SPECIAL ISSUE: WILL TECHNOLOGY KILL PRIVACY?

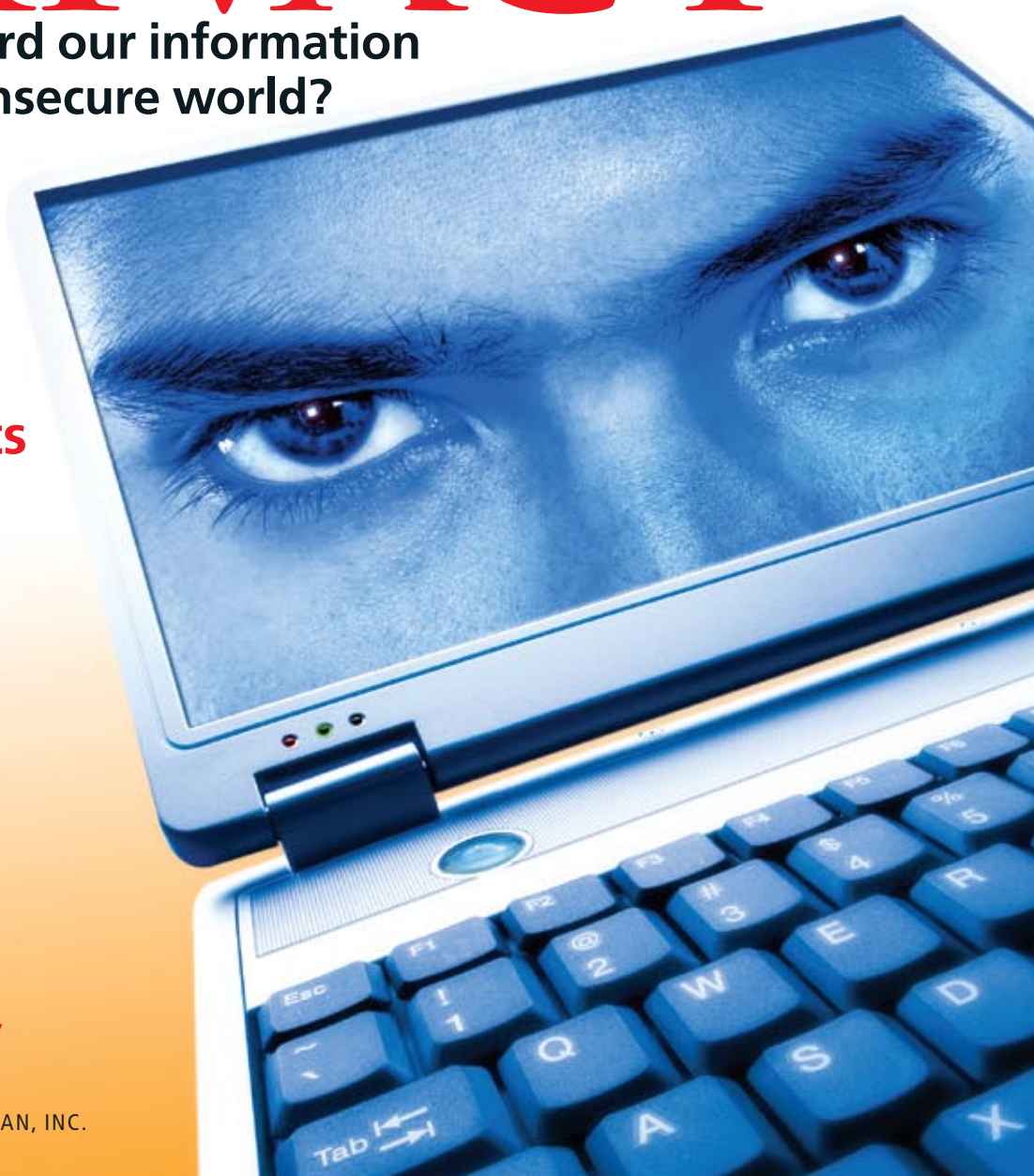
SCIENTIFIC AMERICAN

Bug-Bots and Other **Spy Gadgets**
page 70

September 2008 $4.99 www.SciAm.com

THE FUTURE OF PRIVACY

Can we safeguard our information in a high-tech, insecure world?



Internet-Age **Wiretapping**

Cryptography for **Keeping Secrets**

You Are Tagged: **RFID Chips**

Beyond Fingerprints: **Biometric I.D.**

Privacy in a **Facebook Age**

Defending Genetic **Confidentiality**

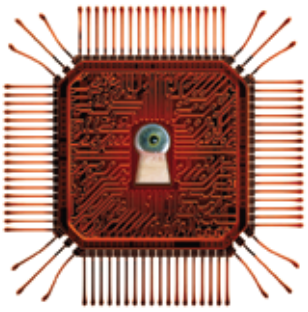
Page Intentionally Blank

SCIENTIFIC AMERICAN September 2008 ■ Volume 299 Number 3

SPECIAL ISSUE

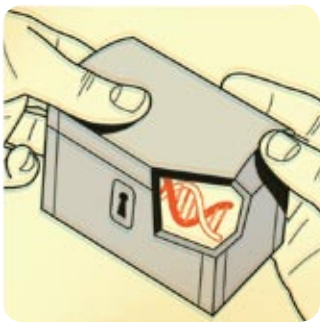
THE FUTURE OF PRIVACY

KENN BROWN



46

56



64

70

ON THE COVER

Advancing technologies will bring many benefits, but we may lose control over who learns our secrets in the process. Is that bad?
Image by Kenn Brown, Mondolithic Studios.

MORE FEATURES

GO TO SCIAM.COM

FOCUS ON CHINA ▼

Our multimedia coverage looks at the country that now leads the world in emitting greenhouse gases. With reports on Yangtze River power, China's first carbon-neutral city, and more.
Also: Doping at the Olympics.

DAVID BIELLO

More at **www.SciAm.com/sep2008**

In-Depth Report: Technology and Privacy
Cyberterrorism, Online Predators, Electronic Voting, and More
Read, listen to and interact with exclusive digital features complementing this print issue on "The Future of Privacy." Goes online August 18.

Feature
Musicophobia: When Your Favorite Song Gives You Seizures
A woman exhibits a rare kind of epilepsy triggered by music.

Fact or Fiction
Men Have a Biological Clock
Does male fertility have an expiration date?

Podcast
Astrophysicist J. Richard Gott on Time Travel
The Princeton University scientist discusses the realities and speculations of voyaging through the fourth dimension.

Scientific American (ISSN 0036-8733), published monthly by Scientific American, Inc., 415 Madison Avenue, New York, N.Y. 10017-1111.

Periodicals postage paid at New York, N.Y., and at additional mailing offices. Canada Post International Publications Mail (Canadian Distribution) Sales Agreement No. 40012504. Canadian BN No. 127387652RT; QST No. Q1015332537. Publication Mail Agreement #40012504. Return undeliverable mail to Scientific American, P.O. Box 819, Stn Main, Markham, ON L3P 8A2. Subscription rates: one year $34.97, Canada $49 USD, International $55 USD. Postmaster: Send address changes to Scientific American, Box 3187, Harlan, Iowa 51537. **Reprints available:** write Reprint Department, Scientific American, Inc., 415 Madison Avenue, New York, N.Y. 10017-1111; (212) 451-8877; fax: (212) 355-0408. **Subscription inquiries: U.S. and Canada (800) 333-1199; other (515) 248-7684. Send e-mail to sacust@sciam.com** Printed in U.S.A.

DEPARTMENTS

37


40


14


16


108

DAN LAMONT


116

Here in the Fishbowl

How much do technologies that affect privacy also influence freedom?

Once upon a time an ethicist had a brilliant idea for a prison. Today we all live in it.

Starting in 1785, English philosopher Jeremy Bentham spent decades (and much of his own fortune) advocating for the construction of a facility he called the Panopticon—the "all-seeing place." Inside its walls, convicted prisoners would be exposed to perpetual view from a central tower by an unseen jailer, who could supervise their behavior, health and menial labor. Bentham insisted that the Panopticon would be safer and more affordable than other prisons—but not because the prisoners were always being watched. Rather the true genius of the idea lay in what made it, in his words, "a new mode of obtaining power of mind over mind." Because the prisoners would not be able to see whether a guard was in the Panopticon's tower, it could often be unmanned and they would never know. Out of fear and uncertainty, the prisoners would in effect stand watch over themselves.

The British government never approved final construction of a Panopticon, despite Bentham's fervent lobbying (at one point he promised to serve as the guard at no wages). Instead, ironically, over recent decades London itself has become one of the most intensively monitored metropolises in the world, with more than 10,000 public security cameras and a far greater number of private ones installed by landlords, shopkeepers and homeowners.

Surveillance is everywhere. A 1998 survey counted almost 2,400 public and private cameras in Manhattan, and that number has surely skyrocketed since then as the cost of video has fallen. The U.S. Department of Homeland Security has distributed hundreds of millions of dollars to cities in grants for cameras to fight terrorism. The available evidence that all this monitoring actually improves security, at least against street crime, is at best thin, however.

Video surveillance is only the tip of the iceberg. As the articles in this special issue describe, the rise of assorted technologies has multiplied manyfold the opportunities for us to share data about ourselves—or for others to spy on us.

In his book *The Transparent Society,* David Brin argues that the modern conception of privacy is historically transient and made obsolete by new technology; rather than trying futilely to keep secrets, he thinks we should concentrate on preventing abuses of them by insisting that everyone, including governments, be an equally open book. How well that strategy can work in practice is debatable. But there is no question that society is, however unwarily, embracing much of the new openness. Millions now post their lives on Facebook and MySpace for all to see. Companies successfully entreat customers to divulge personal information in return for services. In 1948 George Orwell portrayed an all-knowing Big Brother as a totalitarian nightmare. Sixty years later *Big Brother* is reality TV entertainment.

Those developments are not altogether bad. What should concern us most is not whether the changing state of privacy is making us more or less safe or happy. It is whether, as Bentham predicted, it subjects us to a new "power of mind over mind." Does uncertainty about whether someone is observing us, exploiting our secrets or even stealing our identity cause us to preemptively sacrifice our freedom to be and act as we would wish? When privacy disappears, do we first respond by hiding from ourselves? ■

JOHN RENNIE
editor in chief

FLYNN LARSEN (*Rennie*); KENN BROWN *Mondolithic Studios (eye at the window)*

Among Our Contributors

KATHERINE ALBRECHT
directs the consumer privacy organization CASPIAN and is the author of two books abaout the rising privacy threat posed by RFID tags.

WHITFIELD DIFFIE
is chief security officer at Sun Microsystems and one of the inventors of public-key cryptography, the cornerstone of today's online security systems.

ESTHER DYSON
is a prolific author and commentator on emerging digital technologies and their cultural significance. Her book *Release 2.0* discussed online privacy in 1997.

SIMSON L. GARFINKEL
does research on computer forensics and security at the Naval Postgraduate School in Monterey, Calif., and is co-author of the textbook *Web Security & Commerce.*

ANIL K. JAIN
of Michigan State University is a professor in the departments of computer science and engineering, electrical and computer engineering, and probability and statistics.

ANNA LYSYANSKAYA
is associate professor of computer science at Brown University and contributed to the authorization protocol standards incorporated in most new microprocessors.

MARK A. ROTHSTEIN
is chair of law and medicine and director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine.

DANIEL J. SOLOVE
is a professor at George Washington University Law School and author of *The Future of Reputation* and *Understanding Privacy.*

Page Intentionally Blank

editors@SciAm.com

SCIENTIFIC AMERICAN®
Established 1845

Nuclear Recycling ▪ Snow Line ▪ Dark Energy

MAY 2008

"Continuing to discard as 'waste' 99 percent of the energy in uranium ore is clearly unsustainable."
—William H. Hannum, Gerald E. Marsh and George S. Stanford
ARGONNE NATIONAL LABORATORY

Risky Recycling?

In "Rethinking Nuclear Fuel Recycling," Frank N. von Hippel describes why he would like nuclear reprocessing to go away, but it won't. Nuclear power is resurging, both globally and domestically. Continuing to discard as "waste" 99 percent of the energy in uranium ore is clearly unsustainable.

The technology is spreading inexorably, increasing its potential to be subverted for weapons production. To minimize that risk, fuel processing must be done under international auspices—with ironclad guarantees that nations will have uninterrupted access to fuel if they forgo their own enrichment and reprocessing facilities.

Von Hippel is correct that using MOX (plutonium oxide mixed with uranium oxide) to cycle plutonium back into today's "thermal" reactors is expensive, is only marginally useful and produces plutonium of weapons-quality chemical purity. But recycling methods for advanced fast reactors are different. Such methods address resource utilization, waste and proliferation concerns (see our piece, "Smarter Use of Nuclear Waste," in the December 2005 *Scientific American*).

Technology alone cannot remove the proliferation threat. The U.S. Department of Energy's Global Nuclear Energy Partnership (GNEP) is a useful step toward sensible management, and some 21 nations have signed on so far. But without continued U.S. leadership, the GNEP will fade away. Coordination will be lost, and the technology for producing nuclear weapons materials will spread uncontrolled.

William H. Hannum, Gerald E. Marsh and George S. Stanford
Argonne National Laboratory (retired)

VON HIPPEL REPLIES: *Nuclear power could cut the growth of greenhouse emissions by up to 15 percent. Reprocessing makes nuclear power more expensive, however, and breaks down the barrier between it and nuclear weapons.*

Hannum, Marsh, Stanford and I agree that reprocessing and recycling plutonium in water-cooled reactors make neither technical nor economic sense. A dozen countries have not renewed their reprocessing contracts with France, Russia and the U.K. Having lost virtually all its foreign customers, Areva, France's reprocessing company, has not yet been able to agree on more than a one-year extension of its contract with France's nuclear power utility. And the U.K. is giving up on reprocessing altogether.

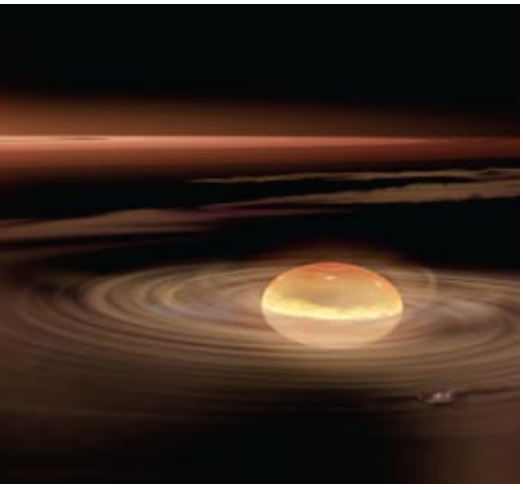
Liquid-sodium-cooled, fast-neutron reactors utilizing recycling could fission plutonium almost completely but are so expensive that no private utility will pay for one. If costs change and proliferation concerns can be dealt with, the potential energy resource in the plutonium and uranium in spent fuel will still be there. In the meantime, we must dispose of hundreds of tons of already separated plutonium that is a legacy of the cold war and premature expectations of breeder reactors. For the foreseeable future, there will be no need to separate more.

Moving Line

"The Genesis of Planets," by Douglas N. C. Lin, describes how, in the leading planet formation theory, planets form within a

disk of gas rotating around a star. At a certain distance from the star is a "snow line" beyond which water stays frozen. I wonder about the stability of the snow line. It seems that it should move as the disk progresses. Could this be why Earth has an ocean?

Tom Brown
Gainesville, Fla.



SEQUENTIAL ACCRETION, the leading theory of planetary formation, involves a chaotic interplay among competing mechanisms, such as relocation of the snow line, that leads to a great diversity of outcomes.

LIN REPLIES: *The snow line does evolve. Because of intense irradiation by central stars and friction heating within the disk, our solar system's snow line was initially located well outside the orbit of Jupiter. It gradually propagated inward as the mass flux through the disk declined and the gas dissipated. Eventually the relocation of the snow line was more or less stalled, although the ice-vapor demarcation face may have moved back and forth over about 1 to 2 AU. This essentially covered a substantial fraction of the region between Mars and Jupiter. The parent bodies of meteorites in the asteroid region formed over several million years. During that epoch, the snow line may have intruded on regions fairly close to Mars. Consequently, the water content in the meteorites gradually increased with the distance of their parent bodies from the sun. This evolution may have promoted the acquisition of Earth's ocean.*

Cosmic Credit

David Appell errs in attributing the discovery of dark energy so completely to Saul Perlmutter's Supernova Cosmology Project (SCP) team in "Dark Forces at Work" [Insights]. The SCP made real contributions to the discovery of dark energy, but other groups had solved some of these problems earlier.

In 1988 a Danish team searched for distant supernovae using methods anticipating those of the SCP. And the program of supernova discovery for nearby objects at Cerro Tololo Inter-American Observatory in Chile formed the basis for using supernovae as distance indicators, not the robotic search Perlmutter worked on. The SCP did publish a result in July 1997 that claimed supernova observations were unlikely to be consistent with dark energy, but our High-Z Supernova Search Team developed superior methods for dealing with dust, published in 1996. With careful observation of supernovae, we were confident that we saw cosmic acceleration, which we announced in February 1998. A paper detailing our work was submitted to the *Astronomical Journal* in March 1998 and appeared in print before the SCP paper was submitted.

Everybody has a lot to be proud of, but credit should be given where it is due.

Robert P. Kirshner
Harvard University

APPELL REPLIES: *Kirshner is not entirely correct and, as a member of the High-Z team, perhaps not entirely objective. The Danish team did perform consequential early measurements, but only on one supernova and too late to obtain its peak brightness. Both the SCP and High-Z teams did important work and exchanged vital data and insights in both directions. But it is undisputed that the SCP announced its discovery first, on January 9, 1998, at a meeting of the American Astronomical Society. In Kirshner's book* The Extravagant Universe *(Princeton University Press, 2002), he describes the two teams' relationship as "getting it first" versus "getting it right."*

I am sure that history will acknowledge the contributions of both teams in the final analysis.

Letters to the Editor

Scientific American
415 Madison Ave.
New York, NY 10017-1111
or editors@SciAm.com

Letters may be edited for length and clarity. We regret that we cannot answer each one. Join the discussion of any article at www.SciAm.com/sciammag

SCIENTIFIC AMERICAN®
Established 1845

CHAIRMAN: Brian Napack
PRESIDENT: Steven Yee
VICE PRESIDENT: Frances Newburg
CHAIRMAN EMERITUS: John J. Hanley

ASSOCIATE PUBLISHER, CIRCULATION: Simon Aronin
CIRCULATION DIRECTOR: Christian Dorbandt
RENEWALS MANAGER: Karen Singer
FULFILLMENT AND DISTRIBUTION MANAGER: Rosa Davis

VICE PRESIDENT AND PUBLISHER: Bruce Brandfon
DIRECTOR, GLOBAL MEDIA SOLUTIONS: Jeremy A. Abbate
SALES DEVELOPMENT MANAGER: David Tirpack
SALES REPRESENTATIVES: Jeffrey Crennan, Stephen Dudley, Stan Schmidt

ASSOCIATE PUBLISHER, STRATEGIC PLANNING: Laura Salant
PROMOTION MANAGER: Diane Schube
RESEARCH MANAGER: Aida Dadurian
PROMOTION DESIGN MANAGER: Nancy Mongelli

VICE PRESIDENT, FINANCE, AND GENERAL MANAGER: Michael Florek
BUSINESS MANAGER: Marie Maher
MANAGER, ADVERTISING ACCOUNTING AND COORDINATION: Constance Holmes

DIRECTOR, SPECIAL PROJECTS: Barth David Schwartz

SALES REPRESENTATIVES, ONLINE: Gary Bronson, Thomas Nolan

DIRECTOR, ANCILLARY PRODUCTS: Diane McGarvey
PERMISSIONS MANAGER: Linda Hertz

How to Contact Us

SUBSCRIPTIONS
For new subscriptions, renewals, gifts, payments, and changes of address: U.S. and Canada, 800-333-1199; outside North America, 515-248-7684 or www.SciAm.com

REPRINTS
To order reprints of articles: Reprint Department, Scientific American, 415 Madison Ave., New York, NY 10017-1111; 212-451-8877, fax: 212-355-0408; reprints@SciAm.com

PERMISSIONS
For permission to copy or reuse material: Permissions Department, Scientific American, 415 Madison Ave., New York, NY 10017-1111; www.SciAm.com/permissions or 212-451-8546 for procedures. Please allow three to six weeks for processing.

ADVERTISING
www.SciAm.com has electronic contact information for sales representatives of Scientific American in all regions of the U.S. and in other countries.

DON DIXON

Scientific Creativity ▪ Wright Crash ▪ Fever Riot

Compiled by Daniel C. Schlenoff

SEPTEMBER 1958

THE CREATIVE PROCESS—"The most remarkable discovery made by scientists is science itself. The discovery must be compared in importance with the invention of cave-painting and of writing. Like these earlier human creations, science is an attempt to control our surroundings by entering into them and understanding them from inside. And like them, science has surely made a critical step in human development which cannot be reversed. We cannot conceive a future society without science. —Jacob Bronowski"

INNOVATION IN PHYSICS—"My view, the skeptical one, holds that we may be as far away from an understanding of elementary particles as Newton's successors were from quantum mechanics. Like them, we have two tremendous tasks ahead of us. One is to study and explore the mathematics of the existing theories. The existing quantum field-theories may or may not be correct, but they certainly conceal mathematical depths which will take the genius of an Euler or a Hamilton to plumb. Our second task is to press on with the exploration of the wide range of physical phenomena of which the existing theories take no account. This means pressing on with experiments in the fashionable area of particle physics. Outstanding among the areas of physics which have been left out of recent theories of elementary particles are gravitation and cosmology. —Freeman Dyson"

FITNESS—"Faced with a new mutation in an organism, or a fundamental change in its living conditions, the biologist is frequently in no position whatever to predict its future prospects. He has to wait and see. For instance, the hairy mammoth seems to have been an admirable animal, intelligent and well-accoutered. Now that it is extinct, we try to understand why it failed. I doubt that any biologist thinks he could have predicted that failure. Fitness and survival are by nature estimates of past performance. —George Wald"

[NOTE: Wald won the Nobel Prize in Physiology or Medicine in 1967.]

SEPTEMBER 1908

PASSENGER FATALITY—"Seldom has there occurred a more pitifully tragic disaster than the sudden fall of the Wright aeroplane, involving the death of that promising young officer Lieut. Thomas Selfridge, and inflicting shocking injuries on the talented inventor, Orville Wright. But although the accident is deplorable, it should not be allowed to discredit the art of aeroplane navigation. If it emphasizes the risks, there is nothing in the mishap to shake our faith in the principles upon which the Wright brothers built their machine, and achieved such brilliant success."

MACHINERY VS. MUD—the largest bucket dredger for the Suez Canal, 1908

HUGE DREDGER—"In connection with the widening and deepening of the Suez Canal at Port Said, the authorities have recently increased their dredging fleet by a new vessel, which ranks as the largest bucket dredger afloat. The 'Péluse' [*see illustration*] was built by Messrs. Lobnitz & Co. at their Renfrew yards on the Clyde River, Scotland, and is of similar design to the 'Ptolemée,' which they supplied to the canal company some two years ago. The 'Péluse' has a deck length of 305 feet, and a dredging engine of 600 horse-power. All gearing aboard the vessel has machine-cut teeth."

SEPTEMBER 1858

RUFFIANS—"Some time ago we remonstrated strongly against the course of Dr. Thompson and the Board of Health of this city [New York], for the careless manner in which infected ships were treated by them, and this journal was the first to call the public attention to their official stupidity. The consequence of their careless conduct is that yellow fever has broken out in three distinct parts of Staten Island. Since writing the above, the whole of the Quarantine buildings have been burned to the ground by a mob, and the sick left uncared for. The doctors deserve the credit of having stuck to their posts like brave men during the conflagration. We hope that the perpetrators of the wrong may be apprehended and punished, for it is no way to redress one evil to allow a ruffianly gang to take the law into their own hands."

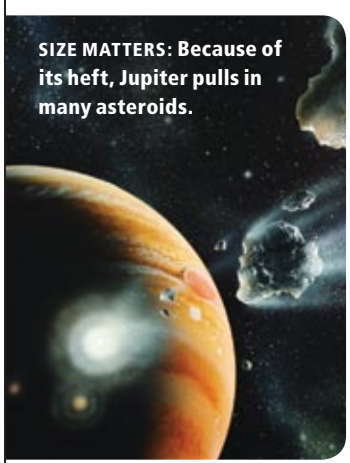
SCIENTIFIC AMERICAN, VOL. XCIX, NO. 11; SEPTEMBER 12, 1908

Jovian Protector ▪ Personal Gene Tests ▪ Anesthesia and Pain ▪ *Valdez* Payout

Edited by Philip Yam

Planetary Protection Racket

As the first planet to form in our solar system, Jupiter helped to sculpt the rest [see "The Genesis of Planets"; SciAm, May 2008]. Because of its gravity, for instance, it has regulated the rate of cosmic impacts on Earth: flinging asteroids in our direction yet also clearing many hazardous space rocks out of our way. Jupiter's net effect depends on its mass, suggest Jonathan Horner and Barrie Jones, both at the Open University in England, in an upcoming paper in the *International Journal of Astrobiology*. Had Jupiter one-fifth its mass, they calculate, it would have failed to clear asteroids out—and Earth might have been struck four times more often than it has been. But if Jupiter were still smaller, it would have flung fewer asteroids toward the inner solar system to begin with—and the dinosaurs might still be walking our planet. —*George Musser*

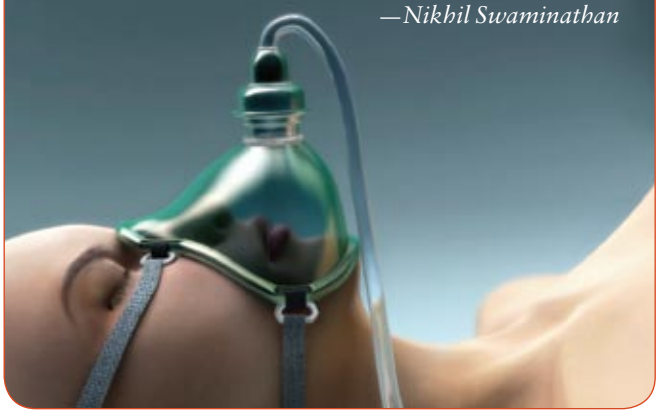


SIZE MATTERS: Because of its heft, Jupiter pulls in many asteroids.

Sleep during Surgery, Wake Up in Pain

General anesthetics knock out patients during surgery by suppressing the central nervous system [see "Lifting the Fog around Anesthesia"; SciAm, June 2007]. Researchers at Georgetown University Medical Center recently discovered that these drugs also interact with specific proteins on the surfaces of nerve cells—which could also lead to increased pain when patients wake up. Studies in mice indicated that drugs that activate the surface protein TRPA1 on pain-sensing nerve cells intensify postoperative pain. These findings could explain why some patients complain of more pain than others who undergo the same surgical procedure. In the future, anesthesiologists may be able to limit postop pain by sticking to drugs that ignore TRPA1. The work appears in the June 24 *Proceedings of the National Academy of Sciences USA*.

—*Nikhil Swaminathan*



No DNA Reading Allowed

Many researchers question the medical relevance of direct-to-consumer genetic tests, some of which are offered for as little as $1,000 [see "Taking Genomes Personally"; SciAm, May 2008]. State officials seem to concur. In June, citing the state's licensing and physician oversight rules, the California Department of Public Health sent notices to stop 13 DNA-testing labs, including 23andMe, Navigenics and deCODEme Genetics, from soliciting customers. The cease-and-desist orders follow actions by New York State, which began sending similar warnings last November. The letters are in part an effort to draw federal oversight into the nascent field, which some fear can cause patients to react inappropriately to their disease risks.

—*Philip Yam*

Prince William Sound and Fury

Controversy has surrounded studies documenting the long-term environmental effects of the *Exxon Valdez* oil spill in 1989 [see "Sounding Out Science"; SciAm, October 1996]. According to a U.S. Supreme Court decision on June 25, oil giant ExxonMobil will pay the equivalent of 24 hours' worth of petroleum sales to the people impacted by the 11 million gallons of crude oil spilled into Prince William Sound in Alaska. The ruling caps the total damages assessed to the company at $507.5 million, a fraction of the $5 billion a jury initially awarded the plaintiffs in 1994. The court majority decided that punitive damages should be limited to the level of actual damages proved—a new legal standard for maritime cases involving tanker spills. —*David Biello*

OIL IN WATER: Sea lions cling to a buoy to avoid the oil spilled by the *Exxon Valdez* in Prince William Sound in 1989.

MEDICALRF.COM (*ventilator*); KUAKO HELAVUO (*Jupiter and asteroids*); FLIP NICKLIN *Minden Pictures* (*stranded sea lions*)

ASTRONOMY

The New Radio Sky

Digital upgrades for a radio-astronomy renaissance BY MARK WOLVERTON

Bell Telephone Laboratories engineer Karl Guthe Jansky was only looking for ways to cut down on shortwave radio static when he found radio waves coming from outer space in 1932. Yet Jansky's serendipitous discovery soon gave birth to radio astronomy, which has since delivered paradigm-shifting revelations ranging from the cosmic microwave background to the presence of dark matter in the universe. That science is now on the verge of a 21st-century renaissance that promises even greater discoveries, ushered in not by traditional huge radio dishes but by vast, powerful arrays of smaller dishes.

First developed by British radio astronomers in 1946, arrays make use of several radio telescopes spaced some distance apart, "synthesizing" a single telescope with an aperture equal to the spacing between the farthest elements. The most famous example, operating since 1980, is the Very Large Array (VLA) near Socorro, N.M., which has 27 active radio antennas mounted on railroad tracks in a Y configuration (another dish is kept as a spare). The instrument's angular resolution is adjusted simply by moving the antennas closer together or farther apart. "The VLA has been and still remains the most powerful and flexible radio synthesis imaging telescope on earth," says veteran VLA researcher Rick Perley. "But since that time there's been enormous changes both in technology and in where science is headed."

