass, I visited I.B.M.'s Thomas J. Watson Research Center, in Yorktown Heights, New York. John R. Smith, the center's manager of artificial-intelligence technology, told me that, in 2016, he'd been part of a team at I.B.M. that helped to create a computer-vision system for detecting malignant melanoma, a potentially lethal form of skin cancer. Dermatologists usually look for symptoms described by an alphabetical mnemonic: Asymmetrical shape, uneven Border, variety of Color, largish Diameter, and Evolution over time. I.B.M. ignored all that, Smith said, and instead created a database of labelled images of malignant and nonmalignant lesions, then gave that database to deep-learning researchers, who used it to train melanoma-recognition algorithms. "The reason we do it that way is that we get better performance when we don't inject suboptimal human features," he said. When the algorithms were tested against the diagnoses of expert dermatologists, the algorithms consistently made fewer mistakes.

Smith also showed me video compilations created by one of I.B.M.'s "multimodal" recognition systems, which is able to automatically generate highlight reels from raw

sports footage by analyzing things like crowd cheers, announcer excitement, fist pumps, high fives, and the location of the three-point-shot line. The company's researchers used a version of the system on tennis matches at the 2017 U.S. Open; it worked flawlessly, Smith said, except with one player, who appeared to the computer to be pumping her fist when she was actually just wiping her face with a towel. "So we had to go in and retrain the system," he said.

Cainthus's headquarters is a rented workspace at Dogpatch Labs, a "curated startup hub" in a former tobacco, tea, and spirits warehouse on Dublin's Custom House Quay. The building is situated near the western end of the city's Silicon Docks area, which extends for more than a mile along both banks of the River Liffey and houses the European offices of many technology companies. Cainthus occupies a cheerful glass-and-exposed-brick box on the ground floor. When I visited, the office contained two dozen white desks (Ross's sitting, David's standing), as well as computers, freshly unboxed Dell PowerEdge rack servers, piles of tangled cables, and a small round bed for Ross's dog. I sat at Ross's desk and put on a pair of virtual-reality goggles. With them on, I could explore a cowshed like the one I'd visited at Stephen Lawlor's farm. These goggles were just for demonstrations—the cows I was looking at were recorded—but a future version will show real-time imagery overlaid with data linked to individual animals, enabling farmers to minutely monitor the health, eating and drinking habits, and inter-cow behavior of their herds, all without having to interfere with their lives.

Standing at a desk at the far end of the room was Jane Cummings, who is Cainthus's head of product science. She grew up in Brooklyn, earned a Ph.D. in high-energy physics from Yale, and spent five years smashing subatomic particles at CERN's Large Hadron Collider, in Switzerland. She is now a student of cow behavior. She and her team were about to meet with Martin Kavanagh, a former large-animal veterinarian, who grew up on a small farm in County Tipperary and now works as a consultant. (His firm is Cow Solutions.) Kavanagh told me, "Cows are slow-moving prey animals, and as a result they are incredibly stoic—because if they show pain they're going to be killed first." Cows regard humans as threats—with good reason—and they are adept at concealing injuries and illnesses. "By the time we see cows in pain as we perceive it, they may have endured a lot already," Kavanagh continued. "So, if we have a system that looks at them when they aren't afraid, we may see the pain sooner." David Hunt said, "One of the joys of facial recognition is that we can see cows' natural behavior, instead

of 'Uh-oh, girls, calm down, don't make eye contact with the predator.' " Once the company's algorithms have been fully trained, a farmer won't have to be present even to know that a cow is about to calve—something that happens on Lawlor's farm an average of once a day.