DAVE FINLEY *NRAO/AUI*

GETTING ENHANCED: The Very Large Array near Socorro, N.M., maintains 28 movable dishes that are each 25 meters in diameter. Various upgrades, to be completed by 2012, will dramatically boost the array's resolution, sensitivity and data-handling ability.

In particular, the VLA is going digital as the EVLA, the Expanded Very Large Array, using more sophisticated computers and electronics that will vastly increase the resolution, sensitivity and data capacity of the facility. The heart of the EVLA, as with any array, is the correlator, the supercomputer system that processes, compares and combines the signals from the antennas. "You just don't go to RadioShack and buy a bunch of PCs and configure them for this kind of thing," explains EVLA project manager Mark McKinnon of the correlator, designed and built by a team from the National Research Council of Canada Herzberg Institute of Astrophysics in British Columbia. It will handle up to 80 times the bandwidth of the old VLA correlator and crunch many more data channels simultaneously.

Engineers also upgraded the path by which signals get from the antenna dishes to the correlator, using all-digital fiber optics that replace the old analog waveguides. The dishes are getting new, exquisitely sensitive digital receivers, providing continuous band coverage from one to 50 gigahertz. All these upgrades will pump up the VLA's capabilities at least 10-fold, making it able, in principle, to detect a signal as weak as a cell phone call from Jupiter.

With $100 million from the National Science Foundation and the VLA's Canadian and Mexican partners, researchers have finished installing the digital data lines and upgrading, by this past May, 16 of the 28 antennas; by early 2010 the new correlator should be up and running. "We are on budget and on schedule, and there

aren't many astronomy projects that can make that claim," McKinnon boasts. "For the most part, we're going to have this thing wrapped up in 2012."

Meanwhile the next generation of radio-astronomy observatories is taking shape. The Atacama Large Millimeter/submillimeter Array (ALMA) is under construction on an Andean plain in northern Chile's Atacama Desert. The high-altitude locale 5,000 meters above sea level will enable the ALMA's 12-meter-wide dishes, at least 50 of them, to probe the shorter radio wavelengths near the infrared that the atmosphere tends to filter out. Two enormous, custom-built, 28-wheel heavy transporter vehicles will be used to move the antennas to give the array some reconfigurability. Barring cost concerns (already approaching $1 billion), technical problems and political exigencies, the ALMA should be ready around 2012.

"These two instruments will just rewrite radio astronomy," Perley predicts. Other new, somewhat smaller projects—such as the Low Frequency Array in Europe and the Allen Telescope Array in northern California—also promise to help brighten the future for radio astronomy. "It's very hard to predict precisely the science that will come from these things," Perley says. "The best stuff is the stuff you don't anticipate." Karl Jansky, who himself made a huge contribution to science through serendipity, would no doubt agree.

Mark Wolverton is a freelance science writer based in Bryn Mawr, Pa.

The Supersize Radio Telescope

The megaproject that radio astronomers are waiting for is the ambitious Square Kilometer Array (SKA), a 19-nation collaboration to build the largest, most sensitive radio telescope ever. Its thousands of small dishes would probe deeper into the universe and further back in time than any previous instrument and also conduct whole-sky surveys for transient phenomena such as gamma-ray and x-ray bursts. "What we're doing with the SKA is combining extraordinary sensitivity with wide field-of-view imaging or sampling," says Cornell University astronomer Rick M. Cordes, who heads the SKA's Technology Development Project.

Right now the array is only in the R&D phase, while researchers debate fundamental issues such as its location (either Western Australia or South Africa), the number and diameter of antennas, and the overall scientific objectives. If all goes well, actual construction of the SKA could begin around 2014.

NEUROSCIENCE

Primate Motions

Swiss ethics ruling could end some basic research on the brain BY LIZZIE BUCHEN

One of the most controversial issues in neuroscience is the use of our fellow primates as research subjects. Their similarities to humans in cognitive capacity, social complexity and neuroanatomy make them essential models for understanding the brain—yet these same attributes also single them out for special protection. In recent years European countries have passed increasingly strict regulations for experiments with nonhuman primates, leading many neuroscientists to fear for the future of their research. Switzerland's highest court may soon set the most rigid precedent yet—a possibility that has the international neuroscience community feeling uneasy.

In 2006 two primate researchers at the Swiss Institute of Neuroinformatics (INI) in Zurich, Daniel Kiper and Kevan Martin, were renewing their licenses through the local veterinary office, as Swiss researchers do every three years. Kiper proposed to look at how the brain changes when an animal learns novel tasks—findings that could eventually help human victims of stroke. His approach called for implanted electrodes and regulated water intake. Martin, head of the INI, wanted to study the circuitry of the macaque neocortex, which carries out higher functions such as spatial reasoning and conscious thought. His research relied on injecting tracer chemicals into the animals and later euthanizing them.

STEVE YEATER *AP Photo*

TOO HUMAN? Experimenters prize rhesus macaques for their similarity to humans. Neuroscientists in Switzerland might soon be unable to conduct basic research on them.

As it had done several times previously, the veterinary office approved their renewals—but this time the process hit a roadblock. An advisory board to the veterinary office, the Committee

on Animal Experiments, protested that the studies' expected benefits to society were not sufficient to justify the burden to the animals. The committee ultimately appealed to the Swiss Health Department, which forced the scientists to cease their experiments.

Meanwhile the application submitted by their INI colleague Hans Scherberger, who uses techniques similar to those of Kiper's work but studies how the brain controls hand movements, was approved without protest. "There was a difference," insists Klaus Peter Rippe, an ethicist who is president of the committee. Scherberger's experiment, he explains, "was developing neural prostheses, which have a very clear application to human welfare. The applications of Kiper's and Martin's experiments were not concrete and would take a long time to benefit society."

Kiper and Martin agree that their research does not have immediate practical value but note that it seeks an improved understanding of the brain—a foundation, they say, that is essential for tackling clinical conditions such as Alzheimer's and Parkinson's disease. Critics "think such basic research is not as important as applied research," Martin says. "But everyone who understands the scientific process knows that you can't distinguish the two. Look at stem cells, gene therapy, deep brain stimulation—they couldn't say when society would see the benefits or what those benefits would be."

Kiper and Martin appealed to the Zurich administrative court, but in a surprising ruling handed down on March 27, the court upheld the original protest, citing in part the macaque's evolutionary proximity to humans and its cognitive abilities. Long-term objectives and uncertain applications are unacceptable, the court ruled.

To many scientists, the ruling implies that research with primates must produce benefits to society within the three-year licensing period—a de facto ban on basic research. "It's antiscientific," Kiper declares. "This reflects a lack of trust in

scientists and a lack of respect for scientific progress in general." The University of Zurich and the Swiss Federal Institute of Technology in Zurich, which together established the INI, are now appealing to the Federal Supreme Court, the country's highest judicial body.

The case is in keeping with the recent European trend of increasingly stringent regulations for animal research; most notably, a September 2007 petition in the European Parliament to end all nonhuman primate experiments gained support from more than half of its members. Although the European Commission denied the petition, the level of political support has alarmed scientists, who fear that upcoming revisions to guidelines could seriously hamper their research.

Even in the U.S., where the political climate for primate research is more permissive, investigators feel an intensifying strain. "Doing primate work just gets tougher and tougher," says Bill Newsome, who studies the visual system at Stanford University. Newsome worries about the "constantly increasing regulatory scrutiny and general anxiety about being on the front line against unscrupulous animal-rights activists."

Newsome and others fear that animal-rights activists may seize on the Swiss ruling. "They network very effectively," says Klaus-Peter Hoffmann, a neuroscientist at the Ruhr University Bochum in Germany, whose home has been the target of British protestors. "They see what happens in one country, and if it works, they will use the same tactics elsewhere."

While the Swiss federal court considers the ruling and leaves Kiper's and Martin's projects struggling, both scientists express the greatest concern for the Swiss research agenda. "We built up a critical mass of talented primate researchers," Martin says. "But now that whole future is at risk. People are going to leave, and I can't recruit any more—why would anyone want to come and build their futures here? It's a catastrophe."

Lizzie Buchen is based in San Francisco.

ASTROPHYSICS

A Solar Big Gulp

Yes, the sun will eventually engulf Earth—maybe BY DAVID APPELL

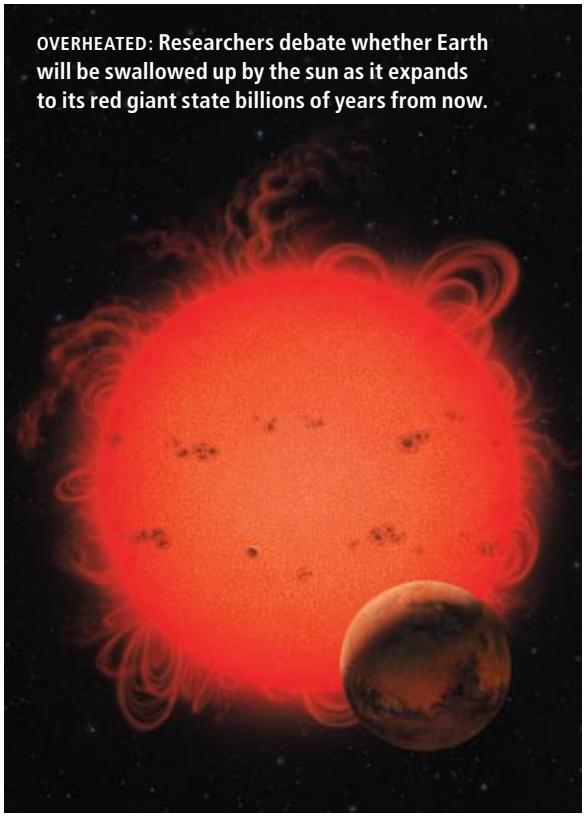
The future looks bright—maybe too bright. The sun is slowly expanding and brightening, and over the next few billion years it will eventually desiccate Earth, leaving it hot, brown and uninhabitable. About 7.6 billion years from now, the sun will reach its maximum size as a red giant: its surface will extend beyond Earth's orbit today by 20 percent and will shine 3,000 times brighter. In its final stage, the sun will collapse into a white dwarf.

Although scientists agree on the sun's future, they disagree about what will happen to Earth. Since 1924, when British mathematician James Jeans first considered Earth's fate during the sun's red giant phase, a bevy of scientists have reached oscillating conclusions. In some scenarios, our planet escapes vaporization; in the latest analyses, however, it does not.

The answer is not straightforward, because although the sun will expand beyond Earth's orbit, or one astronomical unit (AU), it will lose mass along the way. As a result, Earth should drift outward as the gravitational tug lessens over time. (At its maximum radius of 1.2 AU, the sun will have lost about one third of its mass, compared with its current heft.) In this way, Earth could escape solar envelopment.

But other factors complicate the analysis. Drag on the planet from the sun's outermost, tenuous layers will cause Earth to drift inward. Smaller forces from the other planets—all in turn reacting to the same reducing, expanding sun—are even more difficult to account for completely.

Earlier this year two teams reported different kinds of calculations indicating that Earth will be swallowed up by the sun. In a calculation that would thrill any college junior studying classical mechanics, Lorenzo Iorio of Italy's National Institute of Nuclear Physics used perturbation theory. It simplifies analyses by dropping relatively small factors, thereby making complex equations of motions that describe the interactions between the sun and Earth mathematically manageable. Assuming that the sun's yearly mass loss (currently about one part in 100 trillion) remains small for the duration of its evolution to the red giant phase, Iorio calculates that Earth will move outward at about three millimeters a year, or only 0.0002 AU by the sun's red giant phase. But at that point the sun will balloon up, in only a million years, to 1.2 AU in radius, thus vaporizing Earth.



OVERHEATED: Researchers debate whether Earth will be swallowed up by the sun as it expands to its red giant state billions of years from now.

LYNETTE COOK *Photo Researchers, Inc.*

Iorio's paper, submitted to *Astrophysics and Space Science*, has not yet been peer-reviewed. Several scientists question whether quantities that Iorio assumes are small will indeed remain small throughout the sun's evolution.

Even if Iorio got his number crunching wrong, he may have the right answer. In an analysis published in the May *Monthly Notices of the Royal Astronomical Society*, Klaus-Peter Schröder of the University of Guanajuato in Mexico and Robert Smith of the University of Sussex in England also conclude that Earth is doomed, by using more exact solar models and by considering tidal interactions. As the sun loses mass and expands, its rotation rate must also slow down—physics students learn this relation as the conservation of angular momentum. The slowed rotation causes a tidal bulge on the sun's surface. The gravity exerted by this bulge pulls Earth inward. With such a consideration, the researchers find that any planet with a present-day orbital radius of less than 1.15 AU will ultimately perish.

Could Earth be saved if someone is still left at home? In a bold piece of astronomical engineering, Don Korycansky of the University of California, Santa Cruz, and his colleagues have proposed nudging Earth with a large asteroid arranged to pass nearby periodically. It could take one billion years to move our planet out to somewhere safe, like the orbit of Mars. Our moon, though, might have to be left behind, and any miscalculation could mean extinction. Needless to say, more study is required.

David Appell is a freelance science writer based in Portland, Ore.

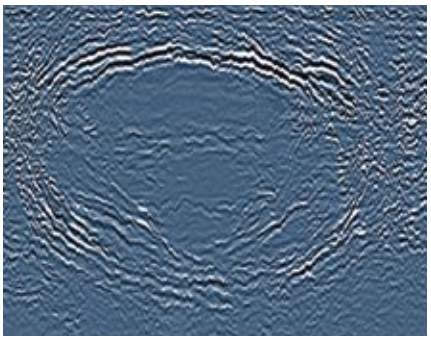
Page Intentionally Blank

OCEANOGRAPHY

Listening to a Mix

Seismic "noise" in oil-prospecting data could decipher ocean mixing BY LUCAS LAURSEN

Three decades ago researchers discovered what are essentially enormous saltwater lakes in the Atlantic Ocean. These "lakes," called meddies, are gently spinning lenses of water up to 100 kilometers across and one kilometer thick. They float a few hundred meters below the surface of the ocean. Such large, warm bodies, which turned out to come from the Mediterranean Sea, should have an impact on heat exchange in the ocean—and on the planet's climate. But efforts to study meddies—conventionally by dropping probes that directly measure the ocean's temperature, salinity and velocity—have proved too costly, infrequent and spread out to reveal how the meddies dissipate their heat.



BERTA BIESCAS AND VALENTÍ SALLARÈS *Marine Technology Unit, Spanish National Research Council*

NICE RING TO IT: Spanning about 80 kilometers, a ring of warm, salty water in the Atlantic, called a meddy, was recently imaged with seismic survey data taken 15 years ago.

Now researchers have demonstrated that a tool adapted from the oil industry can take rapid, high-resolution snapshots of the meddies. The technique, first used to find oil deposits under the seafloor, exploits sound reflections. Prospectors on ships fire air guns just below the sea surface; the acoustic waves then propagate down through the seafloor and bounce back to a towed array of microphones. The timing of sound waves' return reveals the density of the material through which they passed.

Boundaries between bodies of water also have a very faint sonic signature, which the oil industry used to treat as noise. But in 2003 a team led by W. Steven Holbrook of the University of Wyoming adopted the technique and created unexpectedly

clear acoustic images of density boundaries in the ocean. Changes in the density of seawater are interpreted as changes in its temperature and salinity. Because these properties tend to be unique to each ocean current, the researchers could visualize interactions between ocean fronts, much like climatologists map the boundaries of weather fronts.

Since then, researchers have analyzed old oil industry surveys and cobbled together experiments that could be piggybacked on oceanographic and oil industry cruises. Using data from a 1993 seismic survey off Spain's southwestern coast, a team led by Valentí Sallarès of the Marine Technology Unit of the Spanish National Research Council in Barcelona reports in the June 14 *Geophysical Research Letters* that it has imaged three meddies in unprecedented detail.

Sallarès's seismic images reveal "salt fingers" and other mixing features as small as 10 meters across. "At first blush, it's just exciting for people to be able to see these things," says Raymond Schmitt, an oceanographer at the Woods Hole Oceanographic Institution. But Schmitt says he and his colleagues are still grappling with how to interpret seismic images of meddies and other ocean-mixing hotspots such as underwater waves and the boundaries between ocean currents.

Seismic profiling is still not widely used in the oceanography community, in part because nobody has published a reliable quantitative conversion between seismic and traditional oceanographic measurements. Seismology detects reflections from places where the speed of sound changes. Oceanographic probes directly measure water conditions. Sallarès hopes to unify the two types of data: "The first step was the images, but if we're not capable of quantifying mixing processes we won't have anything."

Sallarès says that preliminary results from a recent dedicated seismic oceanography cruise suggest that temperature and salinity values may be harder to distinguish than originally thought. Holbrook, who led his own seismic oceanography survey off the coast of Costa

NEWS SCAN

Rica in April, wrote from his research vessel that seismic oceanography needs to "produce exciting and useful quantitative results" so that oceanographers can view it as "a critical enhancement of their toolbox, rather than a curiosity."

"I'm also hoping that we don't exhaust the patience of the physical oceanography community while we develop the necessary techniques," Holbrook adds. Researchers from both sides of the Atlantic will be gathering in November near Gerona, Spain, to share results from recent expeditions and to hash out the field's next steps.

In the meantime, nobody knows exactly what meddies contribute to the Atlantic's mixing, but Sallarès says that seismic profiling "is a clear first look and is more precise than what the oceanographic data can give us."

Lucas Laursen (www.lucaslaursen.com) is based in Cambridge, England.

A Warm, Salty Sea

The Mediterranean Sea's relative isolation and sunny climate make it vulnerable to rapid evaporation. As a result, it is much saltier than the Atlantic Ocean. Mediterranean waters enter the Atlantic in the form of meddies, gently spinning pools up to 100 kilometers across and one kilometer thick. Meddies carry their salt and heat into the open ocean, so their edges appear as particularly strong boundaries in seismic images.

MEDICINE

First in Class

Rocky debut for a nicotine mimic tempers hope for widespread use BY CHRISTINE SOARES

As the pharmaceutical giant Pfizer was reminded in May, arriving first has its rewards, but they come with the risks of venturing into uncharted territory. This past spring the Federal Aviation Administration banned pilots and air traffic controllers from taking the company's popular smoking-cessation aid, varenicline, which is sold in the U.S. as Chantix. Amid 6.5 million prescriptions written worldwide since 2006, the drug had spawned highly publicized reports of acute psychiatric episodes that included seizures, psychosis and suicidal depression. In May the nonprofit Institute for Safe Medication Practices documented 988 such "adverse events," prompting the aviation ban.

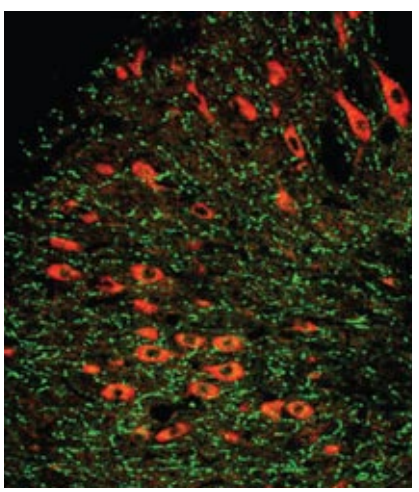
The Food and Drug Administration has now added strong warning language to varenicline's medication guide, and Pfizer is reviewing evidence that might help explain the rare but severe incidents. Although the bad publicity may dampen sales of the drug, observers say that some adverse events are not unexpected when a new drug hits the market, especially one that is the first of its kind. Varenicline is not just a novel smoking-cessation tool; it is the first of an entire class of medications specifically designed to target a powerful family of receptors on the surface of brain cells. Known as neuronal nicotinic acetylcholine receptors, they can mediate pain, mood, memory, attention and other cognitive functions.

Abbott Laboratories, Targacept and AstraZeneca have nicotinic receptor drugs in clinical trials for memory impairment, adult attention-deficit hyperactivity disorder and pain. The National Institute on Drug Abuse is testing varenicline itself as a treatment for cocaine and alcohol dependence. Preclinical studies

are looking at other new nicotinic receptor compounds for Parkinson's disease, Alzheimer's disease, depression, ulcerative colitis and inflammation as well, attesting to the broad influence of this receptor family.

The effects of nicotinic receptors are so pervasive, in fact, that some of the mechanisms involved are not completely understood. "It's a story that's still evolving, and it's very complicated, so going in with a drug like varenicline, I'm not surprised that there are side effects," says Lorna Role, who studies the receptors' biology at Columbia University and Stony Brook University. This type of acetylcholine receptor, which also responds to nicotine, acts as "a volume control" for other neurotransmitters, according to Role. "A little nicotine turns up transmitter release," she explains. "It's been shown to increase the release of dopamine, glutamate, GABA—every major neurotransmitter."

Activating a subtype of nicotinic receptor known as alpha4beta2 causes dopamine to be released in a part of the brain involved in reinforcing reward, for example, and that receptor is the primary target of varenicline. The drug works as a "partial agonist," meaning it binds to the receptor, producing moderate stimulation intended to stave off nicotine withdrawal. In so doing, it blocks



COURTESY OF MILLIPORE CORPORATION

NICOTINIC RECEPTORS (*red*) on the surface of brain cells are the targets of new drugs for a wide range of cognitive problems.

nicotine from getting to the receptor as well, which prevents a smoker from receiving a dopamine surge from a cigarette.

In cell studies, varenicline also acts as a potent full agonist for another receptor subtype called alpha7 that is associated with some of the positive cognitive effects of nicotine, such as enhanced focus. Variations in the alpha7 receptor gene are implicated in the difficulties schizophrenics tend to have with shutting out sounds or other stimuli. "I was hopeful that varenicline could be used for schizophrenia," Role says, "then the first report came out of it causing a psychotic episode, and it was hands off."

Given the complexity of the neuropsychological systems affected by nicotinic receptors, most of the episodes involving varenicline may never be explained. Pfizer representatives point out that smokers as a group have higher than average rates of anxiety and depressive disorders, suggesting that mild or undiagnosed preexisting mental illness might have played a part in some of the reactions to the drug. Moreover, symptoms such as agitation and suicidal thinking are well-documented side effects of tobacco withdrawal, notes Anjan Chatterjee, a director of medical affairs for Pfizer: "So it's hard to decide, is it the smoker's past history, or is it varenicline?"

Antidepressants in the class known as selective serotonin reuptake inhibitors (SSRIs), which debuted more than 20 years ago, have also been associated with adverse events such as suicidal thinking. The first generation of such drugs, which included Prozac, was notorious, too, for lesser side effects, including stomach upset and sexual dysfunction. Subsequent generations of SSRIs addressed some of those issues by building in blockers of certain serotonin receptor subtypes to eliminate unwanted drug actions.

"As with serotonin, people discovered there are subtypes of [receptor] subtypes. I think as time goes on there will be more sophisticated [nicotinic] drugs coming out," says Edward D. Levin, a behavioral pharmacologist at Duke University, who has consulted for Targacept and for the National Institutes of Health.

"It's just like the SSRIs," Role agrees. "I think refining the compounds in terms of the balance of their activities is really key, but that's not to say that's trivial. It'll take time." Targeting nicotinic receptors "has enormous therapeutic potential," she says, adding that the biggest joke on the tobacco industry may be that they missed seeing it.

FIELD NOTES

Mammoth Sequences

A hunt for DNA from extinct titans in the Klondike BY CHARLES Q. CHOI

DAWSON CITY, YUKON—After revving up with a roar, a core drill designed to punch holes in concrete begins digging into ice more than 100,000 years old. Here in the Klondike, the drill serves as a kind of gas-powered, handheld time machine, bringing up frozen earth from the Pleistocene, when mammoths and other megafauna once ruled. In a land where miners still hunt for gold, paleomammalogist Ross MacPhee of the American Museum of Natural History in New York City and his colleagues seek a different kind of treasure—DNA from extinct titans.

DNA DIG: **Duane Froese (*left*) and Ross MacPhee use a gas-powered drill to collect material that might hold Pleistocene genetic clues.**

Millennia ago, as the earth in the Klondike cracked during the springtime thaw, water leaked in, only to freeze again during winter to form wedges of ice, explains geologist Duane Froese of the University of Alberta. Dripping in with this water was sediment from the surface, which might hold DNA from mammoths, as well as that of the plants, bacteria and other life once found in the region, MacPhee says. Nothing is known about the genetics of mammoths from the middle Pleistocene, and such DNA could elucidate their evolution. The researchers hope to find clear evidence that two species of mammoth, not just one, roamed the Americas at the end of the last ice age.

This area, dominated today by spruce forest mixed with paper birch and aspen trees, was once part of Beringia, the grassland steppe ranging from North America to Asia that nowadays lies submerged under the icy Bering Strait. Froese has worked in the Klondike for the past 15 or so field seasons, aiming to reconstruct a full picture of Beringia over the past few million years. Sampling trapped sediment for DNA could prove a far easier way to analyze how Beringia's ecosystems shifted over time as compared with attempting to collect hundreds of fossils from different taxa.

In joining the team for seven days in June, I learn that ancient DNA molecules are not the only clues the researchers seek here. Paleoentomologist Svetlana Kuzmina

CHARLES Q. CHOI

of the University of Alberta sifts through sediment for fossil insects—by studying where modern examples of these now dwell, she can extrapolate what the climate might have been like back then. Lee Arnold of the University of Wollongong in Australia will scan crystalline grains to pinpoint the ages of all the finds, thus helping to reveal the proper sequence of events—which is as important as having words in the right order in a sentence. And later the scientists will head north by plane, helicopter and boat to dig for bones.

The fact that gold mining continues in the Klondike has proved invaluable. We can drive over mining roads right up to sites, as opposed to lugging heavy equipment a mile or more by foot. The miners have also been very supportive, even using excavators to scrape off tons of surface material, called overburden, from the frozen earth at a rocky site named Paradise Hill. Their help makes research far more cost-effective, Froese explains. MacPhee agrees: "You'd be lucky to get one site done in Siberia in a week."

Still, fieldwork remains a hard, dirty task. The giant wedge of ice we mine at Gold Run Creek on the fourth day of our expedition was hidden under a slope of powdery muck—silt loaded with ancient, decomposing organic material, which smells much like manure. As we expose the ice to the sun, water mixes with the muck to form a slippery ooze that occasionally traps us up to our thighs, much to our chagrin. Field time also can unpredictably vanish, as we discover when the rough, gravel roads take their toll on the rental SUV, which suffers three flats in just two days.

In the end, all the hard-won scientific treasure could help solve key mysteries. MacPhee hopes, for instance, that the DNA could explain why so many megafauna went extinct in the Americas. Did rapid swings in climate kill them off? Or was it the cunning of human hunters? Or was it species-jumping plagues that humans brought over, as MacPhee suggests?

The work could also reveal something about the planet's future. At a site called Lucky Lady Mine are layers of earth that date back roughly 100,000 years to the last interglacial period, the interlude between the advances of glaciers across the Northern Hemisphere. Back then the world was warmer than it is today, so analyzing sediment from that time could shed light on the global warming the planet is experiencing now, Froese remarks. (He discovered the site after meeting the Lucky Lady Mine's owner, a paleontology enthusiast, at the Snake Pit bar in Dawson City.)

At one point, when we are mired deep in muck, I ask MacPhee whether this is the glamorous life of a paleontologist. He smiles and replies, "You can't beat it."

Charles Q. Choi is a frequent contributor. Blogs of his days with the researchers, as well as photos and video clips, are posted at **www.SciAm.com/sep2008**

PARTICLE PHYSICS

A New Neutrino Hunt

Fermilab hopes to glimpse a possible visitor from another dimension BY MARK ALPERT

The detection of extra dimensions beyond the familiar four—the three dimensions of space and one of time—would be among the most earth-shattering discoveries in the history of physics. Now scientists at the Fermi National Accelerator Laboratory in Batavia, Ill., are designing a new experiment that would investigate tantalizing hints that extra dimensions may indeed exist.

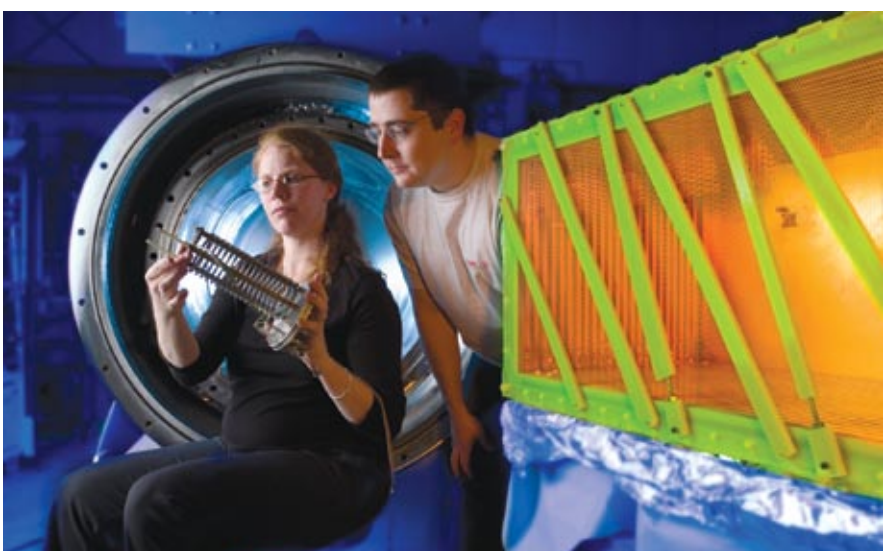
Last year researchers involved in Fermilab's MiniBooNE study, which detects elusive subatomic particles called neutrinos, announced that they had found a surprising anomaly. Neutrinos, which have no charge and very little mass, form out of nuclear reactions and particle decays. They come in three types, called flavors—electron, muon and tau—and oscillate wildly from one flavor to another as they travel along. While observing a beam of muon neutrinos generated by one of Fermilab's particle accelerators, the MiniBooNE researchers found that an unexpectedly high number of the particles in the low-energy range (below 475 million electron volts) had transformed into electron neutrinos. After a year of analysis, the investigators have failed to come up with a conventional explanation for this so-called low-energy excess. The mystery has focused attention on an intriguing and very unconventional hypothesis: a fourth kind of neutrino may be bouncing in and out of extra dimensions.

String theorists, who seek to unify the laws of gravity with those of quantum mechanics, have long predicted the existence of extra dimensions. Some physicists have proposed that nearly all the particles in our universe may be confined to a four-dimensional "brane" embedded within a 10-dimensional "bulk." But a putative particle called the sterile neutrino, which interacts with other particles only through gravity, would be able to travel in and out of the brane, taking shortcuts through the extra dimensions. In 2005 Heinrich Päs, now at the University of Dortmund in Germany, Sandip Pakvasa of the University of Hawaii and Thomas J. Weiler of Vanderbilt University predicted that the extradimensional peregrinations of sterile neutrinos would increase the probability of flavor oscillations at low energies—exactly the result found at MiniBooNE two years later.

Energized by the prospect of discovering new laws of physics, the MiniBooNE team soon proposed a follow-up experiment called MicroBooNE that could test the sterile neutrino hypothesis. The new detector, a cryogenic tank filled with 170 tons of liquid argon, would be able to detect low-energy particles with much greater precision than its predecessor could. A particle emerging from a neutrino interaction would ionize the argon atoms in its path, inducing currents in arrays of wires at the perimeter of the tank. Scientists could then pinpoint the trajectory of the particle, allowing them to better distinguish between electron neutrino interactions and other events and thus determine whether there really is an excess of oscillations at low energies.

Estimated to cost about $15 million, the MicroBooNE tank would be located near the MiniBooNE detector at Fermilab so that it could observe the same beam of neutrinos. This past June the lab's physics advisory committee approved the design phase for the project; if all goes well, the detector could begin operating as soon as 2011. Researchers hope that MicroBooNE will lead to the development of much larger detectors, containing hundreds of thousands of tons of liquid argon in tanks as big as sports arenas. Such facilities could search for other hypothesized phenomena such as the extremely rare decay of protons. "It's a fantastic new technology," says Bonnie Fleming, a physicist at Yale University and spokesperson for MicroBooNE. "And it's crucial for taking the next step in physics."

Mark Alpert is author of Final Theory *(Touchstone, 2008), a physics thriller that features neutrinos and extra dimensions.*



FERMILAB

NEUTRINO HUNTERS Bonnie Fleming and Mitchell Soderberg inspect a prototype liquid-argon detector called ArgoNeuT that will pave the way for the MicroBooNE facility at Fermilab.

Page Intentionally Blank

Data Points

Greenhouse TV

Watching television may be bad for the kids; making televisions, it seems, may be bad for the climate. To produce flat-panel displays, manufacturers rely on nitrogen trifluoride (NF_3), a potent greenhouse gas that was not covered by the emissions-regulating Kyoto Protocol when it was drafted in 1997, because so little of it was used then. Now exploding sales of flat-panel TVs and other digital devices, coupled with incomplete recapture of the chemical during manufacture, could spell trouble, warn Michael J. Prather and Juno Hsu, both at the University of California, Irvine. They advocate further study to document the presence of atmospheric NF_3.

Atmospheric lifetime of NF_3:
550 years

Greenhouse potency factor (global warming potential), as compared with carbon dioxide, of:

Methane: **25**

NF_3: **17,200**

Estimated number of tons of NF_3 to be produced in 2008: **4,000**

Equivalent amount of CO_2, in tons: **67 million**

Percent of NF_3 not recaptured during manufacturing: **2 to 3**

CO_2 emissions in 2005, in tons: **15,128 million**

SOURCE: Geophysical Research Letters, *June 26, 2008*

EVOLUTION

Not So Rapid Eye Movement

The bizarre metamorphosis that occurs in halibut and other flatfish had even Charles Darwin floundering for an explanation. At birth, these fish have one eye on each side of the skull, but as adults, both eyes reside on the same side. Certainly, for fish that spend their lives along the sea bottom, having both eyes topside confers a survival advantage. But there seemed to be no evolutionary reason to start down the gradual path toward such lopsidedness—any intermediate steps would not seem to be especially helpful. So some biologists theorized that the fish evolved from a single, sudden mutation.

EYES UP: Flounder and other bottom-dwelling flatfishes have two eyes on one side of the skull.

That does not seem to be the case: Matt Friedman of the Field Museum in Chicago reports finding some missing links. He investigated two roughly 50-million-year-old primitive flatfish fossils hidden in museums in Europe for more than a century. These adult specimens possessed somewhat asymmetrical skulls that nonetheless kept eyes on opposite sides of the head. Even incomplete lopsidedness may have given the carnivorous bottom dwellers a better view of the world above than no asymmetry at all, Friedman conjectures. Eye the study in the July 10 *Nature*. —*Charles Q. Choi*

OUTBREAKS

Germ-Spreading Playdates

As parents have long known, children in day care centers and schools readily spread respiratory diseases among one another. Chimpanzee communities seem to suffer in a similar way: playdates drive the dissemination of respiratory infections among the primates, according to a new study.

Scientists led by Hjalmar Kuehl and Peter Walsh of the Max Planck Institute for Evolutionary Anthropology in Leipzig, Germany, examined two chimpanzee groups in Taï National Park in Ivory Coast. Infants were more likely to die from a respiratory disease the more they played together—typically during the peak fruit season, when chimps congregate. Between the ages of two and three, chimps spend up to 18 percent of their day engaged in close physical contact with their peers. This period represents the peak of their social interaction and serves to connect all members of their community.

PLAYTIME helps young chimps develop socially, but it also spreads infections.

Once playful chimpanzees precipitated an outbreak, infants of all ages succumbed to disease. Affected mothers quickly entered into estrus, ultimately perpetuating the three-year cycle of infant population boom and bust. Coupled with poaching, climate change and predation, infant mortality from infectious disease is taking a toll on the area's chimps, says Kuehl, whose research findings appear in the June 18 *PLoS ONE*. These days few infants reach adulthood, he states, with "only four out of 10 surviving to the age of five."

—*Barbara Juncosa*

SCOTT LESLIE *Minden Pictures (flatfish)*; ANUP SHAH *NPL/Minden Pictures (chimps)*; ILLUSTRATION BY MATT COLLINS

In Brief

MOUNTAIN-CLIMBING TREES

Global warming is leaving trees behind. Some two thirds of forest species in six French mountain ranges have moved at least 18.5 meters higher on the mountainsides per decade during the 20th century. Previous research has demonstrated that plants at the highest elevations on mountains and in the polar regions have shifted to adjust to global warming. The latest result marks the first confirmation that entire ecosystems in lower, more temperate regions are moving as well. The study is in the June 27 *Science*. —*David Biello*

LOCATION INFLUENCES VOTERS

The voting location may tip the balance on some election issues. Researchers examined the 2000 Arizona general election that included a proposed tax increase to support school initiatives. After controlling for political preferences and zip codes, the researchers found that voters casting ballots at schools tended to support the measure (63.6 percent in favor) more so than those at nonschool booths (56.3 percent). A follow-up experiment revealed that voters could be subconsciously "primed" with images of lockers and classrooms to vote for a hypothetical tax for school spending. The July 1 *Proceedings of the National Academy of Sciences USA* contains the findings. —*Philip Yam*

KHAMPHA BOUAPHANH *AP Photo (voter)*; E. WALKER *Photo Researchers, Inc. (kidney stones)*; MARKUS SCHREIBER *AP Photo (electric chair)*

MARTIAN HIT-AND-RUN

Researchers have long suspected that a massive asteroid caused Mars's "hemispheric dichotomy": its crust thins from 50 to 20 kilometers over a south-north span covering 42 percent of its surface. Using gravity data and other measurements, scientists have discovered the hidden outline of the impact—in particular, an elliptical mark spanning 10,600 by 8,500 kilometers. Simulations suggest that the asteroid measured 1,600 to 2,700 kilometers wide, moved at about six to 10 kilometers per second, and struck at an angle of 30 to 60 degrees with the ground. —*JR Minkel*

NEUROBIOLOGY

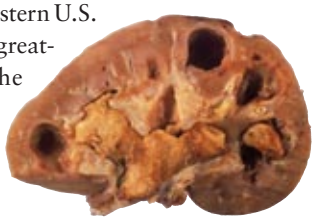
Another Gene for Alzheimer's

A newly identified genetic mutation increases the risk for the most common form of Alzheimer's disease—the second major gene to be linked to the neurodegenerative disorder. The mutation occurs in the so-called *CALHM1* gene, which controls calcium concentrations in nerve cells. Researchers observed that mutant *CALHM1* led to increased accumulation of amyloid beta plaques, the sticky protein clumps characteristic of the disease. In the U.S. Alzheimer's affects one in 20 adults aged 65 to 74; carrying one defective copy of *CALHM1* escalates the risk to one in 14 (and to one in 10 for those carrying two defective copies). The mutation also leads to an earlier age of onset. Reporting in the June 27 *Cell*, lead author Philippe Marambaud of the Feinstein Institute for Medical Research in Manhasset, N.Y., states that the *CALHM1* gene—along with the first Alzheimer's gene, *APOE*, discovered 15 years ago—will be important in screening for the disease. —*Barbara Juncosa*

CLIMATE AND HEALTH

The New Stone Age

Kidney stones will become more prevalent in the 21st century as the world warms up, according to Tom H. Brikowski of the University of Texas at Dallas and his colleagues. A crystallization of minerals dissolved in urine, a stone can form with the help of fluid loss. Such dehydration is more common in hotter conditions; the incidence in the southeastern U.S. is 50 percent greater than in the northwestern region of the country, for instance, and some U.S. soldiers shipped to desert conditions developed stones just 90 days after deployment. Factoring in the expected rise in mean temperature in the U.S.—upward of two to five degrees Celsius this century—the researchers figure that the nation will see 1.6 million to 2.2 million more kidney stone cases by 2050. This 7 to 10 percent increase could exact $1.3 billion in medical costs. The findings are crystallized in the July 15 *Proceedings of the National Academy of Sciences USA*. —*Philip Yam*

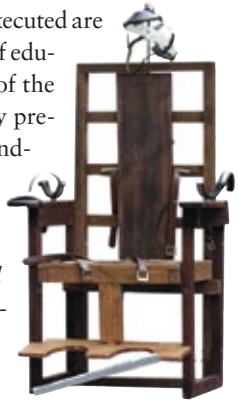


STONED: Kidney cross section shows stones and resultant cavities.

SOCIOLOGY

Who Will Die?

Researchers have built a computer system that can predict which death-row inmates are most likely to be executed. It consists of 18 computer processors that analyzed data on about 1,000 death-row prisoners, including their sex, age, race, schooling and whether they were ultimately executed or spared. Then the researchers fed it similar information about 300 more prisoners, leaving out whether they had lived or died. The system, using logic it had developed from the first set of data, correctly predicted the outcome for 92 percent of those cases. It found that death-row inmates with the highest chance of being executed are those with the lowest levels of education; neither the severity of the crime nor race could reliably predict a prisoner's fate. The findings, which the researchers hope will lead to a fairer appeals process, appear in the Spring 2008 *International Journal of Law and Information Technology*. —*Larry Greenemeier*



Read More ...

News Scan stories with this icon have extended coverage on **www.SciAm.com/sep2008**

SciAm Perspectives

Seven Paths to Privacy

History is ambiguous about government willingness to protect private life, but a few recommendations can help keep its future secure

BY THE EDITORS

I am not only retired from all public employments, but I am retiring within myself, and shall be able to view the solitary walk and tread the paths of private life with heartfelt satisfaction.

—George Washington,
letter to the Marquis de Lafayette, 1784

That is one view of privacy. Here is another:

We must all watch one another.

—Rev. Robert Browne,
guiding principles, 1582

Browne was an Anglican minister, and his dark view of the human spirit as weak and prone to wickedness without the constant "support" of a community of spies and informers had enormous influence on the New England Puritans. Both quotations are drawn from Robert Ellis Smith's essential study of the history of privacy in America, *Ben Franklin's Web Site*.

Those two deeply rooted but antagonistic approaches to privacy have simmered together for centuries, but today converging forces in politics, technology, commerce and law have brought them to a boil. We offer seven policy recommendations that would help preserve Washington's idyllic picture of private life without having to endure Browne's nightmare.

1. *Restore the role of the Foreign Intelligence Surveillance Act (FISA) court in issuing warrants for wiretapping.* Targeted wiretapping approved by a warrant is essential for fighting crime and terrorism. But the amendment to FISA that Congress approved this past July could violate the rights of innocent people. There was no need to extend the period of emergency, warrantless wiretapping from three days to seven. And the reduced oversight by the FISA court under the new law amplifies the risk of error or abuse in authorizing wiretaps.

2. *Deny the Federal Bureau of Investigation's proposal to require all "telephone" capabilities of the Internet to be "wiretap-ready."* True, many telephone conversations are being partly routed over the Internet—not only by services such as Skype but also by the nation's cell phone carriers. But granting the FBI's proposal would have such crippling side effects that it would do much more harm than good. One key reason for opposing it is that such wiretap capability could open up a new backdoor entry to the Internet, which the nation's enemies could then exploit.

3. *End the secrecy surrounding the Cyber Initiative.* To protect the Internet from such attacks, the Bush administration has launched a "Cyber Initiative," a program that could end up costing billions of dollars. The initiative clearly aims to conduct widespread surveillance of Internet traffic, yet plans for it are so hush-hush that there has been little or no public debate about it. Plenty of discussion about other kinds of defense spending has taken place without tipping off the enemy; here, too, debate is needed.

4. *Grant people control over their own medical information.* Patients should be able to determine who sees which parts of their personal medical and genetic records—with one exception. Once proper safeguards are in place to protect individuals, the information should be made available anonymously for studies in medicine and public health.

5. *Encrypt and control all records.* Organizations that store personal information—including those that hold biometric data and data generated by radio-frequency identification (RFID) tags—must keep it from falling into the wrong hands. The threat of lawsuits as well as criminal sanctions through tougher privacy laws is needed to enforce this obligation.

6. *Regulate the use of RFID tags.* When RFID tags are embedded in a retail product, they should be disabled once the shopper has paid for the product. Even if they store nothing more than a serial number, they enable anyone who carries such a tag to be followed surreptitiously. If they must remain readable—as in licenses, passports, and the like—their presence should be disclosed to the carrier. If the tags store personal information, including information about time and place, it should be encrypted and the carrier should be warned about its presence.

7. *Develop educational curricula about the risks to privacy in the online world.* Schools and educators should also prepare students to take advantage of the tools available for protecting privacy. ■

MATT COLLINS

Sustainable Developments

The Specter of Malthus Returns

It remains to be seen whether his famously gloomy prediction is truly wrong or merely postponed

BY JEFFREY D. SACHS

In 1798 economist Thomas Robert Malthus famously predicted that short-term gains in living standards would inevitably be undermined as human population growth outstripped food production and thereby drove living standards back toward subsistence. We were, he argued, condemned by the tendency of population to grow geometrically while food production would increase only arithmetically.

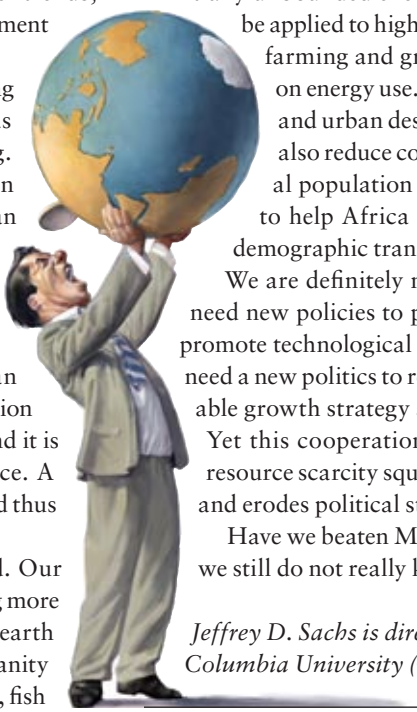
For 200 years economists have dismissed Malthus for overlooking technological advancement. Their argument is that food production can indeed grow geometrically because production depends not only on land but also on know-how. With advances in seed breeding, chemical fertilizers, irrigation, mechanization and more, the food supply can stay well ahead of the population curve. More generally, advances in technology in all its aspects can keep production rising ahead of population. Malthus also seemingly did not reckon with the demographic transition: improvements in public health, family planning and modern contraception, together with urbanization and other trends, can dramatically reduce fertility rates to the "replacement rate" of 2.1 children per household—or even less.

When I trained in economics, Malthusian reasoning was a target of mockery, held up by my professors as an example of a naive forecast gone wildly wrong. After all, since Malthus's time, incomes per person averaged around the world have increased by at least an order of magnitude despite a population increase over that period from around 800 million to 6.7 billion. Some economists have gone so far as to argue that rising populations have been a major cause of increased living standards, rather than an impediment, because the eightfold increase in population has proportionally raised the number of geniuses, and it is genius above all that propels global human advance. A large human population, in that interpretation, would thus be just what is needed to propel progress.

Yet the Malthusian specter is not truly banished. Our increase in know-how has not only been about getting more outputs for the same inputs but also about mining the earth for more inputs more efficiently and intensively. Humanity has learned to dig deeper for minerals and fossil fuels, fish the oceans with larger nets, divert rivers with greater dams and canals, and cut down forests with more powerful land-clearing equipment. In countless ways, we have not gotten more for less but rather more for more, as we have converted rich stores of natural capital into high flows of current consumption.

And although family planning and contraception have indeed secured a low fertility rate in most parts of the world, the overall fertility rate remains at 2.6, far above replacement. Global population continues to rise by about 79 million a year, with much of the increase in the world's poorest places. According to the medium-fertility forecast of the United Nations Population Division, we are on course for 9.2 billion people by midcentury.

If we indeed run out of inexpensive oil and fall short of food, deplete our aquifers and destroy remaining rain forests, and gut the oceans and fill the atmosphere with greenhouse gases that tip the earth's climate into a runaway hothouse with rising ocean levels, we might yet confirm the Malthusian curse. Yet none of this is inevitable if future technology enables us to economize on natural capital rather than finding ever more clever ways to deplete it rapidly. In the coming decades we will have to convert to solar power and safe nuclear power, both of which offer essentially unbounded energy supplies. Know-how will have to be applied to high-mileage automobiles, water-efficient farming and green buildings that cut down sharply on energy use. We will need to rethink modern diets and urban design to achieve healthier lifestyles that also reduce consumption. And to stabilize the global population at around eight billion, we will have to help Africa and other regions in speeding their demographic transition.



We are definitely not yet on such a trajectory. We will need new policies to push markets down that path and to promote technological advances in resource saving. We will need a new politics to recognize the importance of a sustainable growth strategy and global cooperation to achieve it. Yet this cooperation will have to come at a time when resource scarcity squeezes living standards in many places and erodes political stability.

Have we beaten Malthus? Two centuries after his work, we still do not really know. ■

Jeffrey D. Sachs is director of the Earth Institute at Columbia University (www.earth.columbia.edu).

SCI AM An extended version of this essay is available at **www.SciAm.com/sep2008**

PHOTOGRAPH BY BRUCE GILBERT/EARTH INSTITUTE; ILLUSTRATION BY MATT COLLINS

Skeptic

Folk Numeracy and Middle Land

Why our brains do not intuitively grasp probabilities, Part 1

BY MICHAEL SHERMER

Have you ever gone to the phone to call a friend only to have your friend ring you first? What are the odds of that? Not high, to be sure, but the sum of all probabilities equals one. Given enough opportunities, outlier anomalies—even seeming miracles—will occasionally happen.

Let us define a miracle as an event with million-to-one odds of occurring (intuitively, that seems rare enough to earn the moniker). Let us also assign a number of one bit per second to the data that flow into our senses as we go about our day and assume that we are awake for 12 hours a day. We get 43,200 bits of data a day, or 1.296 million a month. Even assuming that 99.999 percent of these bits are totally meaningless (and so we filter them out or forget them entirely), that still leaves 1.3 "miracles" a month, or 15.5 miracles a year.

Thanks to our confirmation bias, in which we look for and find confirmatory evidence for what we already believe and ignore or discount contradictory evidence, we will remember only those few astonishing coincidences and forget the vast sea of meaningless data.

We can employ a similar back-of-the-envelope calculation to explain death premonition dreams. The average person has about five dreams a night, or 1,825 dreams a year. If we remember only a tenth of our dreams, then we recall 182.5 dreams a year. There are 300 million Americans, who thus produce 54.7 billion remembered dreams a year. Sociologists tell us that each of us knows about 150 people fairly well, thus producing a social-network grid of 45 billion personal relationship connections. With an annual death rate of 2.4 million Americans, it is inevitable that some of those 54.7 billion remembered dreams will be about some of these 2.4 million deaths among the 300 million Americans and their 45 billion relationship connections. In fact, it would be a *miracle* if some death premonition dreams did not happen to come true!

These examples show the power of probabilistic thinking to override our intuitive sense of numbers, or what I call "folk numeracy," in parallel with my previous columns on "folk science" (August 2006) and "folk medicine" (August 2008) and with my book on "folk economics" (*The Mind of the Market*). Folk numeracy is our natural tendency to misperceive and miscalculate probabilities, to think anecdotally instead of statistically, and to focus on and remember short-term trends and small-number runs. We notice a short stretch of cool days and ignore the long-term global-warming trend. We note with consternation the recent downturn in the housing and stock markets, forgetting the half-century upward-pointing trend line. Sawtooth data trend lines, in fact, are exemplary of folk numeracy: our senses are geared to focus on each tooth's up or down angle, whereas the overall direction of the blade is nearly invisible to us.

The reason that our folk intuitions so often get it wrong is that we evolved in what evolutionary biologist Richard Dawkins calls "Middle World"—a land midway between short and long, small and large, slow and fast, young and old. Out of personal preference, I call it "Middle Land." In the Middle Land of space, our senses evolved for perceiving objects of middling size—between, say, grains of sand and mountain ranges. We are not equipped to perceive atoms and germs, on one end of the scale, or galaxies and expanding universes, on the other end. In the Middle Land of speed, we can detect objects moving at a walking or running pace, but the glacially slow movement of continents (and glaciers) and the mind-bogglingly fast speed of light are imperceptible. Our Middle Land timescales range from the psychological "now" of three seconds in duration (according to Harvard University psychologist Stephen Pinker) to the few decades of a human lifetime, far too short to witness evolution, continental drift or long-term environmental changes. Our Middle Land folk numeracy leads us to pay attention to and remember short-term trends, meaningful coincidences and personal anecdotes.

Next month, in Part 2, we will consider how randomness rules our lives through the metaphor of "the drunkard's walk," well elucidated by physicist Leonard Mlodinow of the California Institute of Technology in his new book of the same title. ■

Michael Shermer is publisher of Skeptic *(www.skeptic.com). His latest book is* The Mind of the Market.

PHOTOGRAPH BY BRAD SWONETZ; ILLUSTRATION BY MATT COLLINS

Anti Gravity

The Bird Bomb

You really didn't want to be under these feathered flyers

BY STEVE MIRSKY

Watch a pigeon dodge traffic, both vehicular and pedestrian. The bird seems to be the very embodiment of unfulfilled potential—it can fly, and yet it walks. Of course, during World War II, pigeons did a fair amount of flying, carrying messages between the front and command posts. But full pigeon promise was never realized. Because the birds were denied the chance to show what they could do in the air—as pilots.

The story of pigeon pilots, as well as all else pigeon, is told in the new book *Superdove: How the Pigeon Took Manhattan … And the World,* by Courtney Humphries. She explains that the idea of using pigeons as pilots first occurred to a young B. F. Skinner in 1940, when he watched a flock do some fancy maneuvering. (He presumably did not get the idea from watching the movie *Flight Command,* which came out the same year and featured a pilot played by Walter Pidgeon.)

Skinner had already shown that a simple reward system—a nibble of kibble—could get rats to engage in increasingly complex behaviors. Because pigeons already had great navigation skills, Skinner really thought outside the box, coming up with the radical notion of actually putting them in the cockpit. Oh, the birds wouldn't be piloting planes, because who would get on a plane with a pigeon pilot, unless the airlines agreed to drop the baggage fee. No, these pigeons were going to pilot missiles.

Step one, of course, was putting "a toeless sock over the pigeon's body to restrain the wings and feet," Humphries explains. The pigeon was thus forced to use its beak to peck at a target—such as a ship, building or specific street corner. Successful pecks were rewarded with pellets of grain. A jerry-built apparatus took the movements of the bird's head and neck and translated them, using electric motors, into steering moves. Project Pigeon was presented to the National Defense Research Committee for further funding. The committee apparently thought that Skinner should also be restrained and rejected the proposal.

Following Pearl Harbor, however, Skinner resumed his efforts to turn pigeons into WMDs: winged murdering doves. He got a $5,000 check from General Mills—the cereal company, not the unfortunately named army officer of the same period, Major General John S. Mills, who was in fact a pilot and bomb squadron member himself. Ironically, considering the funding source, one key to the enterprise was keeping the birds hungry. "Skinner found that if they were kept just a bit underfed, the birds would work tirelessly for their reward," Humphries notes. The birds were so good, she says, that Skinner's team had to work far harder on the mechanical system to translate the avian actions into course corrections than on pilot reliability.

With his pigeon proof-of-concept in place, Skinner was able to get $25,000 from the feds to develop what he called an "organic homing device." He incorporated redundancy into the design by putting three pigeons into the cockpit, with any birds pecking at the wrong target going hungry until they wised up.

At the same time, the army was trying to perfect a gliding missile called the Pelican, which was being tested in the Garden State. So Skinner's birds learned to home in on targets in the area where the missile was being developed. That's right, Skinner was training pigeons to fly a Pelican that would fake-bomb New Jersey.

A final demonstration before the government committee showed that pigeons could indeed be relied on to be ruthless, unrepentant killing machines. But the committee couldn't get over the fact that they were, ya know, pigeons. Humphries quotes Skinner: "The spectacle of a living pigeon carrying out its assignment, no matter how beautifully, simply reminded the committee of how utterly fantastic our proposal was. I will not say that the meeting was marked by unrestrained merriment, for the merriment was restrained. But it was there."

Skinner was left with, as he put it, "a loftful of curiously useless equipment and a few dozen pigeons with a strange interest in a feature of the New Jersey coast." The birds' flying days were over. Well, you know what I mean. ■

PHOTOGRAPH BY FLYNN LARSEN; ILLUSTRATION BY MATT COLLINS

PRIVACY IN AN AGE OF TERABYTES AND TERROR

Our jittery state since 9/11, coupled with the Internet revolution, is shifting the boundaries between public interest and "the right to be let alone"

By Peter Brown

A cold wind is blowing across the landscape of privacy. The twin imperatives of technological advancement and counterterrorism have led to dramatic and possibly irreversible changes in what people can expect to remain of private life. Nearly 10 years ago Scott McNealy of Sun Microsystems famously pronounced the death of privacy. "Get over it," he said. Some people, primarily those younger than about 25, claim to have done just that, embracing its antithesis, total public disclosure. And of course in many cases—determining the whereabouts of a terrorist or the carrier of a disease—public interest has an overwhelming claim on information that is usually private.

Yet in many contexts—banking, commerce, diplomacy, medicine—private communications are essential. The founding fathers of the Republic put great stock in personal privacy; privacy is embodied (though, as we are often reminded, not stated) in the Bill of Rights. In her keynote essay Esther Dyson clarifies what "privacy" means by reminding us what it is not (*page 50*): several important issues commonly labeled dilemmas of privacy are better understood as issues of security, health policy, insurance or self-presentation.

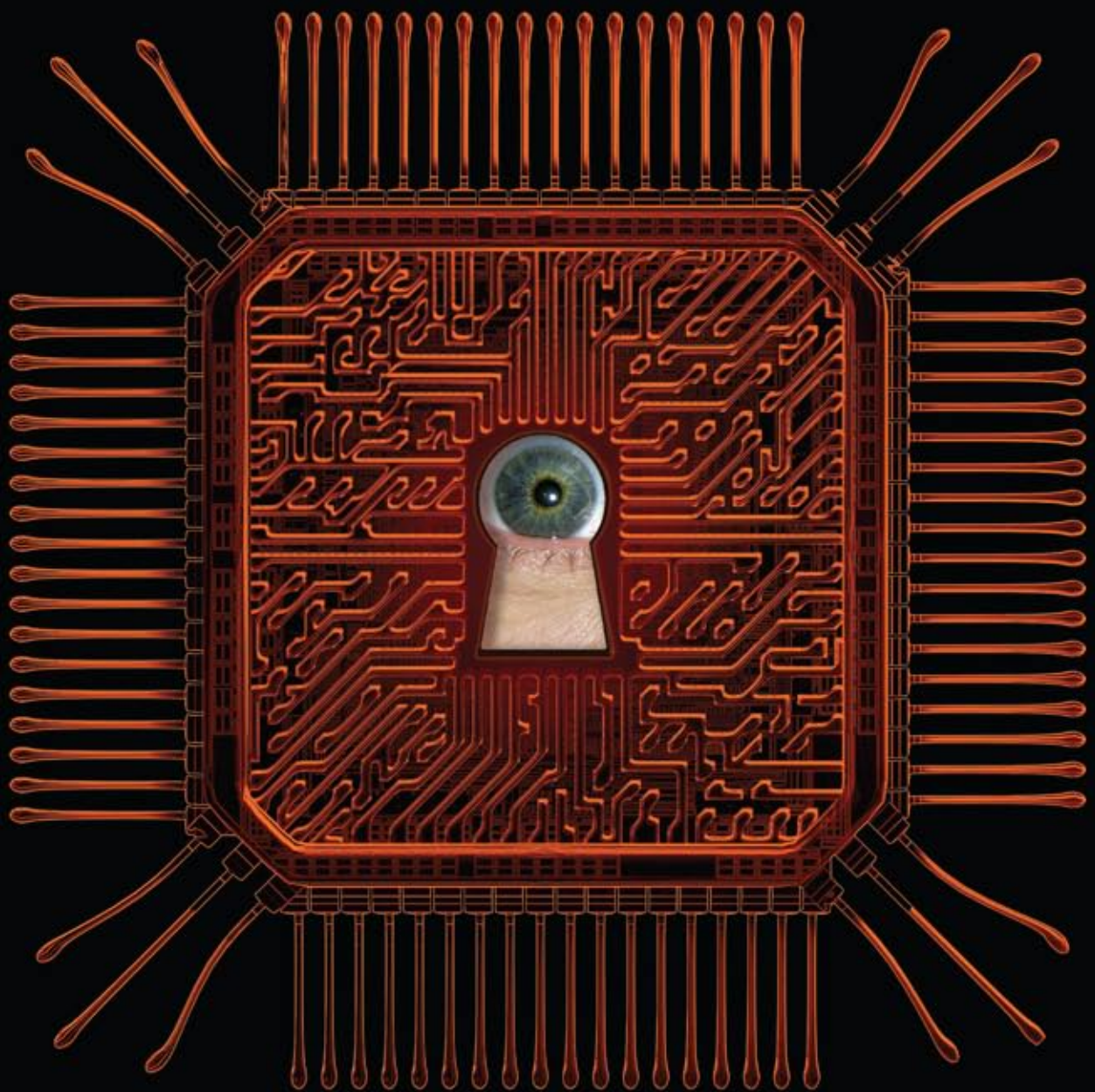
Terrorism and digital connectedness have both made privacy a hot-button issue, but there are plenty of other good reasons to look closely at the future of privacy. One is the upcoming U.S. election, which is being held at a time of tremendous upheaval in the legal and legislative framework of government wiretapping (*page 56*).