In 2016, Joy Buolamwini, a researcher at the M.I.T. Media Lab, gave a TEDx talk in Boston. Buolamwini is black. In her presentation, she played a video showing that a common facial-recognition algorithm didn't even recognize her face as a face—until she covered it with a featureless white plastic mask. (The same thing happened to her in college, when she had to "borrow" a white roommate to complete an artificial-intelligence assignment.) Computer-vision algorithms, she explained, inevitably recapitulate the conscious and unconscious biases of the people who create and train them, a defect that she calls the "coded gaze." I spoke with her recently. "There's an assumption of machine neutrality," she said. "And there's actually a hope that the technology we create will be less biased than we are. But we don't equip these systems to overcome our prejudices." Gender Shades, a project she directed at M.I.T., showed that dark-skinned females are far more likely than light-skinned males to be misidentified by commercial facial-analysis systems. She has founded the Algorithmic Justice League, which employs multiple approaches to identifying and eliminating biases in artificial intelligence, and, with a grant from the Ford Foundation, she created "A.I., Ain't I a Woman?," a poetic multimedia presentation.

In 2012, the New York Police Department implemented what it calls the Domain Awareness System, which it developed in partnership with Microsoft (and from which it earns a royalty when other cities adopt it). The system uses thousands of public-facing surveillance cameras, including many owned by private businesses. One afternoon in September, I sat on a bench in front of One Police Plaza, the N.Y.P.D.'s headquarters, with Clare Garvie, who is a senior associate at the Center on Privacy and Technology, at Georgetown Law School, in Washington. From where we were sitting, I could see two cops in a brick security booth. Like most bored people nowadays, they were staring at their phones, but their inattention didn't matter, because the plaza was being watched by a dozen or so building-mounted cameras, most of which looked like larger versions of the ones that Cainthus uses on cows: dark domes that resembled light fixtures. I asked Garvie what the police were doing with whatever the cameras were recording, and she said there was no way to know.

“The N.Y.P.D. has resisted our efforts to get any information about their technology,” she said. It was only after the center sued the department that it began to receive documents that it had initially requested more than two years earlier. By contrast, San Diego publishes reports on the facial-recognition system used by its police and holds public meetings about it. Last year, the Seattle City Council passed a comprehensive ordinance requiring disclosure of the city’s surveillance technologies; this year, it voted to physically dismantle a network of video cameras and cell-phone trackers, installed in 2013, that was like a smaller version of the Domain Awareness System. But most big cities don’t reveal much about what they’re up to, and no federal law requires them to do so. Chicago and Los Angeles are as secretive as New York, and have put off attempts by Garvie’s group, the American Civil Liberties Union, and other organizations to learn more.

Garvie is thirty-one. She majored in political science and human rights at Barnard, earned a law degree at Georgetown, and stayed on, after graduation, as a law fellow. In 2016, she was the lead author of “The Perpetual Line-Up: Unregulated Police Face Recognition in America,” a study whose title refers to the fact that many states allow police departments to search their databases of mug shots and driver’s-license photos. Garvie doesn’t doubt that facial recognition has legitimate uses in law enforcement, just as wiretaps and personal searches do. But misuse is inevitable. “Right now, quite literally, there’s no such thing as face-recognition abuse, in one sense, because there are really no laws governing its use by police,” she said. If your face appears in an accessible database, as it probably does, you’re effectively a suspect every time it’s searched. And you don’t have to be a cop to have access to the millions of photos on social-media sites—many of which are labelled automatically. (This is less of a threat to happen in Canada and Europe, where comprehensive privacy laws have prevented social-media sites from even offering automated photo-tagging.) Garvie and her colleagues have written a fourteen-page model bill intended to regulate the use of facial-recognition technology in law enforcement. Among many other things, it would require the custodians of arrest-photo databases to regularly purge images of people who are not later convicted of whatever act it was that prompted their arrest. Their first version of the bill was published in 2016; no legislature has adopted it.

People who have grown up with smartphones and social media may think that the very concept of personal privacy has become quaintly irrelevant, but there are reasons for

even habitual oversharers to be alarmed. Faces, unlike fingerprints or iris patterns, can easily be recorded without the knowledge of the people they belong to, and that means that facial recognition can be used for remote surveillance. "We would be horrified if law-enforcement agents were to walk through a protest demanding that everybody show their identification," Garvie said. "Yet that's what face recognition enables." Computer-vision systems potentially allow cops and employers to track behaviors and activities that are none of their business, such as where you hang out after work, which fund-raisers you attend, and what that slight tremor in your hand (recorded by the camera in the elevator that you ride to your office every morning) portends about the size of your future medical claims. In October, Tim Cook, the C.E.O. of Apple, while speaking at a privacy conference in Brussels, said, "Our own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency."