A second is the allure of substantial benefits from disclosing certain kinds of information: enhanced medical care through electronic medical and genetic records (*page 64*), for instance, or better protection from identity theft via biometric authorization (*page 78*). A third is that the threats posed by technology to personal privacy and even personal security are unprecedented, both from the unintended effects of increased self-disclosure as well as from the rapidly evolving sophistication of surveillance gadgetry (*page 70*), radio-frequency ID chips (*page 72*) and data fusion (*page 82*)—not to mention the viruses and other pests that infest the Internet (*page 96*).

In spite of all the threats to privacy, an astonishing variety of technology for protecting privacy has been devised, yet it lies virtually untapped (*page 88*). Maybe part of the reason is that so many young adults find all the anxieties about privacy to be much ado: many in the new generation are only too happy to trade their parents' version of "private information" for a rich life in the fishbowl of social networking (*page 100*).

For all those reasons and more, the editors of *Scientific American* present this issue devoted to the future of what Supreme Court Justice Louis D. Brandeis called "the right to be let alone." ■

JEAN-FRANCOIS PODEVIN



REFLECTIONS ON PRIVACY 2.0

Many issues posing as questions of privacy can turn out to be matters of security, health policy, insurance or self-presentation. It is useful to clarify those issues before focusing on privacy itself

By Esther Dyson

KEY CONCEPTS

- Erosions of privacy are often better understood as other kinds of harms.
- "Loss of privacy" may really be a loss of security.
- Much (though not all) anxiety about genetic privacy would go away if medical care were affordable to everyone.
- Citizens should have the right to monitor and post information about the activities of government and government officials.
- People are gaining effective tools to control what personal information they want to give out and to whom. —*The Editors*

Privacy is a public Rorschach test: say the word aloud, and you can start any number of passionate discussions. One person worries about governmental abuse of power; another blushes about his drug use and sexual history; a third vents outrage about how corporations collect private data to target their ads or how insurance companies dig through personal medical records to deny coverage to certain people. Some fear a world of pervasive commercialization, in which data are used to sort everyone into one or another "market segment"—the better to cater to people's deepest desires or to exploit their most frivolous whims. Others fret over state intrusion and social strictures.

Such fears are typically presented as tradeoffs: privacy versus effective medical care, privacy versus free (advertising-driven) content, privacy versus security. Those debates are all well worn, but they are now returning to the fore in a way they did not when specialists, insiders and die-hard privacy advocates were the only ones paying attention.

On the one hand, the erosion of privacy is unmistakable. Most Americans are online today, and most of us have probably had one or more "Now how did they know that?" experiences. The U.S. administration is breaching people's privacy right and left, while conducting more and more of its operations in obscurity. It has become hard to act anonymously if someone—particularly the government—makes any effort to find out who you are.

On the other hand, new and compelling reasons have arisen for people to disclose private information. Personalized medicine is on the threshold of reality. Detailed and accurate health and genetic information from private medical histories, both to treat individuals and to analyze epidemiological statistics across populations, has enormous potential for enhancing the general social welfare. Many people take pleasure in sharing personal information with others on social-networking Web sites. More darkly, the heightened threat of terrorism has led many to give up private information for illusory promises of safety and security.

Much of the privacy that people took for granted in the past was a by-product of friction in finding and assembling information. That friction is mostly gone. Everyone lives like a celebrity, their movements watchable, their weight gains or bad hair days the subject of comment, questions once left unspoken now explicitly asked: Was that lunch together a "date"? Which of my friends is a top friend?

Boundary Conditions

This issue of *Scientific American* focuses mostly on technologies that erode privacy and technologies that preserve it. But to help frame the discus-

MARK CLEMENS (*photoillustration*); RICHARD NOWITZ *National Geographic Collection* (*crowd scene*)

sion I'd like to lay out three orthogonal points.

First, in defining some disclosure of information as a breach of privacy, it is useful to distinguish any objective harms arising from the disclosure—fraud, denial of a service, denial of freedom—from any subjective privacy harms, in which the mere knowledge by a second or third party of one's private information is experienced as an injury. In many cases, what is called a breach of privacy is actually a breach of security or a financial harm: if your Social Security number is disclosed and misused—and I probably give mine out several times a month—that's not an issue of privacy; it's an issue of security. As for breaches of *privacy*, the "harm" a person feels is subjective and personal. Rather than attempting to define privacy for all, society should give individuals the tools to control the use and spread of their data. The balance between secrecy and disclosure is an individual preference, but the need for tools and even laws to implement that preference is general.

Second, as the borders between private and public are redrawn, people must retain the right to bear witness. When personal privacy is increasingly limited in a friction-free world of trackable data, the right of individuals to track and report on the activities of powerful organizations, whether governments or big businesses, is key to preserving freedom and to balancing the interests of individuals and institutions.

The third point elaborates on the first: in assessing the changes in the expectations people have about privacy, it is important to recognize the granularity of personal control of data. Privacy is not a one-size-fits-all condition: Different people at different times have different preferences about what happens to their personal information and who gets to see it. They may not have the right or ability to set such conditions in coercive relationships—in dealing with a government entity, for instance, or with an organization such as an employer or an insurance company from which they want something in return. But people often have a better bargaining position than they realize. Now they are gaining the tools and knowledge to exploit that position.

Objective Harms

Security is not the only public issue posing as privacy. Many issues of medical and genetic privacy, for instance, are really issues of money and insurance. Should people in poor health be compelled to pay more for their care? If you think they should not, you might feel forced to conclude that they should tacitly be allowed to lie. This conclusion is often misleadingly positioned as the protection of privacy. The real issue, however, is not privacy but rather the business model of the insurance industry in the U.S. People would not care about medical privacy so much if revealing

INCREASING TRANSPARENCY of traditional personal boundaries in our society, brought on by the Internet, will force people to confront ethical issues that would not have arisen when information was more highly compartmentalized. The fictionalized personal profiles given above illustrate this point. If they genuinely applied to the people shown and were posted online, some thorny ethical issues would emerge.

[THE AUTHOR]

Esther Dyson is an active investor in a variety of start-ups, including 23andMe (consumer genome information), PatientsLikeMe (online medical-information sharing) and Boxbe (user-driven e-mail preferences). For the Personal Genome Project she and nine other people will post their full genome sequences and accompanying health information online. She notes: "I was recently in the market for health insurance. I asked my insurance broker if he would like a copy of my genome, and he politely declined." She is author of *Release 2.0,* a book that addressed online privacy way back in 1997.

the truth about their health did not expose them to costly medical bills and insurance premiums.

Genetic data seem to present a particularly troubling example of the potential for discrimination. One fear is that insurance companies will soon require genetic tests of applicants—and will deny insurance to any applicant with a genetic risk. A genome does indeed carry a fair amount of information; it can uniquely identify anyone except an identical twin, and it can reveal family relationships that may have been hidden. Some rare diseases can be diagnosed by the presence of certain genetic markers.

But genes are only one factor in a person's life. Genes tell little about family dynamics, and they cannot say what a person has done with inherited abilities. Genes typically make themselves felt through complex interactions with upbringing, behavior, environment and sheer chance.

And genetic discrimination may soon be against the law anyway. This past May, President George W. Bush signed into law the Genetic Information Nondiscrimination Act (GINA), which outlaws discrimination in insurance and employment on the basis of genetic tests.

Nevertheless, the coming flood of medical and genetic information is likely to change the very nature of health insurance. With better liquidity of health information about a broad population and with better tracking of the outcomes of treatments and diseases, accurate prediction on the basis of statistical studies becomes progressively easier. But if individuals can be assigned to so-called cost buckets with reasonable accuracy, insuring people against high medical costs is no longer a matter of community rating—that is, pooling collective assets against unknown individual risks. Rather it is a matter of mandating subsidies paid by society to provide affordable insurance to those whose high health risks would otherwise make their insurance premiums or treatment prohibitively expensive.

As a consequence, society will have to decide, clearly and openly, which kinds of discrimination are acceptable and which are not. All of us will be forced to confront ethical choices crisply rather than hiding behind the confusion of information opacity. If insurance companies are asked to administer subsidies, they will demand clear rules about which individual health costs, and what proportion of them, society wants—and will pay—to provide. (The trick, as ever, is to make sure the insurers and health care providers keep costs down by providing good care and maintaining their customers' health rather than by limiting care. Increased information about health risks and treatment outcomes that I mentioned earlier will help measure the effectiveness of care and make that happen.)

The Right to Bear Witness

People really need rules about privacy when one party is in a position to demand data from another. The most important example is the government's power to collect and use (or misuse) personal data. That power needs to be limited.

What is the best way to limit government power? Not so much by rules that protect the privacy of individuals, which the government may decline to observe or enforce, but by rules

RICK SMOLAN (*Dyson*); SOURCE FOR TIMELINE: *BEN FRANKLIN'S WEB SITE*, BY ROBERT ELLIS SMITH. PRIVACY JOURNAL, 2000 (WWW.PRIVACYJOURNAL.NET); MPI/GETTY IMAGES (*Puritans*); IMAGEZOO/IMAGES.COM/CORBIS (*envelope*); TODD GIPSTEIN *Corbis (Preamble to U.S. Constitution)*

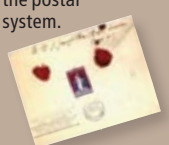
[TIMELINE]

SOCIAL LIFE AND TECHNOLOGY

1600s: The clergy, who keep records of births, marriages and deaths, cast an ever widening net for information about civic affairs. In Massachusetts "tythingmen," or government watchdogs, inspect households for proper moral conduct.

1700s: Little privacy exists within households; family members and even guests customarily share beds.

1700s: Mail is routinely opened as it passes through the postal system.



1800s: The "penny press" publishes unbridled gossip about the private lives of celebrities, under the protection of the First Amendment.

1838: The telegraph is introduced, and the bugging of telegraphed messages begins.

c. 1900: Fingerprints are established as unique and unchangeable identifiers.

1600 | 1700 | 1800 | 1900

Privacy in America, 1600–2008

Americans paradoxically combine an unquenchable curiosity with an insistence on being left alone.

1600s: Under Puritan rules, it is a civic duty to keep an eye on your neighbor. In many towns, people are forbidden to live alone.

1700s: Private life is seen as a haven from public turmoil. The colonists concur with the English and the Romans that "a man's house is his castle."

1791: The Bill of Rights protects freedom of speech and freedom from unreasonable search and seizure.

1787: The U.S. Constitution stipulates that a census be conducted once a decade. Many people regard the census with mistrust.

1890: Samuel D. Warren, Jr., and Louis D. Brandeis argue for a right to privacy in the *Harvard Law Review.*

LAW AND POLICY

that limit the privacy of the government and of government officials. The public must retain the right to know and to bear witness.

A primary instrument for ensuring that right has traditionally been the media. But the Internet is giving people the tools and the platform to take things into their own hands. Every camera and video recorder can bear public witness to acts of oppression, as the Rodney King video showed dramatically back in 1991 and as the Abu Ghraib photographs showed in 2004. The Internet is the platform that gives everyone instant access to a potentially worldwide audience. Reports from nongovernmental organizations (NGOs) and from private citizens around the globe are distributed on the Internet via social-networking and file-sharing sites and as cell phone text messages.

Ironically, perhaps the best model for what citizens should require of government is the kind of information that government requires of business. Business disclosure rules are tightening all the time—about labor practices, financial results, everything a business does. Investors have a right to know about the company they own, and customers have a right to know about the ingredients in the products they buy and how those products were made.

By the same token, citizens have a right to know about the job-related behavior of the people we elect and pay. We have a right to know about conflicts of interest and what public servants do with their (our) time. We should have the same rights vis-à-vis government that shareholders and customers (and, for that matter, the U.S. Securities and Exchange Commission) have vis-à-vis a publicly traded company. In fact, I would argue, citizens have extra rights with respect to government precisely because we are coerced into giving governments so much data. We should be able to monitor what the government does with our personal data and to audit (through representatives) the processes for managing the data and keeping them secure. The Sunlight Foundation (www.sunlightfoundation.com), of which I am a trustee, is encouraging people to find out and post information about their congressional representatives and, ultimately, about all public servants.

DILEMMAS OF I.D.

People need to be able to prove their identity to get a job, drive a car, get credit, and the like.

But so much personal information is available that it is relatively easy to assume the identity of someone real.

Meanwhile what is society to do about the people who can't or don't want to prove who they are: illegal immigrants, people trying to reinvent themselves, people just trying to be private?

Sunshine for Businesses

As for businesses' privacy rights, they don't (and shouldn't) have many. True, they have a right to record their own transactions with customers—and transactions done on credit typically require customers to prove their creditworthiness by giving up private information. But just as a company can refuse to sell on credit, a consumer can refuse to do business with a company that asks for too much data. Beyond that, everything should be negotiable. Customers can demand to know what companies are doing with their data, and if the customers don't like the response, they can move on. What the law needs to enforce is that companies actually follow the practices they disclose.

As with disclosures by government (and especially by politicians when they run for office), disclosure about businesses is going beyond what is required by regulation. In every sphere of activity, the little guy is biting back. All kinds of Web sites are devoted to ratings, discussions and oth-

1973: "There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy."
—Horst Feistel, "Cryptography and Computer Privacy"; *Scientific American,* May 1973.

1976: Whitfield Diffie and Martin E. Hellman invent public-key encryption.

1980s: DNA fingerprinting and cellular telephones become commonplace.

1989: The World Wide Web service is added to the Internet.

1995: The term "spyware" is used for the first time.

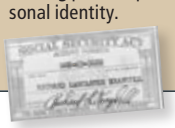
2004: Facebook, the popular social-networking Web site, makes its debut.

facebook

1950 | **1975** | **2000**

1928: The U.S. Supreme Court rules that the seizure of electronic conversations is constitutional.

1936: Social Security numbers are assigned to most adult Americans and become a lifelong piece of personal identity.



1966: Freedom of Information Act (FOIA) is passed.

1968: The Omnibus Crime Control and Safe Streets Act, Title III (sometimes referred to as the "end of privacy"), specifies when a warrant is required for wiretapping.

1978–1994: Congress passes refinements to the wiretapping laws, first in response to the abuses of the Watergate era and later to require telecommunications companies to be "wiretap-ready."

2001: The USA PATRIOT Act grants authorities broad discretion to search databases and conduct surveillance.

2008: Congress updates the 1978 wiretapping law, expanding the surveillance powers of the executive branch.

ARCHIVE HOLDINGS, INC. (*computer technician*); BETTMANN/CORBIS (*Social Security card* and *man with listening device*); GÜRKAN SENGÜN *http://livecd.gnustep.org* (*Web page*); FACEBOOK (*logo*)

BENEFITS AND HARMS of electronic record-keeping are sharply portrayed by the dilemma of making health records available online. Such records could save the life of an unconscious accident victim (*left*). But if the records disclose potentially expensive health problems, insurance coverage could be denied (*above*).

TWO-WAY STREET

The right to bear witness, to track and report on the activities of government, just as government collects information on us, is key to preserving freedom.

U.S. citizens have historically kept an eye on government via:
- **News media**
- **Congressional Record**
- **Other public records**
- **Freedom of Information Act (FOIA), and the like**

The Internet offers new tools for monitoring and uncovering:
- **Activities of public officials**
- **Conflicts of interest**
- **What happens to personal data given up to the government**
- **How those data are kept secure**

er user-generated content about services—hotels, doctors, and the like—as well as products. To be sure, many of the hotel reviews are posted by the hotels themselves or by their competitors. (To discourage such tactics, some sites require user biographies and encourage users to rate the credibility of the other users and reviewers.) Patients can check out doctors and hospitals on a variety of sites, from HealthGrades.com (a paid service) to a number of sites funded by advertising.

For user information about physical products, consider a proposed new service called Barcode Wikipedia (www.sicamp.org/?page_id=21). This service will enable users to post whatever they know or can find out about a product—its ingredients or components, where it was manufactured or assembled, the labor practices of the maker, its environmental impact or side effects, and so on. Companies are free to post on the site as well, telling their side of the story. With such open access, of course, postings are likely to include exaggerations and untruths as well as useful information. Yet with time—as Wikipedia itself has demonstrated—users will police other users, and the truth, more or less, will emerge.

Public Lives

Until recently, privacy for most people was afforded (though not guaranteed) by information friction: Information about what you did in private didn't travel too far unless you were famous or went to extreme lengths to be public about your activities. Now the concept of privacy itself is changing. Many adults are appalled at what they find on Facebook or MySpace. Some adolescents are aware of the risks of using social-networking Web sites but don't take them seriously—a teenage shortcoming from time immemorial. And it's likely that some kind of statute of limitations on foolish behavior will emerge: Most employers (who can search the Web pages of job applicants as well as anybody) will simply lower their standards and keep hiring, though some may remain stricter. Just think of tattoos: 20 years ago adults warned kids against getting them. Now every second woman in my health-club locker room seems to have a tattoo, and I assume it's the same proportion or more for the men.

Kids still have a sense of privacy, and they can still be hurt by the opinions of others. It's just that more of them are used to living more of their lives in public than their parents are. I think that's a real change. But the 20th century was also a change from the 19th century. In the 19th century few people slept alone: children slept together in one room, if not with their parents. Some rich people had rooms of their own, but they also had servants to take out their chamber pots, help dress them and take care of their most intimate needs. Our 20th-century notions of physical privacy are quite new.

For centuries before that, most people in most villages knew a great deal about one another. Yet little was explicit. What was different in the past is that Juan could not go online and see what Alice was saying. Juan might have guessed what Alice knew, but he didn't have to face the fact that Alice knew it. Likewise, Juan could easily avoid Alice. Today if Juan is Alice's ex-boyfriend, he can torment himself by watching her flirt online. Is there such a concept as privacy from one's own desires?

COMSTOCK/CORBIS (*ambulance*); RANDY FARIS *Corbis (mug shot)*; LARRY DOWNING *Sygma/Corbis (presidential seal)*

My Data, Myself

A second major change in personal privacy is that people are learning to exert some control over which of their data others can see. Facebook has given millions of people the tools—and, somewhat inadvertently, practice in using them. Last year Facebook annoyed some of its users with Beacon, a service that tracked their off-site purchases and informed their friends. The practice had been disclosed, but not effectively, and as a result many users discovered the privacy settings they had previously ignored. (Facebook subsequently rejiggered things to a more sensible approach, and the fuss died down.) Now many members change their privacy settings, both for incoming news from their friends (do you really want to know every time Matt goes on a date?) and for outgoing news to your friends (do you really want to tell everyone about your sales trip to Redmond, Wash.?). Users can share photographs within private groups or post them for all to see.

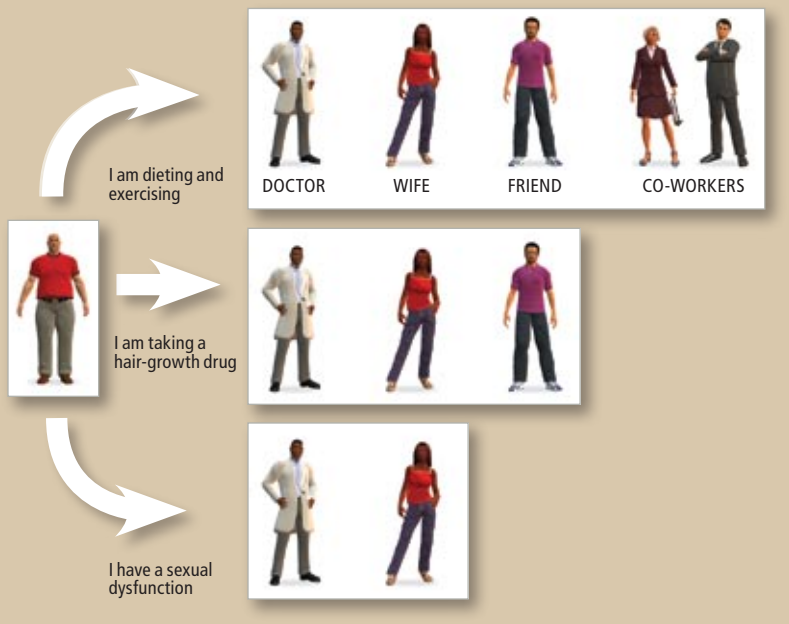
Flickr, a Web site for sharing photographs, enables users to control who sees them, albeit in a limited way. (Full disclosure: I was an investor in Flickr.) But those controls are likely to get more precise. Now, if you want, you can define a closed group, but that's not quite the same as being able to make selective disclosures to specific friends. For example, you might want to create two intersecting family groups: one comprising your full siblings and your mother; the other comprising all your siblings plus your father and your stepmother but not your mother. Other people might create other family subsets—a father and his children, for instance, but not his new wife—the mere existence of which may call for privacy.

The blogger and social-networking expert danah boyd (yes, all lowercase), who is a nonresident fellow at Harvard University's Berkman Center for Internet & Society, recently waxed eloquent about users' desire to control exactly who sees their posts and what ads accompany those posts. In other words, what matters is not the ads I see; it's the ads my friends see on "my" Web page. The issue for boyd—and for many other people—is not privacy so much as presentation of self (including, in boyd's case, her own name). People know they cannot control everything others say about them, but they will flock to online-community services that enable them to control how they present themselves online, as well as who can see which of those presentations.

[CONTROLLING SELF-PRESENTATION]

Disclosure by Degrees

A bald, overweight man might want to control the release of various parts of his electronic medical records to an ever narrowing circle of people. His baldness and his weight are obvious (if not precise), but he sees no need for knowledge of his participation in his employer's diet and exercise program to go beyond his doctor, wife, friends and co-workers. He is willing for his doctor, wife and close friends to know about his antibalding medication, but he wants only his doctor and his wife to know about his sexual dysfunction.



That kind of control will extend, I believe, to the notion of "friending" vendors. Alice is happy for the vendor that sold her a size 42 red sweater to know her purchasing habits, but she doesn't want her friends, her current boyfriend or other vendors to have access to that information. Of course, Alice has no control over what other people say or know about her. If Juan continues wearing the red sweater even after their breakup, some may notice. And they can combine that information in lots of ways.

Nevertheless, transparency doesn't make things simple. These new social tools make services and things, lives and relationships, appear exactly as complicated as they are—or perhaps as complicated as anyone cares to uncover. And the reality is that no single truth—or simple list of who is allowed to know what—exists. Ambiguity is a constant of history and novels, political campaigns and contract negotiations, sales pitches, thank-you letters and compliments, to say nothing of divorces, lawsuits, employee resignations and halfhearted invitations to lunch. Adding silicon and software won't make the ambiguity go away. ■

MORE TO EXPLORE

Privacy 2.0: A Design for Living in the Digital Age. Esther Dyson. Broadway Books, 1997.

Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet. Robert Ellis Smith. Privacy Journal, 2000. **www.privacyjournal.net**

For Esther Dyson's thoughts on disclosure and transparency, visit **www.huffingtonpost.com/esther-dyson**

For more information about the Personal Genome Project, visit **www.personalgenomes.org**

To learn more about the Sunlight Foundation and its tools for transparency, visit **www.sunlightfoundation.com**

KENN BROWN *Mondolithic Studios*

BRAVE NEW WORLD OF WIRETAPPING

As telephone conversations have moved to the Internet, so have those who want to listen in. But the technology needed to do so would entail a dangerous expansion of the government's surveillance powers

By Whitfield Diffie and Susan Landau

As long as people have engaged in private conversations, eavesdroppers have tried to listen in. When important matters were discussed in parlors, people slipped in under the eaves—literally within the "eavesdrop"—to hear what was being said. When conversations moved to telephones, the wires were tapped. And now that so much human activity takes place in cyberspace, spies have infiltrated that realm as well.

Unlike earlier, physical frontiers, cyberspace is a human construct. The rules, designs and investments we make in cyberspace will shape the ways espionage, privacy and security will interact. Today there is a clear movement to give intelligence activities a privileged position, building in the capacity of authorities to intercept cyberspace communications. The advantages of this trend for fighting crime and terrorism are obvious.

The drawbacks may be less obvious. For one thing, adding such intercept infrastructure would undermine the nimble, bottom-up structure of the Internet that has been so congenial to business innovation: its costs would drive many small U.S. Internet service providers (ISPs) out of business, and the top-down control it would require would threaten the nation's role as a leader and innovator in communications.

Furthermore, by putting too much emphasis on the capacity to intercept Internet communications, we may be undermining civil liberties. We may also damage the security of cyberspace and ultimately the security of the nation. If the U.S. builds extensive wiretapping into our communications system, how do we guarantee that the facilities we build will not be misused? Our police and intelligence agencies, through corruption or merely excessive zeal, may use them to spy on Americans in violation of the U.S. Constitution. And, with any intercept capability, there is a risk that it could fall into the wrong hands. Criminals, terrorists and foreign intelligence services may gain access to our surveillance facilities and use them against us. The architectures needed to protect against these two threats are different.

Such issues are important enough to merit a broad national debate. Unfortunately, though, the public's ability to participate in the discussion is impeded by the fog of secrecy that surrounds all intelligence, particularly message interception ("signals intelligence").

A Brief History of Wiretapping

To understand the current controversy over wiretapping, one must understand the history of communications technology. From the devel-

KEY CONCEPTS

- The advent of computer-based telephone switches and the Internet has made it more difficult for the government to monitor the communications of criminals, spies and terrorists.
- Federal agencies want Internet companies to comply with the same wiretapping requirements that apply to telecommunications carriers. This proposal, though, may stifle Internet innovation.
- Furthermore, the new surveillance facilities might be misused by overzealous government officials or hijacked by terrorists or spies interested in monitoring U.S. communications.

—The Editors

HARRY CAMPBELL

opment of the telephone in the 19th century until the past decade or two, remote voice communications were carried almost exclusively by circuit-switched systems. When one person picked up the phone to call another, one or more telephone switches along the way would connect their wires so that a continuous circuit would be formed. This circuit would persist for the duration of the call, after which the switches would disconnect the wires, freeing resources to handle other calls. Call switching was essentially the only thing that telephone switches did. Other services associated with the telephone—call forwarding and message taking, for example—were handled by human operators.

Wiretapping has had an on-and-off legal history in the U.S. The earliest wiretaps were simply extra wires—connected to the line between the telephone company's central office and the subscriber—that carried the signal to a pair of earphones and a recorder. Later on, wiretaps were installed at the central office on the frames that held the incoming wires. At first, the courts held that a wiretap does not constitute a search when it involves no trespass, but over time that viewpoint changed. In 1967 the U.S. Supreme Court decided in the case of *Katz v. United States* that the interception of communications is indeed a search and that a warrant is required. This decision prompted Congress in 1968 to pass a law providing for wiretap warrants in criminal investigations. But Congress's action left the use of wiretapping for foreign intelligence in legal limbo. Congressional investigations that followed the 1972 Watergate break-in uncovered a history of presidential operations that had employed and, as it turned out, abused the practice, spying on peaceful, domestic political organizations as well as hostile, foreign ones. So, in 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA), which took the controversial step of creating a secret federal court for issuing wiretap warrants.

Most of the surveillance of communications for foreign intelligence purposes lay outside the scope of the wiretapping law, because this activity had primarily involved the interception of radio signals rather than physical intrusions into phone systems. (When operating in other countries, American intelligence services could not place wiretaps on phone lines as easily as they could in the U.S.) Another important distinction between domestic and foreign communications surveillance is scale: inside the U.S., wiretapping has traditionally been regarded as an extreme investigative technique, something to be applied only to very serious crimes. Outside the country, though, the interception of communications is big business. The National Security Agency (NSA) spends billions of dollars every year intercepting foreign communications from ground bases, ships, airplanes and satellites.

How do we guarantee that the communications surveillance facilities we build will not be misused?

But the most important differences are procedural. Within the U.S. the Fourth Amendment to the Constitution guarantees the right of the people to be free from "unreasonable searches and seizures." The logic of a "reasonable" search is that law-enforcement officers must make an unprivileged observation (that is, one that does not invade the suspect's privacy) whose results give them "probable cause" with which they can approach the courts for a search warrant. What they are not permitted to do, in either physical searches or wiretaps, is to search first and then use what they find as evidence that the search was legitimate. This procedure, however, is exactly what intelligence agents do, except that they usually do not employ their results to prosecute criminals. An intelligence officer relies on professional judgment and available information to make the decision to spy on a foreign target; the operation will then be judged as a success or failure depending on what intelligence was obtained and what resources were expended.

The rules established in FISA make three fundamental distinctions: between "U.S. persons" (citizens, legal residents and American corporations) and foreigners; between communications inside and outside the U.S.; and between wired and wireless communications. Briefly, wired communications entirely within the U.S. are

BETTMAN/CORBIS (*telephone receiver*); *NEW YORK TIMES*, PAGE 1, MAY 20, 1916 (*newspaper*); ANGEL FRANCO *AP Photo* (*Bell Labs sign*)

[MILESTONES]

A History of Listening In

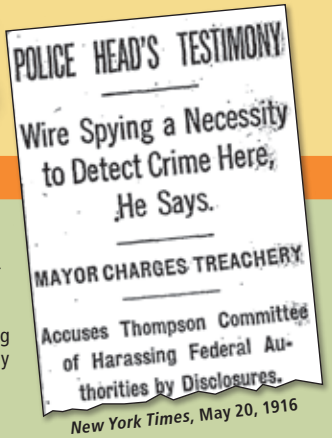
As the technology of voice communications has advanced, government surveillance has raised many legal issues.

1875

1876: Alexander Graham Bell invents the telephone.

1900

TECHNOLOGY


POLICE HEAD'S TESTIMONY

Wire Spying a Necessity to Detect Crime Here, He Says.

MAYOR CHARGES TREACHERY

Accuses Thompson Committee of Harassing Federal Authorities by Disclosures.

New York Times, May 20, 1916

1890s: Law-enforcement agencies begin tapping wires on early telephone networks.

LAW AND POLICY

protected—intercepting them requires a warrant. But radio communications that include people outside the country are protected only if the signal is intercepted in the U.S. and the government's target is a particular, known U.S. person who is in the country at the time.

Until recently, whenever the FISA rules applied, they imposed a burden similar to that imposed by ordinary criminal law. To seek a warrant, an intelligence agency had to specify a particular location, telecommunications channel or person and explain why the target should be subject to surveillance. Operating "foreign intelligence–style," intercepting communications and then using the recorded conversations to justify the interception, was not permitted.

Almost accidentally, the rules set by FISA included an important loophole that Congress had intended to be only temporary: radio communications involving parties who were not U.S. persons could be intercepted from inside the U.S. without warrants. At the time FISA was passed and for many years thereafter, the radio exemption was a great boon to the intelligence community. Satellite radio relays had revolutionized international communications in the 1960s and 1970s and carried most of the phone calls entering and leaving the country. Radio communications that were partly or completely among parties outside the U.S. were legally and physically vulnerable to interception by NSA antennas at places such as Yakima, Wash., and Vint Hill Farms in Virginia.

In the 1970s a new transmission medium emerged as an alternative for long-haul communications. Optical fibers—long, thin strands of glass that carry signals via laser light—offered great advantages in communicating between fixed locations. Fiber lines have tremendous capacity; they are not plagued by the quarter-second delay that slows satellite relays; they are intrinsically more secure than radio; and, for a combination of technical and business reasons, they have become very cheap. From the 1990s onward, the vast majority of communications from one fixed location to another have moved by fiber. Because fiber communications are "wired," U.S. law gives them greater protection. The intelligence community could not intercept these communications as freely as they could radio traffic, and the FISA rules began to chafe.

A particularly sensitive issue for intelligence agencies was the so-called transit traffic. Some 20 percent of the communications carried on U.S. networks originate and terminate outside the country, moving between Europe, Asia and Latin America. Transit traffic is not a new phenomenon; it was already present in the satellite era. But under FISA rules, the interception of fiber communications at points inside the U.S. required a warrant. This requirement upset the standard processes of intelligence agents, who were unaccustomed to seeking probable cause before initiating surveillance.

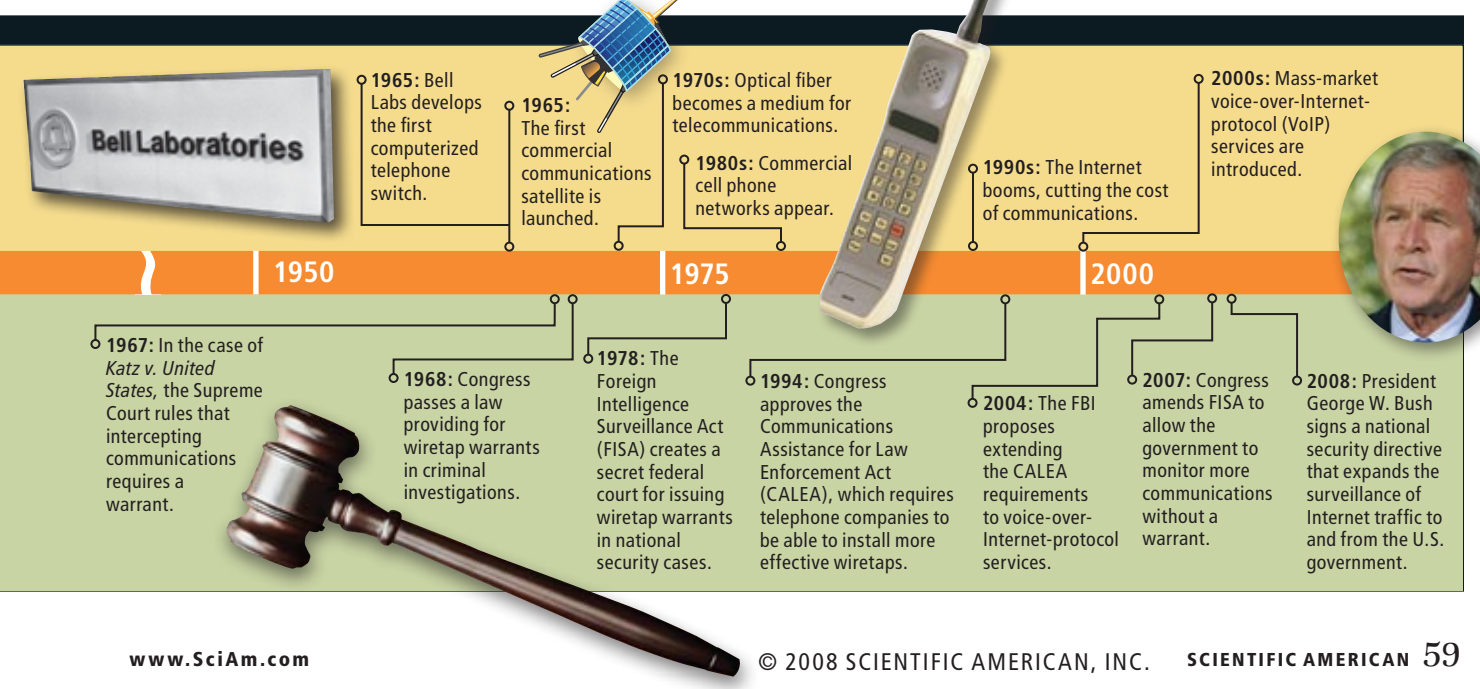
At about the same time, computer-based switching systems began to replace the traditional electromechanical switches in U.S. telephone networks. This computerization paved the way for services such as automated call forwarding and answering systems, which unintentionally but effectively bypassed standard wiretapping techniques.

MINIMIZATION

One of the important procedural differences between law-enforcement wiretapping and surveillance for foreign intelligence lies in the practice of minimization: avoiding the collection of communications other than the targeted ones. A wiretapped phone line, for example, may be used by several people, some of whom are not the targets of the investigation.

U.S. law requires the police to listen to a tapped conversation at the same time they record it and to stop the surveillance when the subjects are not discussing criminal activities.

In foreign intelligence gathering, the minimization rules are generally not so rigid, but because so many signals can be intercepted and analyzed, far more traffic must be discarded as irrelevant.



DAVID MUIR (*gavel*); JEN CHRISTIANSEN (*satellite*); LAWRENCE MANNING *Corbis* (*cell phone*); ROGER L. WOLLENBERG *Pool/CNP/Corbis* (*Bush*)

Suppose that a caller to a wiretapped phone left a message with an answering service provided by the telephone company. If the target of the investigation checked his messages from a phone other than his own, the communication would never travel over the tapped line and thus would not be intercepted.

Congress responded in 1994 with the Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications companies to make it possible for the government to tap all the communications of a targeted subscriber no matter what automated services the subscriber uses. In addition to mandating

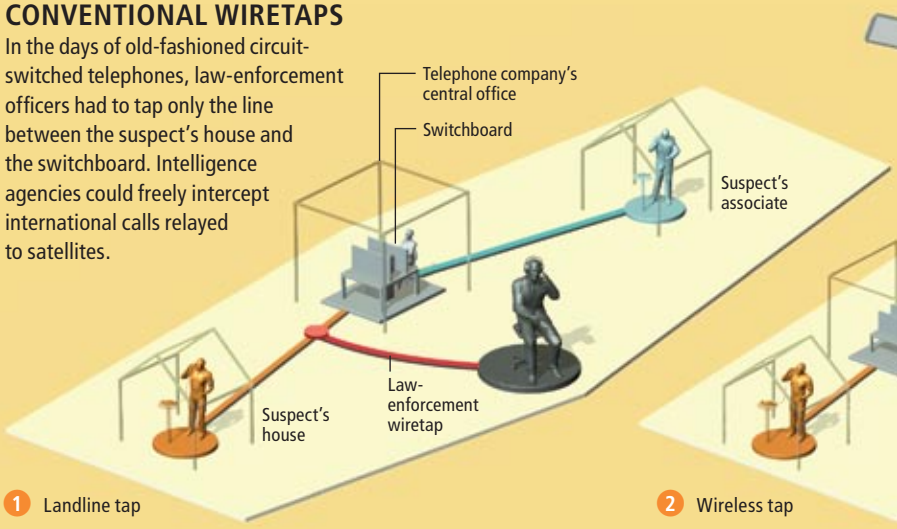
[THE BASICS]

Then and Now: Surveillance Gets Complicated

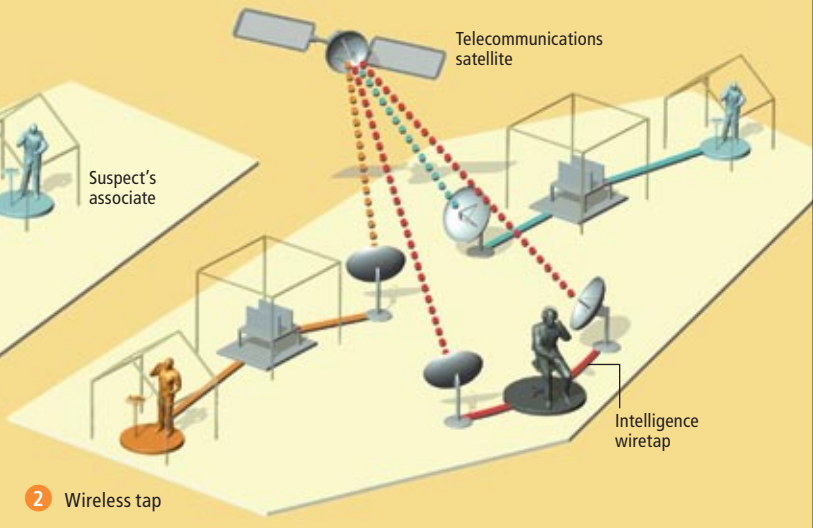
Monitoring voice communications has grown more technically challenging in recent years, requiring more simultaneous wiretaps.

CONVENTIONAL WIRETAPS

In the days of old-fashioned circuit-switched telephones, law-enforcement officers had to tap only the line between the suspect's house and the switchboard. Intelligence agencies could freely intercept international calls relayed to satellites.



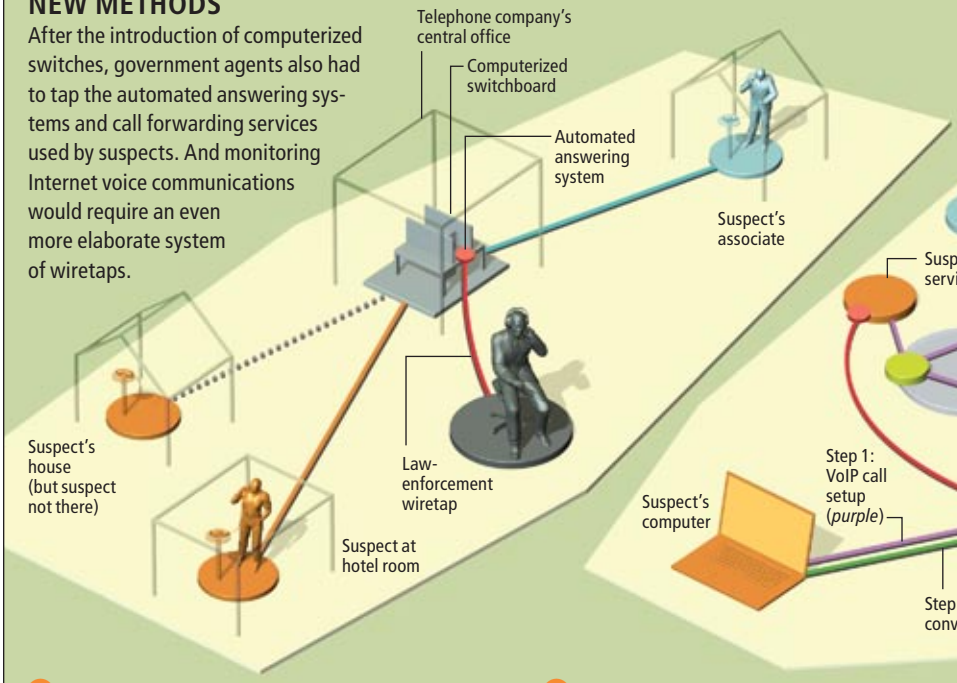
1 Landline tap



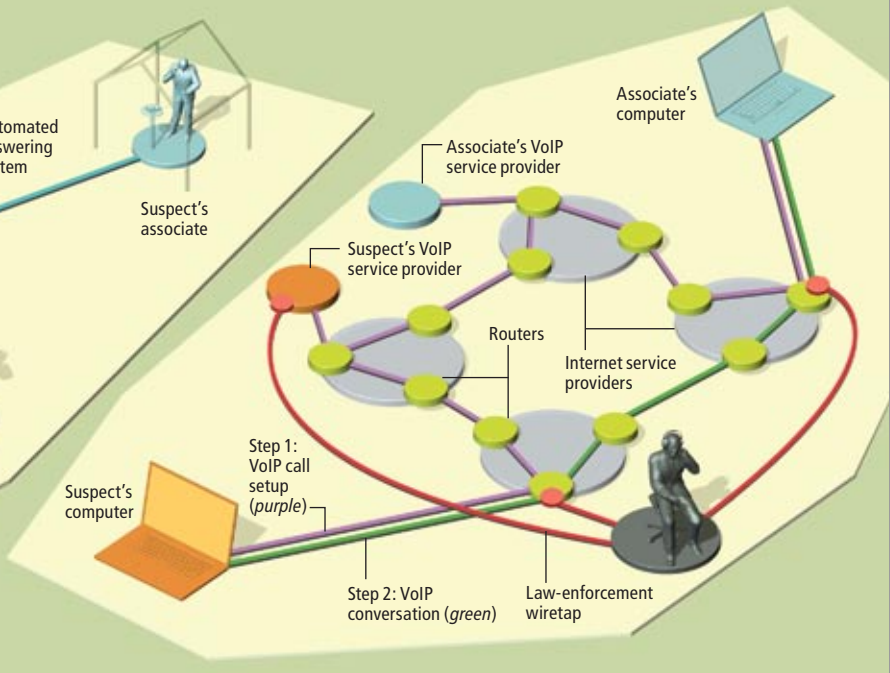
2 Wireless tap

NEW METHODS

After the introduction of computerized switches, government agents also had to tap the automated answering systems and call forwarding services used by suspects. And monitoring Internet voice communications would require an even more elaborate system of wiretaps.



3 Computerized networks



4 Tapping Internet communications

an improvement in the quality of information that can be obtained from wiretaps, CALEA obliged telecommunications carriers to be able to execute far more simultaneous wiretaps than had previously been possible.

Tapping the Net

CALEA was passed just as large numbers of people began using the Internet, which employs a communications method that is entirely different from circuit-switched telephony. Internet users send information in small packets, each of which carries a destination address and a return address, just like a letter in the postal system. With circuit switching, a brief telephone call incurs the same setup costs as a long one, so making a call to send only a few words is uneconomical. But on a packet-switched network, short messages are cheap and shorter messages are cheaper. Web browsing is possible because Internet connections can be used briefly and discarded. Each time you click on a Web link, you establish a new connection.

In the era of circuit-switched communications, wiretapping worked because telephone instruments, numbers and users were bound closely together. A telephone was hard to move, and a new telephone number was hard to get. An organization's messages moved on the same channels for long periods, so it was easy to intercept them repeatedly. Computerized switching and the Internet have made surveillance much more challenging. Today people can easily get new telephone numbers as well as e-mail addresses, instant messaging handles and other identifiers. And the advent of voice-over-Internet protocol (VoIP), the standard that allows the transmission of voice communications over packet-switched networks, has further decentralized control of the communications infrastructure. In a VoIP system such as the popular Skype service, for example, the setting up of phone calls and the transmission of traffic are entirely separate.

If CALEA, as interpreted literally, were applied to decentralized VoIP services, the provider would be required to intercept targeted customers' phone calls and relay them to the government but might be totally incapable of complying with such a demand. Consider a typical VoIP call running between the laptop computers of two people, both of whom are traveling. Alice initiates the call from a lounge at O'Hare airport in Chicago, and Bob receives it at a hotel bar in San Francisco. The VoIP provider's role in the process is limited: it discovers the Internet protocol (IP) addresses through which Alice and Bob are connected and communicates each person's address to the other's computer. After the setup is completed, the VoIP provider plays no further role. Instead the actual voice conversation is carried by the Internet service providers (ISPs) through which Alice and Bob access the Internet, together with other Internet carriers to which those ISPs are connected.

In this environment a government agency might have to serve wiretap warrants on many telecommunications carriers just to monitor a single target. Suppose we imagine a CALEA-style intercept regime that could capture a VoIP call. It must begin with an order to the VoIP provider targeting either Alice or Bob. When law-enforcement agents receive word from the provider that the target is engaged in a call, they must consider the IP addresses of Alice and Bob and send an intercept warrant to one or more ISPs at which the call can be intercepted. The ISPs must be prepared to accept, authenticate and implement the warrant in real time. One problem with this scenario is that only ISPs in the U.S. (and possibly some in cooperating countries) would be required to honor the warrant. A more serious difficulty is the massive security problem that such an arrangement would present. Anyone who could penetrate an ISP's wiretap function would be able to spy on its subscribers at will.

CALEA recognized the difference between traditional telephony and the Internet and exempted the Internet, referred to as "information services," from the provisions of the new law. Yet in 2004, despite that distinction, the U.S. Department of Justice, the Federal Bureau of Investigation and the U.S. Drug Enforcement Administration responded to the challenge of monitoring Internet communications by proposing that providers of broadband Internet access be required to comply with the CALEA requirements. The Federal Communications Commission and the courts have so far supported law enforcement in extending CALEA to "interconnected VoIP" (the form most like traditional telephony), relying on a provision of CALEA that refers to services that are a "substantial" replacement for the telephone system. This proposal, if adopted, would be the first step on a road leading to dangers not present in conventional wiretapping.

In particular, the government's actions threaten the continued growth of the Internet, which has become a hotbed of innovation as a consequence of its distributed control and loose con-

[THE AUTHORS]

Whitfield Diffie began his career in security as the inventor of the concept of public-key cryptography. In the 1990s he turned his attention to public policy and played a crucial role in opposing government key-escrow proposals and restrictive regulations on the export of products incorporating cryptography. He is now chief security officer at Sun Microsystems and is studying the impact of Web services and grid computing on security and intelligence. **Susan Landau** is a distinguished engineer at Sun Microsystems Laboratories, where she works on security, cryptography and policy, including surveillance and identity-management issues. Landau had previously been a faculty member at the University of Massachusetts Amherst and Wesleyan University, where she worked on algebraic algorithms.

ILLUSTRATIONS BY GEORGE RETSECK (*opposite page*); SUN MICROSYSTEMS (*Diffie*); NEIL IMMERMAN *University of Massachusetts* (*Landau*)

nectivity. Unlike a telephone carrier's network, the Internet is not centrally planned and managed. The addition of a new service, such as call forwarding, in the telephone system typically takes years of planning and development. But an Internet entrepreneur can start a new business in a garage or dorm room, using nothing but a home computer and a broadband connection. If law enforcement succeeds in mandating interception facilities for every Internet carrier, the industry as a whole could be pushed back into the procrustean bed of conventional telecommunications. To incorporate extensive surveillance capabilities, new Internet services would have to be developed in long cycles dependent on federal approval. In a century in which the great opportunities lie in information-based businesses, Americans must do everything possible to foster innovation rather than stifling it. If we do not, we may fall behind countries that follow a different course. Such an outcome would represent a long-term threat to national security.

Another threat is more immediate. Since the collapse of the Soviet Union, no opponent has had the ability to spy on U.S. communications with anything approximating comprehensive coverage. The Soviets had fleets of trawlers patrolling both coasts of the U.S., diplomatic facilities in major American cities, satellites overhead and ground bases such as the Lourdes facility near Havana. Their capabilities in signals intelligence were second to none. In comparison, the current opponents we most fear, such as al Qaeda, and even major nations such as China have no such ability. They are, however, trying to achieve it, and building wiretapping into the Internet might give it to them. Computers would control the intercept devices, and those computers themselves would be controlled remotely. Such systems could be just as much subject to capture as Web sites and personal computers. The government's proposed interception policies must be judged in the light of such vast and uncertain dangers.

Cyberwars

The administration of President George W. Bush recently relaxed some of the 30-year-old restrictions on communications surveillance mandated by FISA. In 2007 Congress, under intense pressure from the White House, passed the Protect America Act (PAA), which amended FISA by expanding the radio exemption to cover all communications. The law provided that any communication reasonably believed to have a participant outside the U.S. could be intercepted without a warrant. Given the degree to which business services in the U.S. are being outsourced to overseas providers, the new law made a large fraction of American commercial and personal telecommunications activity subject to monitoring. Congress was sufficiently nervous about this course of action that it provided for PAA to expire in 2008.

This past July, after months of controversy, Congress passed a bill fundamentally expanding the executive branch's wiretapping authority and reducing the FISA court's role in international cases to reviewing the general procedures of a proposed wiretap rather than the specifics of a case. Political debate over the bill, however, did not center on wiretapping authority, as one might expect for a sweeping change. Most attention focused instead on giving retroactive immunity for past illegal wiretapping.

In early 2008 the administration offered a new rationale for expanding communications surveillance: securing the Internet. The current state of Internet security is indeed abysmal. Most computers cannot protect themselves from penetration by malware—software designed to infiltrate and damage computer systems—and a substantial fraction of the computers linked to the Internet are under the control of parties other than their owners. These machines have been surreptitiously captured and organized into "botnets," whose computing power is then resold in a kind of electronic slave trade. In

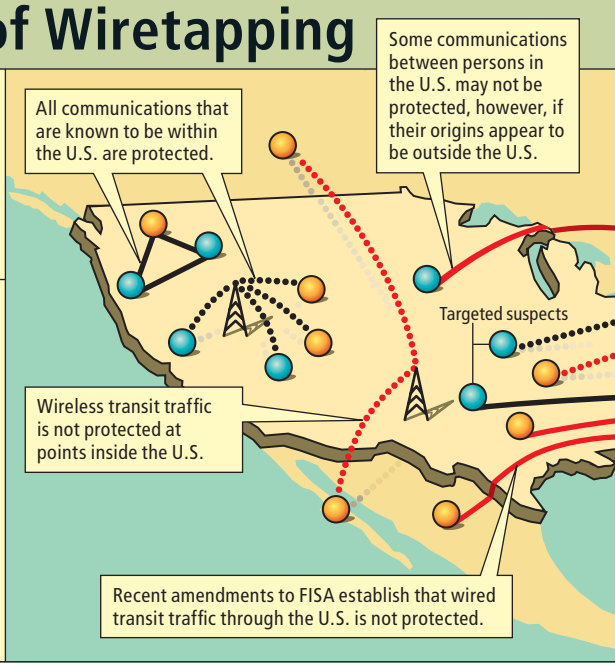
Communication is fundamental to our species; privacy of communication is fundamental to both our national security and our democracy.

[SURVEILLANCE LAW]

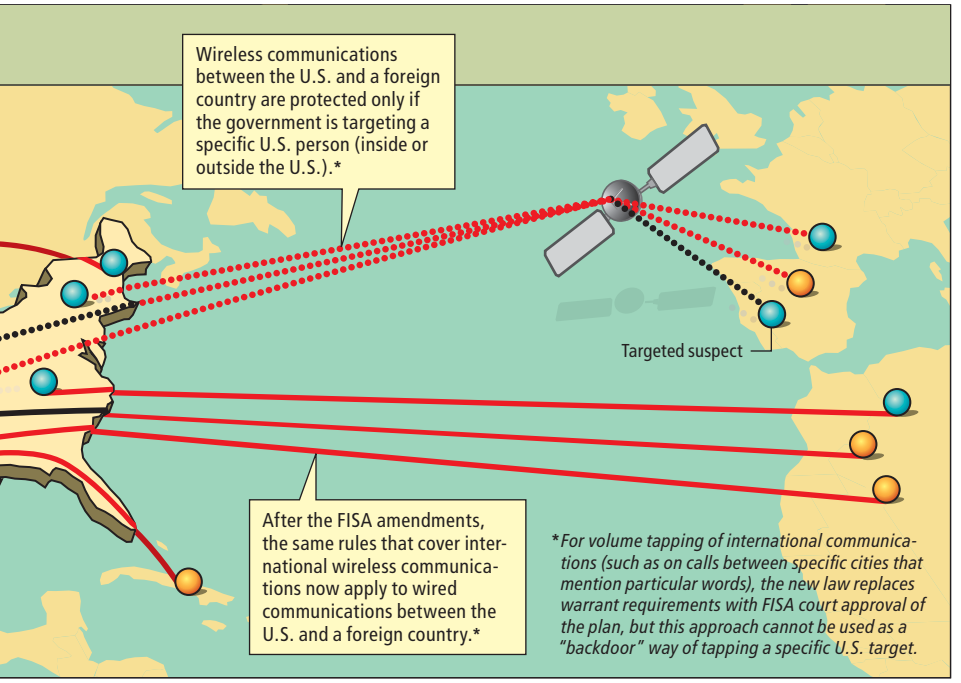
Geography of Wiretapping

The Foreign Intelligence Surveillance Act (FISA), amended this year, details which communications are legally protected and which can be monitored without a warrant.

- U.S. person (citizen, legal resident or American corporation)
- Non-U.S. person
- Wired (*solid*)
- Wireless (*dashed*)
- Protected communication (wiretap requires a warrant)
- Unprotected communication (can be tapped without a warrant)



JEN CHRISTIANSEN



response to the failure of traditional defensive approaches, President Bush signed a national security directive in January authorizing a Cyber Initiative. Most of the initiative is secret, but its initial move—extensive surveillance of the substantial amount of Internet traffic that moves in and out of the U.S. government—is too sweeping to be concealed. To facilitate the surveillance, the administration plans to reduce the number of connections between government agencies and the Internet from thousands to fewer than a hundred, and that requires changing or retiring thousands of IP addresses. The Cyber Initiative captures the dilemma of signals intelligence perfectly. A system that monitors federal communications for signs of foreign intrusion will also capture all the legitimate communications that Americans have with their government.

The administration is seeking the power to intercept American communications using the same tactics long employed in foreign intelligence gathering—that is, without having to go to the courts for warrants and describe in advance whose communications it intends to intercept. The advocates of expanded surveillance have valid concerns: not only do we face opponents who are not tied to particular nations and can move freely in and out of the U.S., we also have a critical cybersecurity problem. The Internet is swiftly becoming the primary medium for both commercial and government business, as well as the preferred communications method for many individuals. Its security problems are analogous to having the roads overrun with bandits or the sea-lanes controlled by pirates. Under these circumstances, it is not surprising to find the government seeking to patrol the Internet, just as the nation's police and armed services have patrolled the roads or the high seas in the past.

But policing the Internet, as opposed to securing the computers that populate it, may be a treacherous remedy. Will the government's monitoring tools be any more secure than the network they are trying to protect? If not, we run the risk that the surveillance facilities will be subverted or actually used against the U.S. The security problems that plague the Internet may beset the computers that will do the policing as much as the computers being policed. If the government expands spying on the Internet without solving the underlying computer security problems, we are courting disaster.

The inherent dangers are made worse by the secrecy surrounding the government's initiatives. One casualty of recent approaches to communications interception has been what might be called the two-organization rule. The security of many crucial systems, such as those controlling nuclear weapons, relies on the requirement that critical actions be taken by two people simultaneously. Until recently, federal law mandated a similar approach to wiretapping, allowing the government to issue wiretap orders but requiring the phone companies to install the taps. Under this arrangement, a phone company would be reluctant to act on a wiretap order it suspected was illegal, because its compliance would make it vulnerable to both prosecution and civil liability. Eliminating the role of the phone companies removes an important safeguard. If we follow this course, we may create a regime entirely out of view of Congress, the courts and the press—and perhaps entirely out of control.

The distance our world has moved into cyberspace in the past century is minuscule compared with the distance it will move in the next. We are in the process of building the world in which future humans will live, as surely as the first city dwellers did 5,000 years ago. Communication is fundamental to our species; private communication is fundamental to both our national security and our democracy. Our challenge is to maintain this privacy in the midst of new communications technologies and serious national security threats. But it is critical to make choices that preserve privacy, communications security and the ability to innovate. Otherwise, all hope of having a free society will vanish. ■

MORE TO EXPLORE

Information Privacy Law: Cases and Materials. Second edition. Daniel J. Solove, Marc Rotenberg and Paul Schwartz. Aspen, 2005.

Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. Steven M. Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson and John Treichler. Information Technology Association of America, 2006. Available at **www.itaa.org/news/docs/CALEAVOIPreport.pdf**

Privacy on the Line: The Politics of Wiretapping and Encryption. Updated and expanded edition. Whitfield Diffie and Susan Landau. MIT Press, 2007.