In May, forty-one nonprofit organizations, including the A.C.L.U. and the Electronic Frontier Foundation, sent an open letter to Jeff Bezos, Amazon's C.E.O., requesting that the company stop selling its facial-recognition system, called Rekognition, to governments and government agencies. Two months after the letter was sent, the A.C.L.U. conducted a test, in which Rekognition erroneously matched twenty-eight members of Congress with individuals in a database of twenty-five thousand publicly available mug shots. The matches included a disproportionate number of members of the Congressional Black Caucus—a clear example of the coded gaze. Amazon objected that the A.C.L.U. had set its "confidence thresholds," which represent the probability that a given match is correct, at a level lower than the company recommends for law-enforcement searches. But, even so, there is no law that prevents police departments from doing the same thing. A recent investigation by the British civil-liberties group Big Brother Watch found that the automated facial-recognition system used by the Metropolitan Police Service, in Greater London, had a false-positive rate of ninety-eight per cent, and that the police retained images of thousands of innocent citizens, for future searches.

A man who helped to develop the N.Y.P.D.'s facial-recognition system has said that when he was with the police department he enhanced surveillance photos by, for example, using Photoshop to replace suspects' closed eyes with other people's open eyes, creating what he once called "a second opportunity to return a match." Garvie told me,

“Eyes are incredibly important to a face identification, and here they were using someone else’s. It’s like taking half of a latent fingerprint and drawing in the rest.”

Both Garvie and Buolamwini believe that some uses, such as the incorporation of real-time facial identification into police body cameras, should be banned entirely. Body cams have generally been viewed as a valuable check on violence by cops—and as a backup for cops who’ve been wrongly accused—but the dangers are huge, they said. Garvie told me, “In most face-recognition systems that exist today, there is a human analyst somewhere who is given time to look at the photos and determine whether they represent a similar individual. But with body cams the technology itself becomes the final arbiter. An alert goes into a headset or a mobile device, and an officer with a gun has a moment to decide whether or not there is a threat to public safety.” Last year, Axon—the leading manufacturer of body cams, formerly known as Taser International—bought Dextro and Misfit, two startups in computer vision and artificial intelligence. In April, the Algorithmic Justice League and the Center on Privacy and Technology were among the signers of an open letter to Axon’s artificial-intelligence ethics board, urging, among other things, that the company not include real-time facial recognition in its body cams. Buolamwini told me, “Decisions to end lives are too precarious to be left to artificial intelligence. And, given what we know about the current state of the technology, it’s absolutely irresponsible.”

Using computer vision to identify an individual cow in a farmer’s herd is much easier and more reliable than using it to identify an unknown human in a surveillance photograph. One reason is that, in the case of the cow, the farmer knows for certain that a perfect match exists in the farm’s database. There is also more than one way to visually identify a cow. Cainthus identifies animals by distinctive markings, tufts, and swirls in the pelt on their faces and bodies, and it’s able to confirm its matches whenever its cameras pick up the numbered identification tag that’s attached to every animal’s ear. (Humans have distinctive pelts, too, sort of, but we largely conceal them under clothes.) No single element is visible at all times, but each one helps to confirm the others, enabling the system to double-check its identifications and to track animals even when their faces and bodies are partially obscured. Cainthus hopes someday to identify animals also by their gait, a trait that’s as individual as a face.