More information on communications surveillance issues is available at the Web sites of the Center for Democracy and Technology: **www.cdt.org;** the Electronic Frontier Foundation: **www.eff.org;** and the Electronic Privacy Information Center: **www.epic.org**

KEEPING YOUR GENES PRIVATE

In spite of recent legislation, tougher laws are needed to prevent insurers and employers from discriminating on the basis of genetic tests

By Mark A. Rothstein

KEY CONCEPTS

- Genetic testing will expand quickly and soon, adding highly targeted data to people's medical records. As those records go electronic, outsiders will find it increasingly easy to peruse an individual's health information.
- Able to uncover private details, health and life insurers could deny coverage to someone with a complex medical condition, and employers could fire or refuse to hire the person to avoid burdening the company health plan.
- Existing laws offer weak protection at best; legislation is needed to give individuals more control over their own data, to limit unauthorized disclosures by others and to penalize wrongdoers.

—The Editors

In years gone by, if colon cancer ran in your family all you could do was wait and worry about whether you might get it, too. Today a genetic test can determine whether you have inherited a greater-than-average risk of the disease and so could benefit from preventive care. The more doctors know about your genes, the better able they are to prevent, treat or cure illnesses.

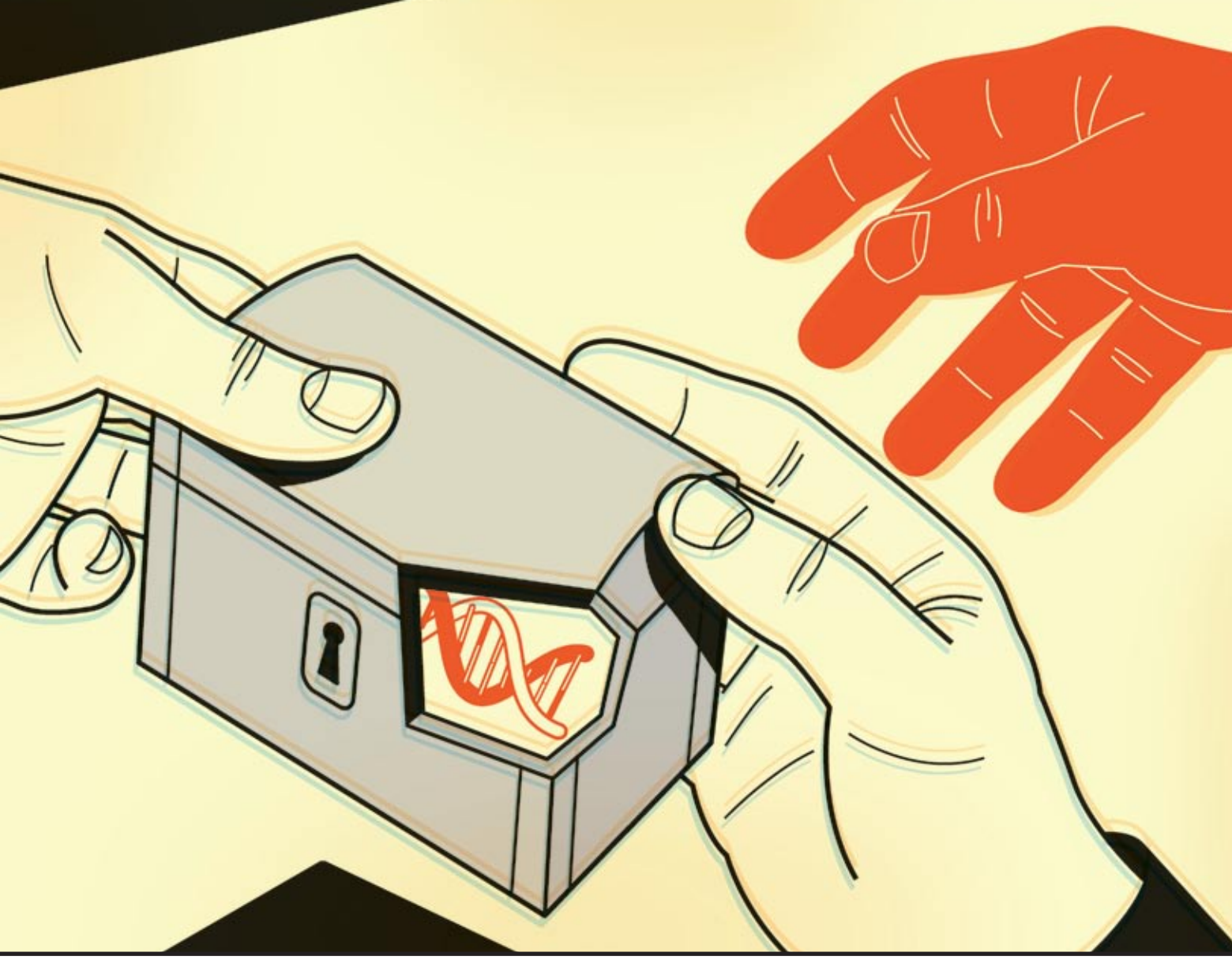
Excitement about such prospects surrounded the start of the Human Genome Project in 1990. But the enthusiasm was soon tempered by widespread concern about the need to protect the privacy of a person's genetic information. Simple tests that could readily reveal an individual's genetic endowment could also readily cause embarrassment or stigma. Furthermore, insurers could deny people health coverage or raise the premiums they have to pay. And employers seeing the results could deny people jobs or fire them. At the same time, scientists and public health officials recognized that the potential to improve health care based on genetic studies across large populations could never be achieved if legions of people refused to participate out of fear that the results could be misused.

Worries about discrimination have not come true—yet. Even though the Human Genome Project was completed in 2003, genetic testing has not become widespread, so there is little in the average person's health record to divulge. And genome-wide analyses remain costly—as much as several thousand dollars each. What is more, scientists still lack standard techniques for making whole-genome scans useful for health risk assessment.

Nevertheless, in many societies—particularly the wealthy ones—genetic testing for multiple disorders will soon become routine. New technologies and scientific discoveries are making the tests more useful and affordable. The health care sector's sweeping transition from paper to electronic records will also make genetic information more readily accessible. Safeguarding genetic privacy is more complicated than many people realize, and recently enacted laws such as the 2008 Genetic Information Nondiscrimination Act offer little protection. Better regulations must be developed soon, before testing spreads and abuses grow.

More Information Everywhere

Figuring out how best to secure genetic privacy would be simpler if "genetic information" and "genetic conditions" were easy concepts to define. But they are not. Medical investigators are finding that almost all illnesses have a genetic component. Distinguishing between genetic and nongenetic health information is becoming increasingly meaningless. Yet policymakers have been inclined to give special protection to genetic information. For legal purposes, the



most common definitions include the results of an individual's genetic tests, those of his or her family members, and the health histories of all these people (because disorders that run in families typically have a genetic link).

The data that fit into these categories are expanding noticeably. In the past decade genetic research and its clinical applications have shifted from disorders linked to a single gene, such as cystic fibrosis and muscular dystrophy, to more common and complex ills characterized by the interactions of multiple genes and environmental factors, including asthma, cancer, cardiovascular disease and diabetes. More than 1,500 genetic tests are now in use, and hundreds more are being developed. As these tools become part of standard medical practice, including primary care, most, if not all, health records will contain substantial genetic information.

Genome-wide analyses could vastly expand those contents. These tests can look for single changes in hundreds of thousands of nucleotide bases—the famous A, T, C and G "letters" of DNA code—associated with particular illnesses and conditions. Although most scientists think that it is premature to apply this technology routinely, some companies such as 23andMe in Mountain View, Calif., and deCODE Genetics in Reykjavik, Iceland, have started aggressively marketing genome-wide scans, even if they do not have a license to operate as a medical laboratory. Within a decade, whole-genome sequencing that reads all three billion bases in human DNA might well be available for less than $1,000.

At least two other factors will add to the amount of information in health records. The great desire for personalized medicine—drug therapies tailored to each person's body to improve effectiveness and reduce side effects—depends on genome-wide analytical tools. This "pharmacogenomic" testing is already becoming standard practice in selecting drugs and doses for treatment of certain cancers, and the trend

HARRY CAMPBELL

will continue. Likewise, "toxicogenomics"—the use of genome-wide tools to study how individuals respond to toxins—is becoming more important in assessing a person's health risks in the workplace and in the general environment.

Networks Amplify Risk

The challenge of protecting health information is compounded by an increasing reliance on digital data. Medical records of all kinds are shifting from largely paper-based systems to electronic health records (EHRs), which should improve the quality of care and reduce its cost. The transition is under way in many developed countries. In the U.S., a Nationwide Health Information Network (NHIN) is being developed as a "network of networks." Its key goal is establishing electronic formats that will make records of all kinds compatible and thus easy to transport across networks and across the country. Ultimately, a person's EHR will include all his or her medical information from "cradle to grave." The Office of the National Coordinator for Health Information Technology in the Department of Health and Human Services is leading the NHIN's development, but state governments and the private sector are engaged in research, development and trial implementation.

The NHIN raises contentious issues. In a paper-based system, privacy is mainly protected by chaos. Precisely because the system is fragmented, people find it impossible to compile, or even to locate, an individual's records from a multitude of providers in different locations over extended periods. But comprehensive, longitudinal records will inevitably contain sensitive information. Individuals will no longer have the option of "selective recall" in giving facts to health care providers or of obtaining care from one provider without the knowledge of another. Unlike today, an old diagnosis of depression made at a college mental health clinic or the results of a genetic test taken because of family history will become a permanent part of one's EHR. Many people with conditions that might stigmatize them, such as a history of substance abuse, might delay or forgo treatment. Such a result could be disastrous for individuals and for public health.

People fear they might not get a job if they could be a burden to the company medical plan.

INTRIGUED BUT WARY

According to a May 2008 Knowledge Networks survey:

Forty-seven percent of Americans are interested in using online personal health record services such as Google Health or Microsoft HealthVault. The services allow consumers to control their own medical records online.

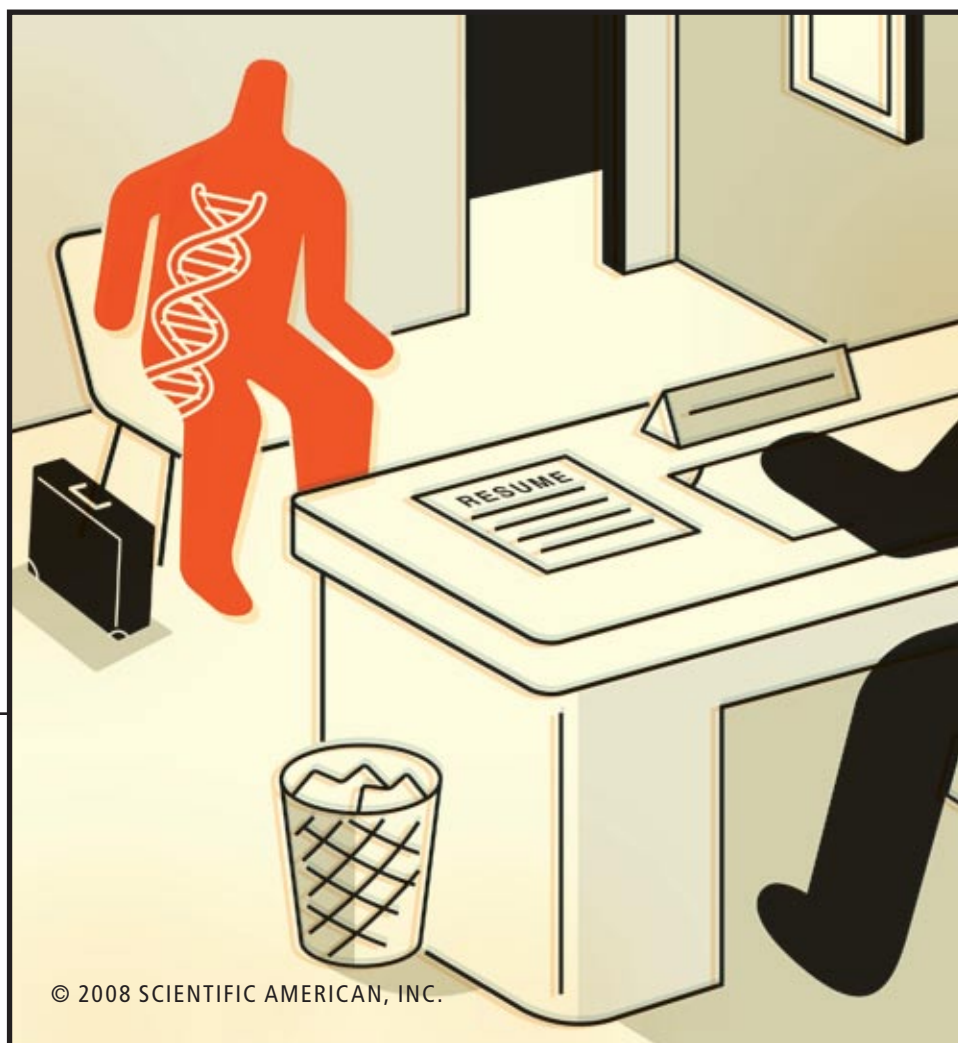
Ninety percent of the respondents, however, indicated they would be wary about the services' ability to keep records private.

In response, the Markle Foundation has recommended ways to make such systems as private as possible. Provisions would allow consumers to audit who is accessing their medical data and to dispute information provided by health care providers.

A full report is not needed to render effective care, however. A physician treating a sprained ankle does not need to know if a patient has a predisposition to breast cancer. A dentist filling a cavity does not need to find out about a family history of Huntington's disease.

To protect patients from unnecessary disclosures of sensitive information, countries such as Canada, the Netherlands and the U.K. are considering ways to restrict which information is revealed to which health care providers. These measures include giving patients complete control of their health records, permitting individuals to remove certain old information, limiting disclosures only to details needed for a given diagnosis or type of provider, applying special rules to sequester especially sensitive information, creating a subset of basic health data that would be available to all providers and establishing independent health record banks to disclose files according to a patient's direction. In Denmark's EHR network—one of the most advanced—people can "block" any information in their records. Although this option is rarely exercised, it is greatly valued.

The U.S. has no such measures in place. This



HARRY CAMPBELL

past February the National Committee on Vital and Health Statistics (which advises the secretary of health and human services) recommended that individuals be able to prevent the routine disclosure of sensitive health information in predefined categories, such as domestic violence, substance abuse, mental health, sexually transmitted diseases and genetic information. But methods for doing that have yet to be created. And how to strike the right balance between broad and narrow disclosure remains unclear. If patients have too much control, physicians will not have confidence in the accuracy or completeness of the records. In response, they will likely feel compelled to retake histories and order new tests, undermining the efficiencies of networks and adding cost to care. On the other hand, if patients have too little control, many may engage in defensive steps such as opting out of networks, paying cash for off-record services or declining certain care altogether.

Other issues must also be resolved. For example, should privacy rules be set for systems that scan electronic records and advise clinicians on possible drug interactions, so the systems do not divulge actual drugs taken? Should health care providers see an electronic notation in a patient's file indicating that certain health information has been made unavailable at the patient's request? And in such cases, will doctors have a way to lift those restrictions if the person needs emergency care?

Weak Laws

With more genetic information and far-reaching electronic networks on the horizon, legislation protecting health privacy is essential. Unfortunately, comprehensive laws do not exist in the U.S. The closest thing to a national safeguard is the 1996 Health Insurance Portability and Accountability Act (HIPAA) and the 2003 Privacy Rule attached to it. The Privacy Rule spells out the permissible uses and disclosures of individual health information by providers, plans and record clearinghouses.

There is a big loophole, however: the Privacy Rule applies only to entities that handle health claims data electronically. Hundreds of thousands of providers still do not, including doctors who take cash payments exclusively, fitness clubs that ask for medical information when putting members on workout plans and health care providers who work under contract to third parties, such as personnel in on-site employer clinics. A related problem is the lack of enforcement. About 36,000 complaints related to the Privacy Rule were filed with the Department of Health and Human Services's Office for Civil Rights between April 2003 and May of this year. Although corrections were made, only one civil monetary penalty has been assessed to date. Wrongdoers face few deterrents.

In addition, HIPAA only applies to entities involved in health care. The public, however, is most worried about stigma or discrimination from others. People fear complications when applying for a job, obtaining a life insurance policy or filing for workers' compensation benefits. Yet it is common for administrators involved in these and other everyday situations to require people to sign an authorization directing their provid-

DAVID ELLIS

Should Family Members Be Warned?

Sarah, a 40-year-old mother of three, has found out from various tests that she has an elevated risk of Alzheimer's disease, as well as of breast cancer. Does she have a legal or moral obligation to tell her children or close relatives that they, too, might be at high risk of getting these illnesses in the future?

The legal issue is straightforward: no court has held an individual liable for failing to warn a relative about genetic test results. The moral issue depends on many factors, including the severity of a genetic condition, the number of years before it is likely to produce symptoms, and whether the condition is treatable. The nature of relationships (parent and child) and their emotional closeness matter, too, as do relatives' ages, their interest in knowing about the chance of future ills, and the individual's own concern about not divulging his or her personal problems.

The nature of the danger often plays a strong role. In rare cases, genetic conditions can be lethal if combined with environmental stressors. For example, individuals with the genetic mutation for malignant hyperthermia can die during surgery if certain anesthesia is used. People with hypertrophic cardiomyopathy can suffer sudden death from strenuous exercise. The potential for these types of harm warrant notifying at-risk relatives.

Yet sharing one's genetic information with family members can be perilous. Testing may reveal, for instance, that the man everyone thought was a child's father actually is not, sending a family into turmoil. Genetic counselors can help people decide whether to undergo genetic testing and how to respond to possible results, but currently only 2,500 counselors practice in the U.S. The most common mistake is getting tested and waiting for results before considering what to do. Anyone contemplating testing should determine in advance whether to share the results with close relatives. There is no simple answer. The best advice is to consult with professionals and think ahead about the possible consequences. ***—M.A.R.***

ers to release their health information. According to one estimate, at least 25 million such authorizations occur every year in the U.S.

The parties requiring the disclosures are usually acting lawfully. And one's health can have legitimate bearing on decisions. An electric power company, for example, would not want to hire someone who is prone to seizures to fix wires at the tops of utility poles. The problem is the amount of information disclosed. The electric company has no need to know whether a job applicant has a genetic mutation that may increase susceptibility to heart disease decades from now. Judging a worker's compensation claim for a broken leg does not require reproductive health information. An automobile insurance adjuster handling a claim for a chipped tooth sustained in an accident does not need any genetic test result. But most of the laws authorizing disclosure of health information are written so broadly that no limits are placed on the scope of the requests.

Ironically, EHR networks could solve this problem. Software programs could scan electronic records and select only the data related to a specific inquiry. Yet this capability requires the use of "contextual access criteria"—software algorithms specifying that, for an inquiry of type X, only data A, B and C are needed. For example, contextual access criteria would disclose only information bearing on mortality risk to a life insurer. This technology is feasible but not yet available. And because commercial demand alone probably will not provide adequate incentives to develop the technology, laws may be needed to require it.

Legislation of Little Help

Given the general weakness of federal regulations, various state legislatures have enacted their own protection laws. In so doing, the states have adopted the notion of "genetic exceptionalism"—that genetic information is treated differently from other forms of sensitive health information. Whether this approach is desirable is an open question, but it parallels how some mental health, substance abuse and HIV information is handled.

Although the laws vary, 12 states require people to give written, informed consent for a genetic test, and 27 states require express consent to disclose test results. Nevertheless, these laws, like the federal regulations, continue to allow insurers and employers to legally require individuals to sign an authorization for the release of their medical information. As a result, 47 states have laws that prohibit insurers from denying or restricting coverage or charging different rates, based on an individual's genetic information. HIPAA already covers these cases for people in employer-sponsored group health plans, however, so the state laws in effect only extend protection to people who buy individual insurance.

Other laws in 35 states prohibit employers from requiring a genetic test as a condition of employment and from using predictive genetic information to deny an individual a job. Yet after a conditional offer of employment, the laws allow an employer to require prospective employees to authorize the release of their health records as a condition of being hired. The states differ on whether genetic information may be disclosed at this time, but that provision is largely immaterial: it is impracticable for anyone to excise genetic information from paper records and equally infeasible to exclude it from electronic records until the contextual access algorithms are devised.

Given such shortcomings, Congress has been under increasing pressure to improve privacy. In May members finally passed the Genetic Information Nondiscrimination Act (GINA), which had been pending since the mid-1990s. The act prohibits health insurance companies from discriminating in providing coverage, and in setting rates, on the basis of genetic predispositions. Unfortunately, the legislation is not much better than or even different from many state laws, and it doesn't cover life, disability or long-term care insurance.

Universal Solutions

The flaws in GINA, HIPAA and state regulations are not loopholes or oversights. They are the natural result of a health care system in which individual coverage is medically underwritten [see "Reflections on Privacy 2.0," by Esther Dyson, on page 50]. People in the U.S. can obtain insurance in one of three ways: a group health plan such as that offered by most employers, individual insurance, or federal programs such as Medicare and Medicaid. For group and individual plans, underwriters calculate the individual or collective health risks of those covered and impose premiums based on the relative risk they represent. Of course, one prime purpose is to protect the financial interests of the insurer. Insurers want to know about each person's past ailments and the possibility of future illnesses (genetic and otherwise) so they can bet-

GENE DETAILS COMING SOON

The 1000 Genome Project, an international research consortium started this year, intends to create a map of the human genome that is five times more detailed than the one created by the International HapMap Project.

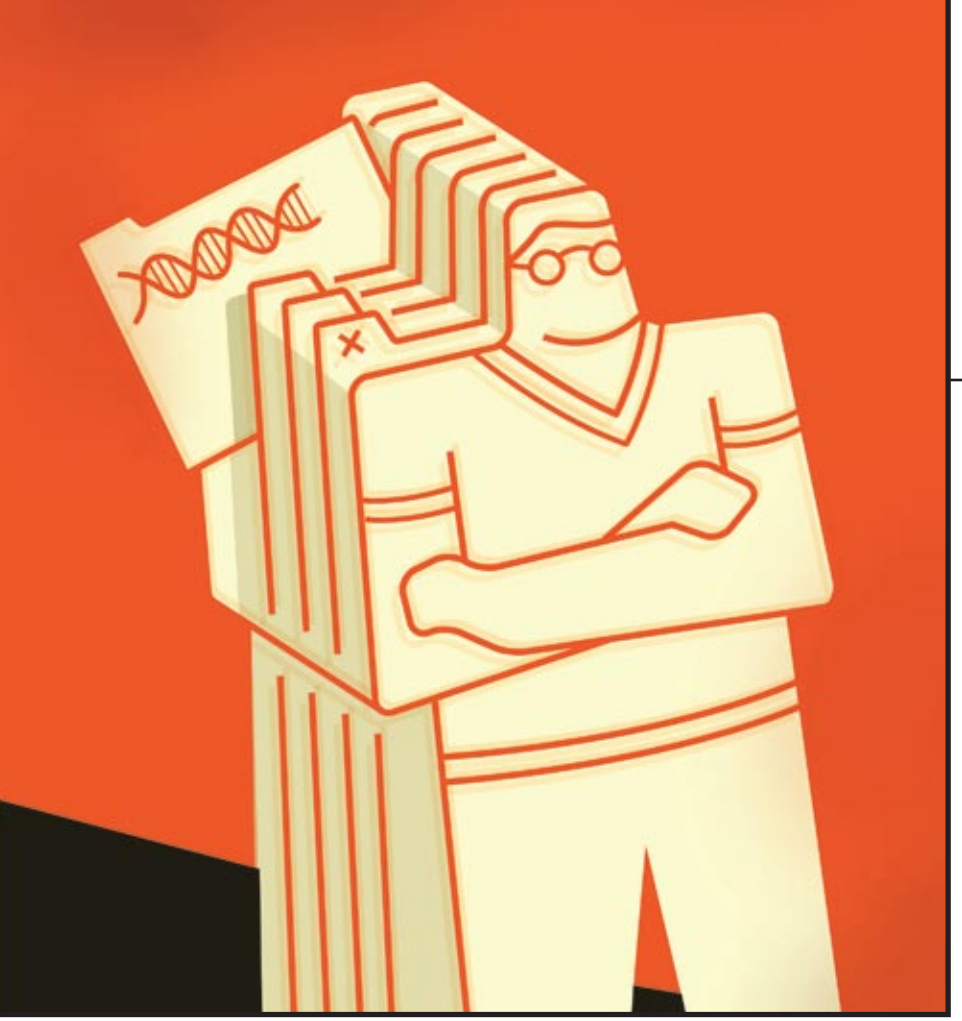
HapMap discoveries spawned the recent explosion of genome-wide studies that have identified more than 130 genetic variants linked to a range of diseases, including type 2 diabetes, coronary artery disease, prostate and breast cancers, rheumatoid arthritis and mental illnesses.

In the next three years the 1000 Genome Project hopes to sequence the genomes of at least 1,000 people drawn from populations around the world. For more see www.1000genomes.org

[THE AUTHOR]

Mark A. Rothstein is chair of law and medicine and director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. From 2001 to 2008 Rothstein chaired the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, which advises the U.S. secretary of health and human services.

LESLIE FRIESEN *University of Louisville*



HARRY CAMPBELL

ter determine price and ward off those who might make huge claims.

None of the privacy laws mentioned apply to Medicare or Medicaid, because technically these programs are entitlements, not insurance. Different laws attempt to protect information within these programs, but the government has no real incentive to look at anyone's genetic information because there are no rates to adjust.

Indeed, concerns about keeping information private are best addressed by a national system of universal health care, as in Canada. In universal plans, risk is spread across the entire population, and the plan is funded by the entire population. Whether any given person has a high risk for any disease has no bearing on the equation, so there is no incentive for others to seek protected information. The situation eliminates people's two greatest worries: that they will have trouble obtaining or will be dropped from health insurance, and that they will be denied a job because their medical conditions could impose a burden on the company's health plan.

Complications in obtaining life insurance must still be addressed, however. And health information still has to be made secure so records are not stolen or improperly disclosed. But the big incentives to discriminate largely disappear.

MORE TO EXPLORE

Genetic Privacy: A Challenge to Medico-Legal Norms. Graeme Laurie. Cambridge University Press, 2002.

Genetic Privacy. Pamela Sankar in *Annual Review of Medicine,* Vol. 54, pages 393–407; 2003.

Genetic Exceptionalism and Legislative Pragmatism. Mark A. Rothstein in *Hastings Center Report,* Vol. 35, No. 4, pages 27–33; July/August 2005.

Ensuring the Privacy and Confidentiality of Electronic Health Records. Nicolas P. Terry and Leslie P. Francis in *University of Illinois Law Review,* pages 681–735; 2007.

Canada and the Netherlands may give patients complete control of their health records.

The U.S., though, is unlikely to adopt universal health care anytime soon, even though it is front and center in the 2008 presidential campaign. Thus, better privacy laws must be enacted, even though some observers say new genetic technologies add little threat to privacy. Although very few legal cases have been brought over discrimination in employment or health insurance, almost all medical geneticists and genetic counselors know of numerous patients who have declined to undergo genetic testing because they feared possible discrimination or stigma. (According to Francis S. Collins, former director of the National Human Genome Research Institute, one third of eligible people decline to participate in genetic research because they fear discrimination.) Furthermore, the number of genetic tests and the number of people taking them, along with the tests' usefulness, will increase significantly in the next decade. And EHR networks will make it easy to disclose the information widely with the click of a mouse.

As the U.S. and other countries contemplate better ways to deal with genetic information, policymakers are seeing that protecting privacy is neither cheap nor easy. Improved security measures can keep information from being disclosed without authorization, but restricting the scope of authorized disclosures is equally important. It is essential, and challenging, to decide which individuals and entities have a right to which information and for what purposes.

Effective legislation should, at minimum, include four elements. First, it should address the underlying difficulties in gaining access to health insurance and carefully balance the rights of employers and employees. Second, legislation should limit nonmedical uses of predictive health information, including for life insurance, disability insurance and long-term care insurance. Third, any legislation should limit the scope of disclosures, penalize wrongdoers and provide remedies for people harmed by wrongful disclosures. And fourth, EHRs and EHR networks should be designed so that they can limit disclosures to relevant health information. Tackling these matters will provide an effective first step toward shaping the future of medical privacy. ■

TOOLS OF THE SPY TRADE

Night-vision cameras, biometric sensors and other gadgets already give snoops access to private spaces. Coming soon: palm-size "bug-bots"

Compiled by Steven Ashley

Visual Aids

1. **DIGITAL STILL AND VIDEO CAMERAS** fitted with large telephoto lenses make it possible for agents to discern the details of a faraway scene. An operative wielding a telephoto camera can read a newspaper headline (and, perhaps, subheads) from a football field's length away.
2. **NIGHT-VISION GOGGLES** or telescopes fitted with photomultiplier tubes can dramatically brighten available light; thermal sensors can reveal warm bodies and hot engines in total darkness.

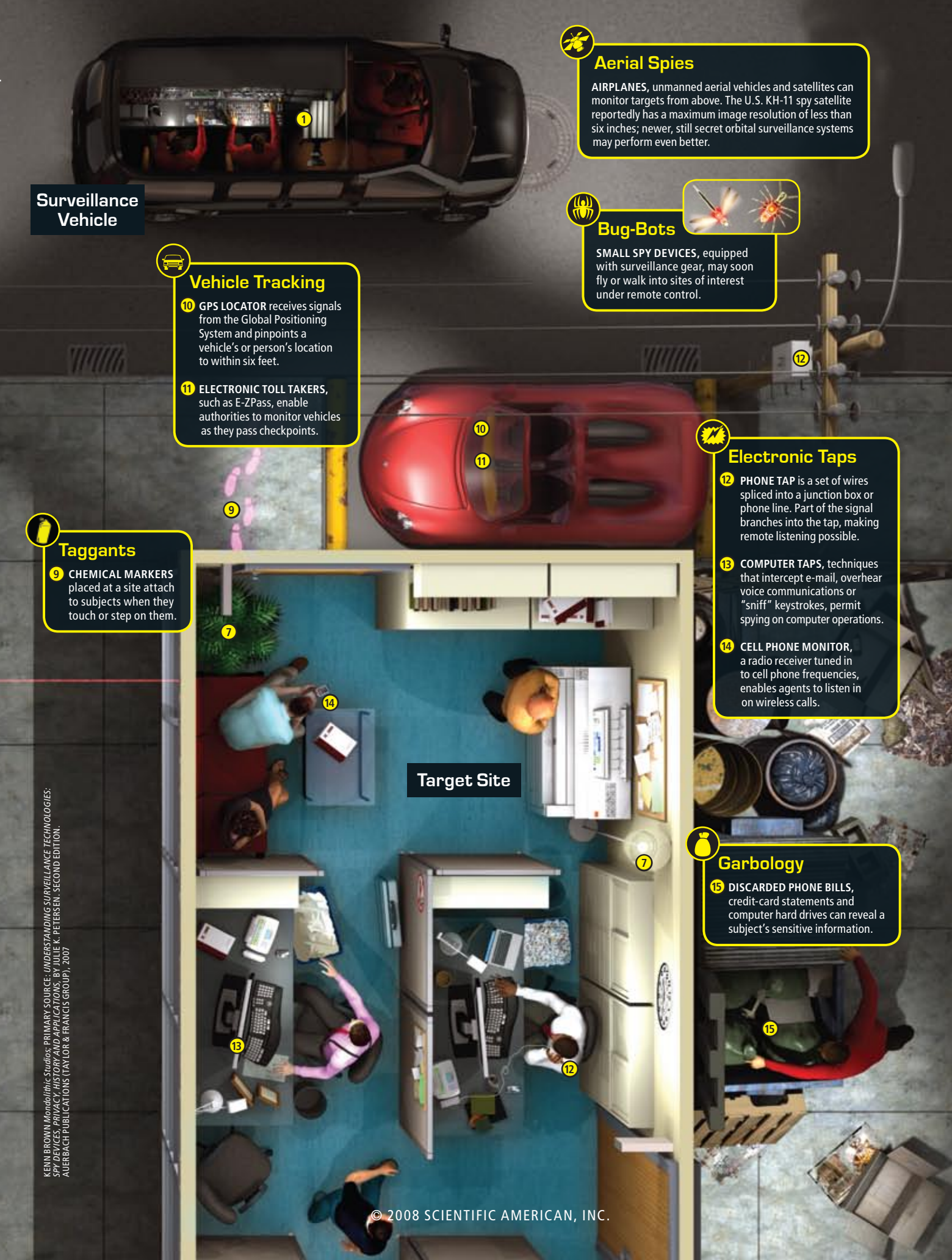
Biometric Identifiers

3. **VOICE**, facial features, walking gait and other characteristics can identify a person whose physical or behavioral traits are registered in an existing database.
4. **DNA SENSOR**, one of the latest biometric systems, samples DNA left, say, on a glass or doorknob and compares it with genetic information on file.
5. **ARTIFICIAL NOSE** detects a subject's body "odor print," which is matched against records.

Listening Devices

6. **DIRECTIONAL MIKE**, assisted by a parabolic dish or a "shotgun" (linear wand), can pick up open-air conversations from several hundred feet away.
7. **BUG**, a tiny, hidden microphone and short-range radio transmitter (*in potted plant on opposite page, for example*), sends conversations to a radio receiver, which relays the speech to a recorder or headphones (*seated agent, below*).
8. **LASER BEAM** bounced off a window can detect vibrations of the glass produced by the sounds of indoor conversations. An optical receiver converts patterns in the reflected beam into sounds a snoop can hear.

Surveillance Stakeout



KENN BROWN *Mondolithic Studios*; PRIMARY SOURCE: *UNDERSTANDING SURVEILLANCE TECHNOLOGIES: SPY DEVICES, PRIVACY, HISTORY AND APPLICATIONS*. BY JULIE K. PETERSEN. SECOND EDITION. AUERBACH PUBLICATIONS (TAYLOR & FRANCIS GROUP), 2007

RFID TAG— YOU'RE IT

Tiny radio-frequency identification tags, long used for tracking supplies and inventory, are now appearing in a growing range of consumer items. A privacy activist argues that the devices pose new security risks to those who carry them, often unwittingly

By Katherine Albrecht

KEY CONCEPTS

- Radio-frequency identification (RFID) tags are embedded in a growing number of personal items and identity documents.
- Because the tags were designed to be powerful tracking devices and they typically incorporate little security, people wearing or carrying them are vulnerable to surreptitious surveillance and profiling.
- Worldwide, legislators have done little to address those risks to citizens.

—The Editors

If you live in a state bordering Canada or Mexico, you may soon be given an opportunity to carry a very high tech item: a remotely readable driver's license. Designed to identify U.S. citizens as they approach the nation's borders, the cards are being promoted by the Department of Homeland Security as a way to save time and simplify border crossings. But if you care about your safety and privacy as much as convenience, you might want to think twice before signing up.

The new licenses come equipped with radio-frequency identification (RFID) tags that can be read right through a wallet, pocket or purse from as far away as 30 feet. Each tag incorporates a tiny microchip encoded with a unique identification number. As the bearer approaches a border station, radio energy broadcast by a reader device is picked up by an antenna connected to the chip, causing it to emit the ID number. By the time the license holder reaches the border agent, the number has already been fed into a Homeland Security database, and the traveler's photograph and other details are displayed on the agent's screen.

Although such "enhanced" driver's licenses remain voluntary in the states that offer them, privacy and security experts are concerned that those who sign up for the cards are unaware of the risk: *anyone* with a readily available reader device—unscrupulous marketers, government agents, stalkers, thieves and just plain snoops—can also access the data on the licenses to remotely track people without their knowledge or consent. What is more, once the tag's ID number is associated with an individual's identity—for example, when the person carrying the license makes a credit-card transaction—the radio tag becomes a proxy for that individual. And the driver's licenses are just the latest addition to a growing array of "tagged" items that consumers might be wearing or carrying around, such as transit and toll passes, office key cards, school IDs, "contactless" credit cards, clothing, phones and even groceries.

RFID tags have been likened to barcodes that broadcast their information, and the comparison is apt in the sense that the tiny devices have been used mainly for identifying parts and inventory, including cattle, as they make their way through supply chains. Instead of having to scan every individual item's Universal Product Code (UPC), a warehouse worker can register the contents of an entire pallet of, say, paper towels by scanning the unique serial number encoded in the attached RFID tag. That number is associated in a central database with a detailed list of the pallet's con-

MELISSA THOMAS (*photoillustration*); RICHARD SCHULTZ (*RFID tags*); SAM JORDASH (*woman*); BURAZIN (*key fob*); © 2005 TRANSPORT FOR LONDON (*Oyster card*); IDENTITY STRONGHOLD (*passport sleeve*); DIMA GAVRYSH AP Photo (*Chase blink credit card*); ROLF VENNENBERND *DPA/Corbis (EASyRFID)*; WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY (*SmarTrip card*)

tents. But people are not paper products. During the past decade a shift toward embedding chips in individual consumer goods and, now, official identity documents has created a new set of privacy and security problems precisely because RFID is such a powerful tracking technology. Very little security is built into the tags themselves, and existing laws offer people scant protection from being surreptitiously tracked and profiled while living an increasingly tagged life.

Beyond Barcodes

The first radio tags identified military aircraft as friend or foe during World War II, but it was not until the late 1980s that similar tags became the basis of electronic toll-collection systems, such as E-ZPass along the East Coast. And in 1999 corporations began considering the tags' potential for tracking millions of individual objects. In that year Procter & Gamble and Gillette (which have since merged to become the world's largest consumer-product manufacturing company) formed a consortium with Massachusetts Institute of Technology engineers, called the Auto-ID Center, to develop RFID tags that would be small, efficient and cheap enough to eventually replace the UPC barcode on everyday consumer products.

By 2003 the group had developed a working version of the technology and attracted investment from more than 100 companies and government agencies. The tags' promoters promised the tiny chips would revolutionize inventory management and counterfeiting prevention [see "RFID: A Key to Automating Everything,"

AVERAGE CONSUMERS may not realize how many RFID tags they carry around. The devices are embedded in personal items and even some clothing.

by Roy Want; Scientific American, January 2004].

To kick-start government adoption of the technology, the General Services Administration (GSA), a federal bureau that manages purchasing for other government institutions, issued a memo in 2004 urging the heads of all federal agencies "to consider action that can be taken to advance the [RFID] industry." Suddenly, virtually every agency, from the Social Security Administration to the Food and Drug Administration, began announcing RFID trials.

During the same period, similar initiatives were under way around the world. In 2003 the International Civil Aviation Organization (ICAO), a United Nations agency that sets global passport standards, endorsed the use of RFID tags in passports. ICAO now calls for their use in all scannable "e-passports." Today dozens of countries, including the U.S., issue e-passports with RFID tags embedded in their covers.

Since their debut, the new passports have been controversial on both privacy and security grounds. In a 2006 report one ICAO official promised that encryption measures would provide a "level of protection [that] should reassure the most anxious passport holder that his personal data cannot be read without his knowledge."

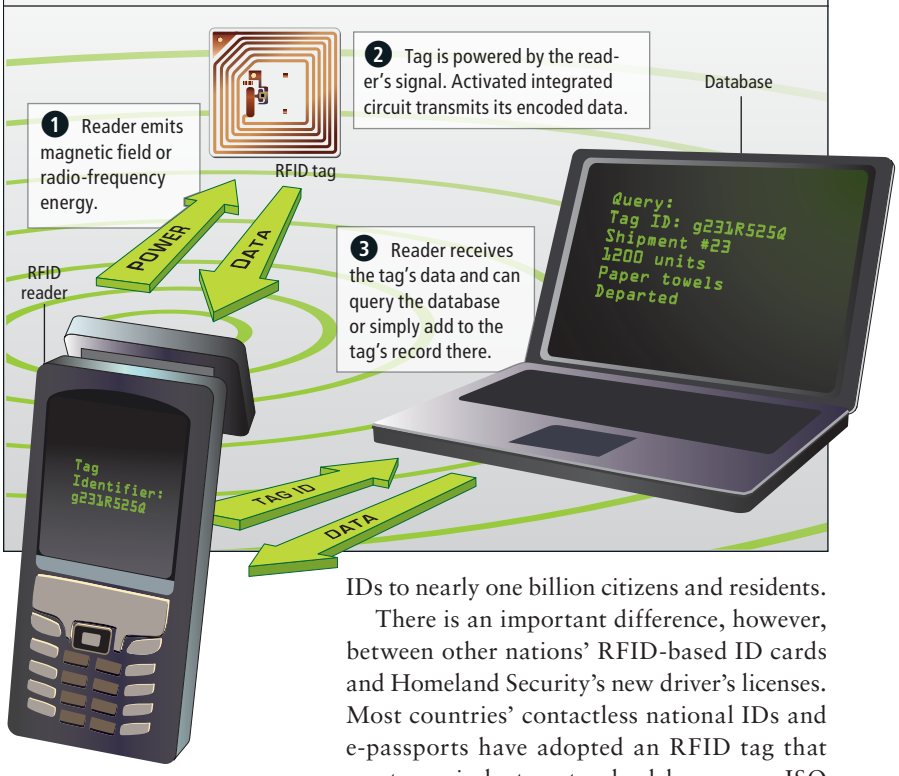
Security experts quickly proved otherwise. In 2007 British security consultant Adam Laurie cracked the encryption code on a U.K. passport and "skimmed," or remotely read, its personal information—while it was still sealed in its mailing envelope. Around the same time, German security consultant Lukas Grunwald copied the data from a German passport's embedded chip and encoded it into a different RFID tag to create a forged document that could fool an electronic passport reader. Investigators at Charles University in Prague, finding similar vulnerabilities in Czech e-passports, wrote that it was "a bit surprising to meet an implementation that actually encourages rather than eliminates [security] attacks."

Yet these demonstrated security problems have not slowed the adoption of RFID. On the contrary, the technology is being deployed for domestic ID cards around the world. Malaysia has issued some 25 million contactless national identity cards. Qatar is issuing one that stores the cardholder's fingerprint in addition to personal information. And in what industry observers are calling the single largest RFID project in the world, the Chinese government is spending $6 billion to roll out RFID-based national IDs to nearly one billion citizens and residents.

[BASIC TECHNOLOGY]

How RFID Works

Typically an RFID system relies on the interaction of a reader device with both an RFID tag and a database containing information associated with that tag. At a minimum, tags consist of an integrated circuit encoded with a unique ID number and a metal coil or antenna able to conduct energy received from the reader.



WHAT'S IN STORE

Retailers are exploring uses of RFID beyond inventory tracking. This "magic mirror" can read RFID tags attached to, or embedded in, clothing and then display product information, additional colors or complementary items.

There is an important difference, however, between other nations' RFID-based ID cards and Homeland Security's new driver's licenses. Most countries' contactless national IDs and e-passports have adopted an RFID tag that meets an industry standard known as ISO 14443, which was developed specifically for identification and payment cards and has a degree of security and privacy protection built in. In contrast, U.S. border cards use an RFID standard known as EPCglobal Gen 2, a technology that was designed to track products in warehouses, where the goal is not security but maximum ease of readability.

Whereas the ISO 14443 standard includes rudimentary encryption and requires tags to be close to a scanner to be read (a distance measured in inches rather than feet), Gen 2 tags typically have no encryption and only minimal data safeguards. To skim the data from an encrypted ISO 14443 chip, you have to crack the encryption code, but no special skills are required to skim a Gen 2 tag; all you need is any Gen 2 reader. Such readers can be purchased readily and are in common use in warehouses worldwide. A hacker or criminal armed with one could skim a border card through a purse, across a room, even through a wall.

As of this past April, more than 35,000 Wash-

LILA RUBENSTEIN AND TOMMY MOORMAN (*illustration*); COURTESY OF AVERY DENNISON AND THEBIGSPACE (*magic mirror*)

ington State motorists had signed up for enhanced driver's licenses, and other border states, including Arizona, Michigan and Vermont, have agreed to participate in the program. New York State will begin making the new licenses available to its residents after Labor Day.

But the possibility that the security of such cards could be compromised is just one reason for concern. Even if tighter data-protection measures could someday prevent unauthorized access to RFID-card data, many privacy advocates worry that remotely readable identity documents could be abused by governments that wish to tightly monitor and control their citizens.

China's national ID cards, for instance, are encoded with what most people would consider a shocking amount of personal information, including health and reproductive history, employment status, religion, ethnicity and even the name and phone number of each cardholder's landlord. More ominous still, the cards are part of a larger project to blanket Chinese cities with state-of-the-art surveillance technologies. Michael Lin, a vice president for China Public Security Technology, a private company providing the RFID cards for the program, unflinchingly described them to the *New York Times* as "a way for the government to control the population in the future." And even if other governments do not take advantage of the surveillance potential inherent in the new ID cards, ample evidence suggests that data-hungry corporations will.

Living a Tagged Life

If the idea that corporations might want to use RFID tags to spy on individuals sounds farfetched, it is worth considering an IBM patent filed in 2001 and granted in 2006. The patent describes exactly how the cards can be used for tracking and profiling even if access to official databases is unavailable or strictly limited. Entitled "Identification and Tracking of Persons Using RFID-Tagged Items in Store Environments," it chillingly details RFID's potential for surveillance in a world where networked RFID readers called "person tracking units" would be incorporated virtually everywhere people go—in "shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, [and] museums"—to closely monitor people's movements.

According to the patent, here is how it would work in a retail environment: an "RFID tag scanner located [in the desired tracking location] … scans the RFID tags on [a] person.… As that person moves around the store, different RFID tag scanners located throughout the store can pick up radio signals from the RFID tags carried on that person and the movement of that person is tracked based on these detections.… The person tracking unit may keep records of different locations where the person has visited, as well as the visitation times."

The fact that no personal data are stored in the RFID tag does not present a problem, IBM explains, because "the personal information will be obtained when the person uses his or her credit card, bank card, shopper card or the like." The link between the unique RFID number of the tag and a person's identity needs to be made only once for the card to serve as a proxy for the person thereafter. Although IBM envisioned tracking people via miniature tags in consumer goods, with today's RFID border cards there is no need to wait for such individual product tags to become widespread. Washington's new driver's licenses would be ideally suited to the in-store tracking application, because they can already be read by Gen 2 inventory scanners in use

VOLUNTARY GUIDELINES

EPCglobal, Inc., an organization that sets standards for RFID tags, also offers principles for their use as "electronic product codes" in consumer goods.

Notice: "Consumers will be given clear notice of the presence of EPC on products or their packaging … through the use of an EPC logo or [other] identifier."

Choice: "Consumers will be informed of the choices … to [remove or disable] EPC tags from the products they acquire."

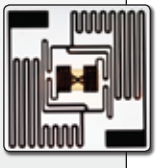
Education: Companies using EPC tags will "familiarize consumers with the EPC logo and help [them] understand the technology."

Records: Consumer data associated with tags "will be collected, used, maintained, stored and protected by EPCglobal member companies in compliance with applicable laws."

[CAPABILITIES]

Types of Tags

Technical standards set by EPCglobal enable RFID tags to be grouped according to minimum capabilities. Each class adds to features of the basic class 1 tag, which is "passive": it depends on a reader to initiate communication and supply power. Passive tags can be read from as far away as 30 feet, active tags from 300 feet or more.



	Minimum function	Some uses
CLASS I (Passive)	• Unique identifier number • "Kill function" to disable tag • Memory programmable only once • Newer "Gen 2" versions may be rewritable and password-protected	• Parts and inventory • Enhanced U.S. driver's license • Key card
CLASS II (Passive)	• Extended ID number • Additional memory, rewritable • Password access	• E-passport • Credit card • National IDs
CLASS III (Semi-passive)	• One or more sensors and a power source	• Container and storage sensors
CLASS IV (Active)	• Transmitter and power source • Can initiate communication with a reader or another tag	• Car key fob • Animal tag • Toll pass

EPCGLOBAL, INC. (*logo*); VERICHIP CORPORATION (*chip with penny*); ALIEN TECHNOLOGY CORPORATION (*squiggle RFID tag*)

today at stores such as Wal-Mart, Dillard's and American Apparel.

A tracking infrastructure will become increasingly fruitful to marketers as more people begin carrying, and even wearing, RFID-tagged items. At present, tens of millions of contactless credit and ATM cards containing RFID tags are in circulation, along with millions of employee access badges. RFID-based public-transit passes, widely used in Europe and Japan, are also coming to U.S. cities. IBM's person tracking unit is still only a patent, but an English amusement park called Alton Towers provides a living illustration of RFID's tracking potential. On entering the park, each visitor is offered an RFID wristband encoded with a unique ID number. As people enjoy the attractions, a network of RFID readers placed strategically throughout the park detects each wristband as it comes within range and triggers nearby video cameras. Candid footage of each individual is stored in a file labeled with the wristband ID number, then made available to the customer on a keepsake DVD at the end of the day.

Protecting the Public

If RFID tags can enable an amusement park to capture detailed, personalized videos of thousands of people a day, imagine what a determined government could do—not to mention marketers or criminals. That is why my colleagues in the privacy community and I have so firmly opposed the use of RFID in government-issued identity documents or individual consumer items. As far back as 2003, my organization, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)—along with the Privacy Rights Clearinghouse, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the American Civil Liberties Union, and 40 other leading privacy and civil liberties advocates and organizations—recognized this threat and issued a position paper that condemned the tracking of human beings with RFID as inappropriate.

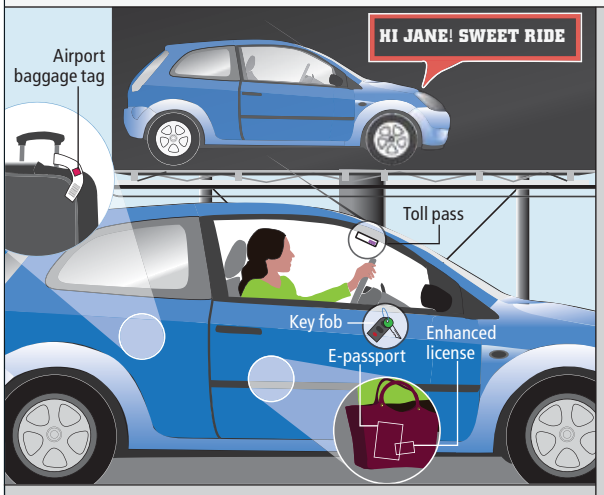
In response to these concerns, dozens of U.S. states have introduced RFID consumer-protection bills—which have all been either killed or gutted by heavy opposition from lobbyists for the RFID industry. When the New Hampshire Senate voted on a bill that would have imposed tough regulations on RFID in 2006, a last-minute floor amendment replaced it with a two-year study instead. (I was appointed by the governor to serve on the resulting commission.) That same year a California bill that would have prohibited the use of RFID in government-issued documents passed both houses of the legislature, only to be vetoed by Governor Arnold Schwarzenegger.

On the federal level, no high-profile consumer-protection bills related to RFID have been passed. Instead, in 2005, the Senate Republican High Tech Task Force praised RFID applications as "exciting new technologies" with "tremendous promise for our economy" and vowed to protect RFID from regulation or legislation.

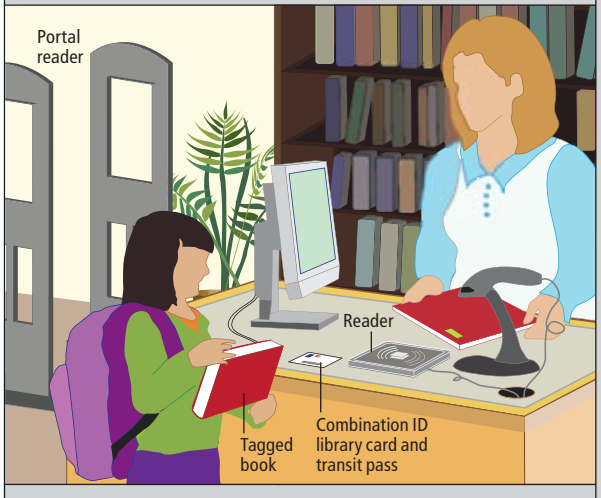
[APPLICATIONS]

Everyday RFID

RFID tags are embedded in a growing number of items people use regularly. They provide conveniences to con-



Travel may involve multiple RFID tags, including toll passes and key fobs readable from significant distances, e-passports, "enhanced" driver's licenses and some airport baggage tags.



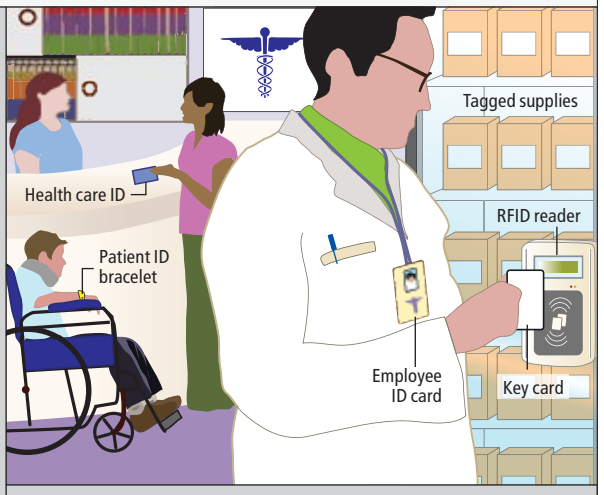
Schools and public libraries incorporate tags in student IDs, library cards and books. In the District of Columbia a new RFID-tagged "One Card" will serve as a public school student ID, library card and public-transit pass.

KARL SIMONS; MAKEUP: SCOTT BARNES (*Albrecht*)

[THE AUTHOR]

Katherine Albrecht holds a doctorate in education from Harvard University and is director of CASPIAN, a 15,000-member consumer privacy organization opposing retail surveillance. Since 2003 she has worked to expose and prevent unethical uses of RFID in products and in people. She regularly testifies before legislators and delivered a keynote address at a workshop on RFID and privacy held at the Massachusetts Institute of Technology. She has also co-authored two books describing how corporate and governmental uses of RFID could threaten individual privacy and security.

sumers or help businesses manage inventory or security. Increasingly, they also offer opportunities for marketing.



Workplaces routinely distribute tagged key cards and employee IDs. In hospitals the tags help to control and monitor access to medical supplies and to keep track of patients.

Retail goods are tagged for inventory monitoring, and some stores provide shoppers with tag readers that can display information or discounts. Stores should offer to deactivate tags on purchased items, but many do not.

LILA RUBENSTEIN

In the European Union, regulators are at least examining the situation. The European Commission—the executive arm of the E.U.—has acknowledged the potential for serious privacy problems with RFID and opened a public comment period earlier this year. As of July, when this issue went to press, recommendations stemming from the public comments were set to be released later in the summer, but expectations for any consumer-privacy regulations were low. In a March 2007 speech, E.U. commissioner for information society and media Viviane Reding announced that the commission would not regulate RFID but instead would allow businesses to regulate themselves. "I am here to tell you that on RFIDs, there is not going to be a regulation," she said. "My view is that we should underregulate rather than overregulate so that this sector can take off."

Unfortunately, industry self-regulation has little force when it comes to protecting the public from RFID risks. EPCglobal, the industry body that now sets technical standards for RFID tags, also produced a set of guidelines for the use of the chips in retail. The organization's recommendations require, among other things, notice to consumers whenever products contain RFID tags—for instance, in the form of a recognizable RFID logo. Yet when Checkpoint Systems, a member company of EPCglobal, designed RFID tags to be hidden in the soles of shoes—in clear violation of the organization's own provisions—Mike Meranda, then president of EPCglobal, told me that since the guidelines were voluntary, there was nothing he or his organization could do about it.

The Washington State Department of Licensing reassures citizens that their personal information is safe because the RFID tag in an enhanced driver's license "doesn't have a power source" and "doesn't contain any personal identifying information"—even though those facts have no bearing on whether the card can be used for tracking. For some people, a false sense of assurance provided by such official mollifications could be dangerous. The National Network to End Domestic Violence, a group that vocally opposes the use of RFID in identity documents and consumer products, has submitted legislative testimony describing how abusers could use the technology to stalk and monitor their victims.

Meanwhile the RFID train is barreling forward. Gigi Zenk, a spokesperson at Washington's licensing agency, recently confirmed that there are 10,000 enhanced licenses "on the street now—that people are actually carrying." That's a lot of potential for abuse, and it will only grow. The state recently mustered a halfhearted response, passing a law that designates the unauthorized reading of a tag "for the purpose of fraud, identity theft, or for any other illegal purpose" as a class C felony, subject to five years in prison and a $10,000 fine. Nowhere in the law does it say, however, that scanning for other purposes such as marketing—or perhaps "to control the population"—is prohibited. We ignore these risks at our peril. ■

MORE TO EXPLORE

Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID. Katherine Albrecht and Liz McIntyre. Thomas Nelson, 2005.

Radio-frequency Identification (RFID): Addressing Concerns over Information Collection and Usage. Video of a roundtable discussion at the University of Washington School of Law, July 19, 2007. Available at **www.law.washington.edu/lct/Events/rfid**

Privacy Impact Assessment for the Use of Radio Frequency Identification (RFID) Technology for Border Crossings. U.S. Department of Homeland Security, January 22, 2008.

European Commission RFID policy and information: **http://ec.europa.eu/information_society/policy/rfid/index_en.htm**

The RFID Ecosystem Project at the University of Washington: **http://rfid.cs.washington.edu**

BEYOND FINGERPRINTING

Security systems based on anatomical and behavioral characteristics may offer the best defense against identity theft

By Anil K. Jain and Sharath Pankanti

KEY CONCEPTS

- Biometric identification systems are harder to circumvent and easier to use than are traditional systems based on ID cards and passwords.
- Now that economical and powerful microprocessors are available, the technology is spreading.
- Before these biometric systems can reach their full potential, though, developers will have to lower their error rates.

—The Editors

If you are like many people, navigating the complexities of everyday life depends on an array of cards and passwords that confirm your identity. But lose a card, and your ATM will refuse to give you money. Forget a password, and your own computer may balk at your command. Allow your cards or passwords to fall into the wrong hands, and what were intended to be security measures can become the tools of fraud or identity theft. Biometrics—the automated recognition of people via distinctive anatomical and behavioral traits—has the potential to overcome many of these problems.

Compared with a physical token such as a bank card or with the knowledge of a secret such as a PIN, biometric traits are profoundly more difficult to forge, copy, share, misplace or guess. Indeed, they offer the only way of determining whether a person has been issued multiple official documents, such as a driver's license or passport, under different names. Yet they are quite easy to use as proof of identity. For these reasons, biometric systems have been gaining popularity in recent years. Laptops and mobile phones that can recognize a fingerprint, for instance, are now commercially available. In some countries biometric security is employed to safeguard items such as ATM cards and passports, to determine whether a person can rightfully enter a building or to ensure that someone is entitled to welfare payments. These systems are far from perfect. But with inexpensive sensors and powerful microprocessors now available, biometric technology is certain to become more pervasive.

Measures of Man

Biometrics is not a new idea. In 1879 Alphonse Bertillon, a French police inspector, proposed a complicated system of body measurements—arm and foot length among them—to identify repeat offenders. Over the next decade British scholars established that each print of a finger exhibits a unique pattern that persists over time, setting the stage for the development of the fingerprint classification system in 1896. Shortly thereafter, Scotland Yard began collecting fingerprints left at crime scenes to pinpoint criminals. And today almost every law-enforcement organization in the world relies on fingerprints to identify wrongdoers, solve crimes and conduct background checks on people applying for sensitive jobs.

But fingerprints are not the metric of choice for every purpose; several other physical and behavioral features have also been incorporated, singly or in tandem, into ID systems. The current emphasis in biometrics is to design fully automatic systems that are extremely fast, accurate, user-friendly and cost-effective and that can be

OPEN SESAME: To enhance accuracy, security systems of the future are likely to assess multiple biometric traits.