China has nearly two hundred million public-surveillance cameras, far more than any other country. In 2015, it announced plans to build an integrated human-monitoring

system, with the goal, according to the Washington *Post*, of making the cameras "omnipresent, fully networked, always working and fully controllable" by 2020. The reliable real-time identification of more than a billion people by their faces alone is not possible yet, but the Chinese system doesn't depend on faces alone. Erik Learned-Miller, of UMass, told me, "Let's assume you're a Chinese citizen and your home address is registered with the government. So when they see a person in Xi'an who looks like you, and they know you live in Xi'an, they'll probably guess it's you. And if they're also tracking your cell phone and they know that twenty minutes ago you were in a restaurant nearby—now it's almost certainly you." Cell-phone signals and digital financial transactions, which in China are highly centralized, are the human-surveillance equivalent of bovine ear tags: they're supplemental identifiers that increase the reliability of facial matches. "The Chinese are integrating massively," Learned-Miller continued. "They can say, 'Hey, we recognized this guy in a Starbucks this morning, and now he's in a McDonald's—he is getting too American, let's bring him in.' "

By the time China's surveillance system is fully implemented, it will include mandatory "social credit" ratings, which score individuals' general worthiness based on factors such as what they buy (too much alcohol?), what they do with their free time (too many video games?), and whom they hang out with online (too many low-rated social parasites?). A voluntary version of the rating system is already in place. People with high scores are given opportunities that others don't receive, including access to jobs, loans, and travel. And virtual ear tags are proliferating. The N.Y.P.D. reads and records the license plates of many vehicles that enter and leave the city. Google knows everywhere I've been with my phone. China has begun employing its own gait-recognition technology, which its developer has said can't be fooled by "limping, walking with splayed feet, or hunching over."

Americans may believe that we would never tolerate the installation of millions of surveillance cameras, but the Hunts told me that we wouldn't necessarily know it was happening. Ross Hunt said, "I want autonomous driving to be a thing, but if you have autonomous-car ubiquity you have the Internet of Eyes everywhere, because on an autonomous car there are cameras all the way around." Self-driving vehicles use their cameras to identify and avoid obstacles, but any camera that sees its surroundings also sees every person it passes. Many electric vehicles record location and driving data

continuously and periodically upload that information to their manufacturers; China now requires all such vehicles operating in the country to transmit the same information to government monitors. Ross went on, "That's today. So, if they already have your telemetry, how long will it be until they also have the imagery? It's just a bandwidth issue."

Facial-recognition technology is advancing faster than the people who worry about it have been able to think of ways to manage it. Indeed, in any number of fields the gap between what scientists are up to and what nonscientists understand about it is almost certainly greater now than it has been at any time since the Manhattan Project. Learned-Miller told me that he now frequently confers with Buolamwini, whom he met at a conference, and that because of her he has become more involved in issues of transparency and fairness. But he's still advancing the state of the art. A few weeks before my visit, he received a big grant from the Department of Defense—historically one of the biggest funders of facial-recognition research—for a project involving "visual common sense," which has to do with teaching computers to be more humanlike in their problem-solving.

He had also just presented a paper at the European Conference on Computer Vision, in Munich, about a simple method that he and several other scientists, including three of his students, had devised, by which neural networks can catch and correct their own errors. On the monitor on his desk, he showed me a PowerPoint slide that included three consecutive frames from the movie "Hannah and Her Sisters." In each frame, an automatic face-detection tool had correctly drawn a box around the face of Barbara Hershey. But in the middle frame it had incorrectly also drawn a box around the right hand of Maureen O'Sullivan, who was talking to Hershey with her back to the camera. (Learned-Miller said that, when a computer misidentifies something as a face, surprisingly often the thing that fools it is a hand.) The paper explained that a detection algorithm can eliminate such errors by comparing consecutive video frames and rejecting putative faces that appear suddenly, as if from nowhere, and immediately disappear. The rejected faces then become training counterexamples, and increase the detector's ability to avoid similar false positives in the future. "This is what gets me excited, because it's automatically improving the algorithm with no human intervention," he said. "But it's also creepy: 'Hi, Dave. My name is HAL. How are you doing? I got smarter overnight.' " ♦

This article appears in the print edition of the December 17, 2018, issue, with the headline "Here's Looking at You."

David Owen is a staff writer and the author of "Where the Water Goes: Life and Death Along the Colorado River," based on his article "Where the River Runs Dry," which appeared in the May 25, 2015, issue of the magazine. Read more »