BIOMETRICS IN ACTION

- Member states of the European Union must begin issuing passports incorporating biometric data by the summer of 2009.
- Some high school cafeterias in the U.K. have instituted a cashless payment system that employs fingerprint recognition.
- A team led by Lockheed Martin recently won a 10-year FBI contract potentially worth $1 billion to develop an identification system incorporating biometric technologies such as face, iris and palm recognition.
- New York City's Office of Payroll Administration has a $181.1-million contract with San Diego–based Science Applications International to install a biometric punch clock that scans palms and fingers.
- The Toshiba Portégé M800 laptop comes with face-recognition software and an optional fingerprint reader.

embedded in existing security infrastructures. In addition to fingerprinting, workers in the past 30 years have developed ID systems based on such characteristics as the face, hand, voice and iris (the colored part of the eye).

Biometric systems require traits with two basic features: they must be unique for each person, and they must not change significantly with time. Some traits promote relatively high accuracy, others greater practicality or relatively low cost. The choice of trait to favor as an identifier therefore depends on the goals of the ID system. No single measurement is optimal for all applications.

Consider the three most popular traits in use today: the fingerprint, the face and the iris. In addition to its use in forensics, fingerprint recognition forms the basis of automated border-control systems in a number of countries. In the U.S. alone, the Department of Homeland Security's US-VISIT program has processed more than 75 million visitors since its debut in 2004. From a commercial standpoint, one of the biggest advantages of using fingerprints is that the sensors for capturing prints are now extremely cheap (around $5) and small enough to be embedded in consumer products such as laptops, mobile phones and even flash-memory sticks. But these compact sensors have higher error rates than their larger, more expensive counter-

KEVIN HAND (*illustration*); TOSHIBA, SINGAPORE (*laptop*)

[COMPARING TRAITS]

How The Metrics Measure Up

The choice of a biometric trait or traits to use in a security system depends on the application; the strengths and weaknesses of each of the four most common biometric identifiers are summarized in the table below. For example, compared with fingerprint recognition, iris recognition allows access to the wrong people less often but currently requires larger and costlier sensors and thus cannot be as easily incorporated into a laptop or other consumer device. Experts concur that in an ideal biometric authentication system, neither the "false accept" rate nor the "false reject" rate should exceed 0.1 percent. In tests conducted by the National Institute of Standards and Technology, however, none of the systems satisfied these error rate requirements.

Property	Biometric Traits: Fingerprint	Face	Iris	Voice
Distinctiveness	High	Low	High	Low
Permanence	High	Medium	High	Low
How well trait can be sensed	Medium	High	Medium	Medium
Speed and cost efficiency of system	High	Low	High	Low
Willingness of people to have trait used	Medium	High	Low	High
Difficulty of spoofing the trait	High	Low	High	Low
False reject rate*	0.4 percent	1.0–2.5 percent	1.1–1.4 percent	5–10 percent
False accept rate*	0.1 percent	0.1 percent	0.1 percent	2–5 percent

*Error rates depend on testing environment, sensors used and composition of users in the population.

parts common in law enforcement, because they scan a smaller portion of the finger and the image they record is lower in resolution.

Face recognition is gaining popularity as a security feature for computers and mobile phones, partly because it can take advantage of the built-in cameras that are becoming ubiquitous components of these devices. ID systems based on face recognition are quite accurate when the images are captured under controlled conditions—with the subject facing forward in indoor lighting and bearing a neutral expression, for example. They falter, however, when the original image and the newer one differ because of changes in pose, lighting, expression, age, and facial accessories such as glasses or a beard. This sensitivity to routine variations is particularly problematic for video surveillance, in which subjects do not present themselves in front of the camera in predetermined poses. Perhaps within 10 years the technology will have advanced sufficiently to permit fully automated, real-time face matching in video surveillance.

As for the iris—whose complex, textured pattern is thought to be unique to each person as well as permanent—recognition is extremely

LUCY READING-IKKANDA

accurate and swift. The subject simply looks into a scanner for a few seconds; the captured pattern is then analyzed and recorded. Matching is done by comparing a person's bit sequence to the sequences in a database. The speed and accuracy of this approach have driven the recent development of large-scale ID systems based on the iris, including the Iris Recognition Immigration System (IRIS) in the U.K. Travelers enrolled in the system's database can sidestep the usual immigration channels at the airport, thereby cutting down on travel wait time.

Iris recognition has its downsides, however. The method depends, for instance, on the use of algorithms that represent the random patterns in the iris as a sequence of bits—no known human experts can determine whether or not two iris images match. Hence, iris data are unsuitable for use as evidence in a court of law.

Imperfect Matches

Developers of biometric systems face other difficulties as well. Unlike ID systems requiring a password or a physical token, biometric systems generally have to make decisions on the basis of imperfect matches. Any system of comparison can lead to two basic types of error. In a "false accept" error, the system incorrectly declares a successful match between the input pattern and a pattern in the database that does not really match it. In a "false reject" error, the system incorrectly pronounces a failed match between the input pattern and a genuine match in the database.

Experts generally agree that neither the false accept rate nor the false reject rate of a biometric authentication system should exceed 0.1 percent (that is, one mistake in 1,000 assertions of a match and one mistake in 1,000 assertions of a nonmatch). But in evaluations conducted by the National Institute of Standards and Technology between 2003 and 2006, error rates for systems based on the fingerprint, face, iris and voice—another commonly used biometric trait—all exceeded the 0.1 percent level [*see box on opposite page*].

Increasing the threshold score for a match can lower the false accept rates, but at the expense of increasing the false rejects. Reducing both error rates simultaneously will require developing biometric sensors that generate higher-quality images and refining the feature extractors and matchers. Designers will also need to ensure that the systems are protected against sabotage: ideally, it should be impossible for biometric data to be intercepted and reentered into the systems. And it should be impossible to tamper with the biometric hardware or software. But these kinds of attacks are common to all authentication systems, including the password- and token-based varieties, and so they can be countered with established tools of the trade. For example, cryptography can hinder hackers from intercepting, replaying or altering information.

Much more challenging is designing a secure biometric system that accepts only the legitimate presentation of traits by their owners without being fooled by doctored or spoofed traits—a plastic copy of a person's finger, for instance. To that end, sensors that detect heat and other signs of life can help guarantee that the input to be compared does not originate from an inanimate object.

But perhaps the most effective strategy for improving the accuracy, reliability and security of biometrics is to detect multiple biometric traits or multiple instances of a trait (more than one fingerprint, for example). Reinforcing the identity of a subject through such combinations offers increasingly irrefutable proof that the biometric data are being presented by their legitimate owner and not an impostor. In fact, many passport systems are already evolving in this way. The US-VISIT program, which used to scan only two fingers of non-U.S. citizens, has started capturing all 10 fingers, and the system has the potential to assess both fingerprints and faces in the future.

The Privacy Conundrum

The use of biometrics raises important privacy concerns. Who owns the data—the individual or the service providers? Will those data be used for an unintended purpose—to deduce something about a person's health, for instance? Biometric systems of the future will probably operate unobtrusively, capturing biometric traits without the active involvement of the user. Such stealth further confounds the privacy issue.

At present we see no concrete, viable solutions on the horizon for addressing the entire spectrum of privacy concerns. We believe these problems can be resolved through public discussion and policy making, however. They will have to be. It is only a matter of time before continued improvements to biometric tools will move them center stage in efforts to combat the rampant problems of security and identity fraud that our society faces. ■

[THE AUTHORS]

Anil K. Jain (*left*) **is a professor in the departments of computer science and engineering, electrical and computer engineering, and probability and statistics at Michigan State University. He is the author of several books on biometrics.** **Sharath Pankanti** (*right*) **is manager of the computer vision group at IBM's Thomas J. Watson Research Center in Yorktown Heights, N.Y., where he is currently developing general-purpose object-recognition systems. Both Jain and Pankanti hold numerous patents related to fingerprinting.**

MORE TO EXPLORE

Biometric Recognition: Security and Privacy Concerns. Salil Prabhakar, Sharath Pankanti and Anil K. Jain in *IEEE Security & Privacy,* Vol. 1, No. 2, pages 33–42; March/April 2003.

Biometric Systems: Technology, Design and Performance Evaluation. Edited by James Wayman, Anil Jain, Davide Maltoni and Dario Maio. Springer, 2005.

Handbook of Multibiometrics. Arun A. Ross, Karthik Nandakumar and Anil K. Jain. Springer, 2006.

Probing the Uniqueness and Randomness of IrisCodes: Results from 200 Billion Iris Pair Comparisons. John Daugman in *Proceedings of the IEEE,* Vol. 94, No. 11, pages 1927–1935; November 2006.

Handbook of Biometrics. Edited by Anil K. Jain, Patrick Flynn and Arun A. Ross. Springer, 2008.

COURTESY OF ANIL K. JAIN (*left*); COURTESY OF SHARATH PANKANTI (*right*)

INFORMATION OF THE WORLD, UNITE!

Mashing everyone's personal data, from credit-card bills to cell phone logs, into one all-encompassing digital dossier is the stuff of Orwellian nightmares. But it is not as easy as most people assume

By Simson L. Garfinkel

KEY CONCEPTS

- The idea of linking together databases, known as data fusion, is the bête noire of privacy advocates. So far, however, it seems to be limited to specific contexts, such as gambling casinos and child-support enforcement.
- Data fusion is challenging because databases are riddled with errors and meaningless coincidences. New algorithms overcome some of these hurdles, but do they shift the overall ratio of cost and benefit?

—The Editors

A few years ago I bought a latte at Starbucks on the way to the airport, parked my car and got on a flight for the U.K. Eight hours later I got off at Heathrow, bought a prepay chip for my cell phone and went to buy a ticket for the train into London, when my credit card gave up the ghost and refused to work anymore. Not until I got back to the U.S. did I find out what had happened. Apparently, the small purchase at Starbucks, followed by the overseas purchase of the cell phone card, had tripped some kind of antifraud data-mining algorithm in my credit-card company's computer. It tried to call me, got my voice mail and proceeded to blacklist my credit card.

What I found so exasperating about the entire experience was that the computer should have known that the person using my card in England was *me*. After all, I had bought my plane ticket with that same card and had flown with a major U.S. carrier. Aren't all those databases supposed to be tied together?

Most people probably assume they are. We have come to expect from Hollywood films such as *Enemy of the State* and the Jason Bourne trilogy that shadowy organizations have instant access to all the databases we rely on and, with a few keystrokes, can spy on our every movement. The process of collecting information from multiple sources and merging it, known as data fusion, is supposed to create an information resource that is more powerful, more flexible and more accurate than any of the original sources. Proponents of data fusion say that their systems let organizations make better use of the data they already have; critics say that fusion threatens civil liberties by using information in ways that were never envisioned when it was first collected. Both sides assume that data-fusion systems actually work. The reality is that the systems are nowhere nearly as omniscient, as reliable or as well developed as many people think.

Out of Many, One

The technology of data fusion can trace its heritage back to the computerized matching programs of the 1970s. When Congress passed the Privacy Act in 1974, it also authorized the creation of the Federal Parent Locator Service, which now operates a giant blacklist, denying a wide range of federal benefits such as passports to noncustodial parents who are behind on their child support. Those data are fused with the National Directory of New Hires to find recently employed parents who are not up to date on their payments so that their wages can be garnished.

The term "data fusion" entered the technical vernacular in 1984, when researchers at Lock-

MULTITUDE OF DATA SOURCES can be merged into a single profile through the process of data fusion.

MELISSA THOMAS (*photoillustration*); PATRIK STOLLARZ *Getty Images* (*cell phone*); THINKSTOCK/CORBIS (*checkout card in book*); JIM CRAIGMYLE *Corbis* (*wand in laptop*); ELISE AMENDOLA *AP Photo* (*driver's license*); PURESTOCK (*passport*); DAVID MACK *Photo Researchers, Inc.* (*DNA*); PHILIP JAMES CORWIN *Corbis* (*bank statement*); SHEILA TERRY *Photo Researchers, Inc.* (*computer hard disk*)

heed Martin's Advanced Technology Center published two articles about a "tactical data fusion" system that would meld battlefield information from sensors, databases and other sources in real time for human analysts. Since then, the idea has blossomed. Bioinformatics investigators speak of genomic data fusion. The Department of Homeland Security has spent more than $250 million setting up some 58 state or local fusion centers. Nielsen, the consumer marketing company, has developed data-fusion products for identifying and targeting potential customers with specific characteristics, rather than wasting effort on the traditional scattershot approach to marketing.

But although data fusion has many faces, its use in identifying potential terrorists has stirred the greatest public debate. "The key to detecting terrorists is to look for patterns of activity indicative of terrorist plots based on observation of current plots and past terrorist attacks," wrote Rear Admiral John Poindexter and Robert L. Popp of the Defense Advanced Research Projects Agency (DARPA) in 2006. They argued that the World Trade Center bombing of 1993 and the Oklahoma City bombing of 1995 might have been prevented if the government could have scanned commercial databases for large purchases of fertilizer by nonfarmers. But getting those purchase records and combining them with a database of farm ownership and employment records would have required unprecedented government access to private computer systems. Every transaction—and thus every person—in the country would have been monitored without probable cause. For these reasons, among others, Congress killed Poindexter and Popp's research program, the Total Information Awareness project, in 2003.

Do Not Fold, Spindle or Mash

A wall of government secrecy does nothing to allay civil libertarians' fears. Agencies have revealed little about the data-fusion systems that they may or may not have deployed to protect national security: they argue that the bad guys would have an easier time evading fusion programs if they knew how they work. But enough information is publicly available to indicate that data fusion poses more than just ethical and legal problems; it also raises technical issues.

Data quality is one. Much of the information in databases was originally collected for purely statistical purposes and may not be accurate enough to make automated judgments with potentially punitive outcomes. In 1994 Roger Clarke of the Australian National University in Canberra studied computerized matching pro-

FUSION AND CONFUSION

To see how much information is out there, a *Scientific American* editor ordered an $80 report from an online consolidator of personal data, including criminal, real-estate and bankruptcy records. It was riddled with errors such as misspellings and confusion with namesakes elsewhere in the country—many of whom had liens on their property, though, thankfully, there were no criminal records. The report showed no signs of identity theft. Many people are not so fortunate.

[CASE STUDY]

Games People Play

Las Vegas casinos have been pioneers in fusing data from various sources because they face so many schemes to rip them off. Here are several examples based on true stories.

grams maintained by federal and state governments in the U.S. and Australia. These systems scanned millions of records and flagged thousands of potential "hits." But most turned out to be false positives. For example, one program for finding welfare cheats matched the employment records of the Department of Health and Human Services against the welfare rolls of the counties surrounding Washington, D.C. It generated roughly 1,000 hits, but further investigation showed that three quarters of the people identified were innocent. The benefits did not justify the costs of collecting data, training personnel and chasing down the false positives.

Many people feel that if a data-fusion program could anticipate and stop a major terrorist attack, it would be worth whatever it cost. Poindexter, a career naval officer, compared the technical problems to finding an enemy submarine in the vastness of the ocean. But finding the signatures of terrorist preparations in an ocean of data is much harder than finding subs in an ocean of water. The world's oceans may be huge, but every spot can be uniquely identified by a latitude, longitude and depth. The data oceans are not so easily categorized. Moreover, the world's seas are not doubling in size every few years, as the data oceans are. Much of information space is unmapped; data are spread across millions of individual computer systems, many hidden or otherwise unknown to the authorities.

Fusion is hard because we are drowning in data from a multitude of sources, all with different levels of detail and uncertainty. The real challenge in data fusion is not getting the data but making sense of them.

What's on Your Hard Drive?

A good way to understand the data-fusion problem is to start with the information on the hard drive of your computer. Between 1998 and 2005 I did just that: I purchased more than 1,000 used hard drives on eBay, at small computer stores and at swap meets; I even scavenged some from computers left abandoned on street corners. In January 2003 Abhi Shelat, now a computer sci-

HIDDEN DATA

Word-processing and other computer files typically contain "metadata" (such as the date of creation and your name and type of computer) and even deleted passages, such as those snide remarks you wrote in the first draft of a memo to your boss. A godsend to detectives and investigative journalists, such information becomes especially incriminating when merged with other data.

The only trouble is, sometimes the metadata are wrong. SCIENTIFIC AMERICAN ran earlier drafts of this article through two freeware metadata analyzers. They said the author had used OpenOffice on a Windows XP machine. But Garfinkel tells us he actually wrote them with Microsoft Office 2008 on a Mac. Oops. We did, however, enjoy seeing that one draft was revision number 139—reassuring us that he had indeed worked hard.

KENN BROWN *Mondolithic Studios*

entist at the University of Virginia, and I published a paper detailing what we found.

About a third of the drives were no longer functional, and another third had been properly wiped before being discarded. But the remaining third were a jackpot of personal information: e-mail messages, memoranda, financial records. One drive had previously been part of an automatic teller machine and recorded thousands of credit-card numbers. Another had been used by a supermarket to submit credit-card payments to its bank. Neither drive had been properly wiped before being resold on the open market.

The tools that enabled me to search the drives are widely available and not particularly sophisticated. Police departments around the world use the same kinds of tools to recover files from computers and cell phones. Sometimes users are unaware of the digital bread crumbs they leave. Consider the case of the so-called BTK killer, who committed eight murders in Wichita, Kan., in the 1970s and 1980s, then went underground. The killer resurfaced in March 2004, sending a letter to the *Wichita Eagle* detailing his earlier crimes and a floppy disk with a Microsoft Word document on it to a local television station. The file contained "metadata" that linked it to a computer at a local church. Police discovered that the person who had used it was president of the congregation council—and the killer.

Making a Hash of the Files

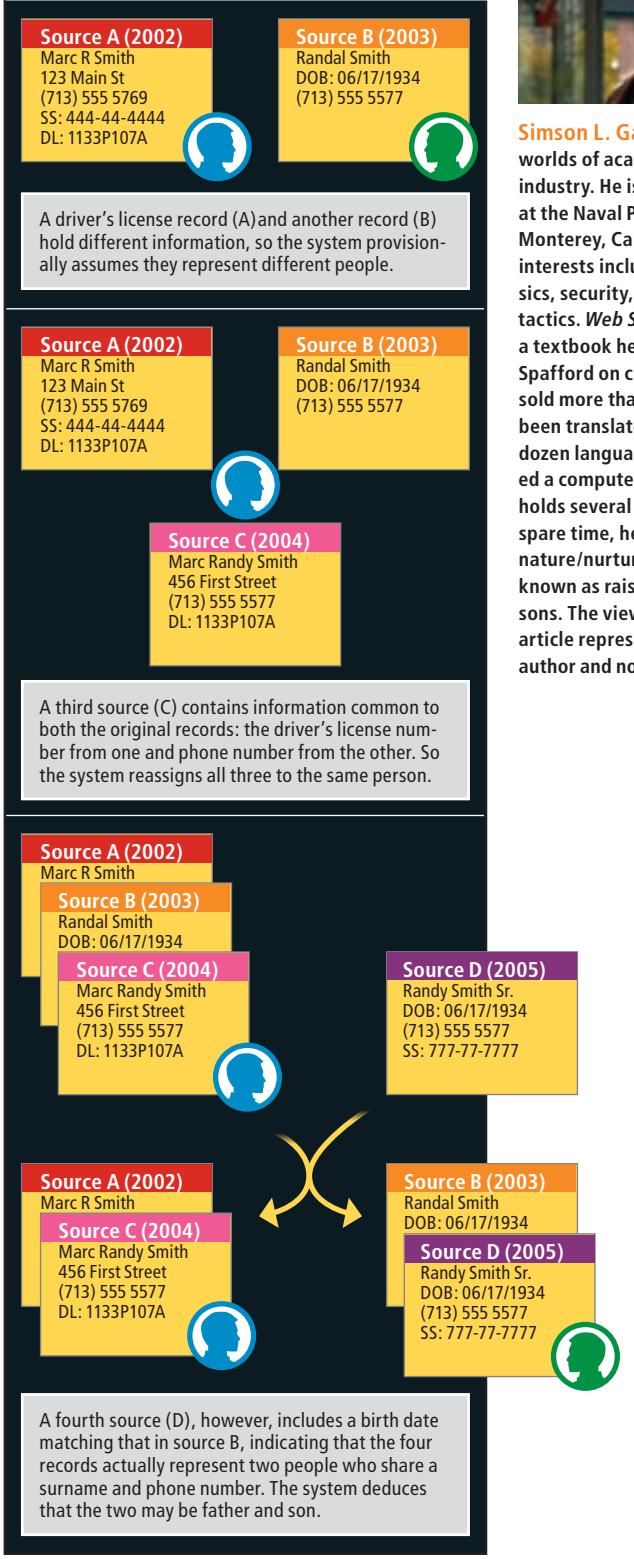
But figuring out which documents are important and which are worthless is difficult and requires fusing outside knowledge with the information on the hard drive. For example, when I started analyzing hard drives back in the 1990s, many of them contained copies of the *Island Hopper News*. It seemed highly suspicious. Then I learned that this electronic newspaper was actually a demo file distributed by Microsoft with a product called Visual Studio 6.0. Had I been unaware, I might have drawn spurious conclusions about the drive's previous owners.

The only way to screen out innocent files is to sample the world of digital documents and build a list of those that are widely available. One fast, automated way to do so is to create a so-called hash set. Cryptographic hash algorithms can assign a unique electronic fingerprint to any digital file. Two of the most popular are MD5, which creates a 128-bit fingerprint, and SHA-1, which generates a fingerprint 160 bits long. Then, instead of comparing two files byte by byte, forensics tools can examine the fingerprints.

[BEHIND THE SCENES OF FUSION]

How It Works

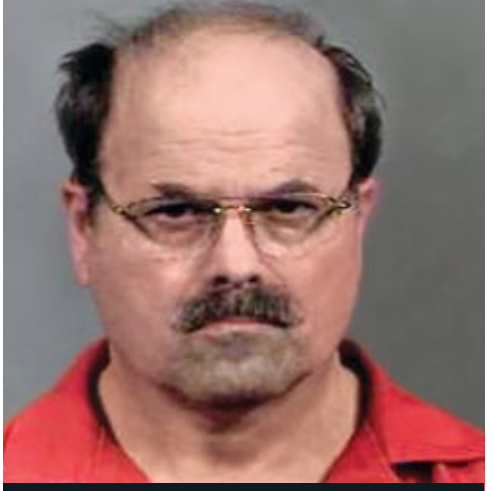
Originally developed for casinos, one data-fusion algorithm illustrates how to deal with partial, ambiguous information.



[THE AUTHOR]

Simson L. Garfinkel bridges the worlds of academia, journalism and industry. He is a computer scientist at the Naval Postgraduate School in Monterey, Calif., where his research interests include computer forensics, security, privacy and terrorist tactics. *Web Security & Commerce*, a textbook he wrote with Gene Spafford on computer security, has sold more than 250,000 copies and been translated into more than a dozen languages. Garfinkel founded a computer security firm and holds several related patents. In his spare time, he is conducting a nature/nurture experiment also known as raising identical twin sons. The views expressed in this article represent the opinion of the author and not the U.S. government.

COURTESY OF SIMSON L. GARFINKEL (*author*); MELISSA THOMAS (*illustration*)



DENNIS RADER, aka the BTK killer, gave himself away through metadata hidden in a Microsoft Word file he had sent to a TV station.

HURRICANE KATRINA evacuees, shown here at the Houston Astrodome, were reunited with relatives by a simple data-fusion system.

Supported by a grant from the Department of Justice, the National Software Reference Library at the National Institute of Standards and Technology (NIST) acquires software from hundreds of publishers and reduces every file to a cryptographic hash. NIST then distributes the database, which now has more than 46 million entries, to give forensic investigators a quick and reliable way of purging files that have been distributed by software publishers—files such as the *Island Hopper News*—and can therefore be safely ignored. Databases available from other federal agencies include e-fingerprints of computer hacker tools and of child pornography.

But despite their utility, hash databases represent only a small sampling of all the documents out there. To augment them, I developed a technique called cross-drive analysis. It can automatically piece together information scattered across thousands of hard drives, USB memory sticks and other data sources. The technique highlights and isolates identifiers such as e-mail addresses and credit-card numbers and weights them according to how frequently they appear: presumably the more common the identifier, the less important it is. Finally, the technique correlates the identifiers across all the individual devices: if an e-mail address or credit-card number appears on only two disk drives among thousands, there is a good chance that those two drives are related.

Who's Who?

Yet another problem for data fusers is identity. In the electronic world there may be dozens of people sharing the same name and dozens of names used by the same person. Some databanks may list Poindexter as John Marlan Poindexter or J. M. Poindexter or even misspell the rear admiral's last name Pointexter. A person's first name may be listed in one database as Robert, in another as Rob and in a third as Bob. A person whose Arabic name is transliterated Haj Imhemed Otmane Abderaqib in West Africa might be known as Hajj Mohamed Uthman Abd Al Ragib in Iraq.

Matching up the various names and account numbers that inhabit the electronic world with physical bodies is called identity resolution. Without it, data fusion is impossible. Curiously, a great deal of innovation in identity-resolution systems has been driven by casinos in Las Vegas. Under Nevada law, casinos are required to bar self-declared problem gamblers from playing their games. These gamblers voluntarily place their names on a list saying, in effect, "Don't let me gamble again!" But gambling can be an illness, and some people on the list still try to sneak in by changing their name or swapping a few numbers in their birth date. Casinos are also determined to exclude suspected or convicted cheaters. And if a guest is winning large sums at the blackjack table, a casino wants to make sure that the dealer and the player are not roommates.

Accordingly, casinos have funded development of a technique called nonobvious relationship analysis (NORA), which combines identity resolution with databases of credit companies, public records and hotel stays. A NORA system, for instance, might discover that the blackjack dealer's wife once lived in the same apartment building as the player who just won $100,000. In the 1990s software engineer Jeff Jonas developed a system that could match the names in a casino's computers with other sources of information in a way that tolerates error, ambiguity and uncertainty. The system works by building hypotheses based on the data and then revising these hypotheses as new information becomes available.

For example, it might receive a driver's license record for a Marc R. Smith, a credit report for a Randal Smith, and a credit application for a Marc Randy Smith. It might guess that the names belong to the same person—particularly if Marc R. Smith and Marc Randy Smith have the same driver's license number and if Randal Smith and Marc Randy Smith share a phone number. But suppose new data show that Randy Smith, Sr., shares the birth date of Randal Smith but that his Social Security number differs from that of Marc R. Smith. Now the system might revise its guess, deciding that Marc R. Smith is Randal Smith, Jr., whereas Randy Smith is Randal Smith, Sr.

IDENTITY THEFT

Many *Scientific American* staffers have suffered mild forms of identity theft. Though disconcerting, the problems remained contained because databases are largely isolated from one another. But as companies increasingly link them together, the theft of one piece of information could infect a person's entire digital identity.

- One staffer's bank recently froze her credit card after detecting some unusual transactions. Several were legitimate, but two were not. The bank sent a new card. Who stole her card number remains a mystery.
- Another person was surprised to receive a change-of-address confirmation request from her brokerage firm. The new address was not hers. The broker, who was new to the firm, played innocent, so the staffer called the police. It turned out the broker was fishing out seemingly inactive accounts and transferring them to a collaborator, who cashed them out.
- One person started receiving delinquency notices from his cell phone provider. Evidently someone had opened an account under his name. It took a year to clear up the problem and restore his credit rating.

THE AUTHOR studied data on abandoned hard drives as a test case of how data fusion can aid police forensics investigations.

JOHN POINDEXTER, former national security adviser, tried in 2002 to set up a master government database to find terrorists.

The key to making all this work is programming the system so that it never confuses original data with a conclusion inferred from those data.

Jonas sold the system and his company to IBM in 2005. Since then, IBM has added a feature called anonymous resolution: two organizations can determine whether they share the name of one person in their respective databases—without sharing the names of all the people who do not match. The technique works by comparing cryptographic hashes instead of real names.

Privacy advocates still maintain that hashes, cross-drive analysis, anonymous resolution and the like do little to overcome their fundamental objections. After all, these systems still use personal information for purposes other than the ones for which it was originally acquired. They also make it routine to sweep up private data in a dragnet regardless of whether the people involved are suspected of committing a crime. Yet these systems generate significantly fewer false positives than did those developed in the 1980s. At some point the social benefits may come to outweigh the privacy costs of having a computer snoop through people's records.

Putting It All Together

So just how well do fusion systems actually work? Data quality remains a serious problem. Pull your credit report from each of the nation's three major credit-reporting agencies, for instance, and each report will probably contain errors and inconsistencies. Those data can lie dormant for years without causing much trouble. The danger arises when some newfangled algorithm reads too much into the inconsistencies.

Even when data are accurate, relationships brought to light by comparing databases may have real meaning or may be purely coincidental, as inevitable as finding two people in a room who share the same birthday. Maybe the four people who meet once a week to take a long drive are planning a crime. Then again, they may belong to a softball team and travel together to each week's big game.

Society's expectations for data fusion may be unreasonably high. If terrorists blend in with the population, human investigators and computers alike will be hard-pressed to find them. Most systems of data mining and fusion have some kind of sensitivity adjustment: move the slider to the left, and the system fails to find genuine matches; move it to the right, and the system makes too many predictions that turn out to be wrong. Where should the slider be set? If a system flags every third airline passenger, it will be more likely to spot a real terrorist. But it will also bring air traffic to a standstill and overwhelm law enforcement.

If a data-fusion system does not work as desired, its algorithms could be fundamentally flawed. But the problem could also be a dearth of data. Likewise, if the system is performing well, giving it more data might make it perform even better. In other words, the people building and using these systems are naturally inclined to want more and more input data, no matter how well the systems are working. Thus, data-fusion projects have a built-in tendency toward mission creep—to the consternation not only of civil-liberties advocates but also of those footing the bill. In his 1994 article Clarke concluded that trade-offs "between the State's interest in social control and individual citizens' interest in freedom from unreasonable interference [are] being consistently resolved in favor of the State."

What makes the public debate over data fusion so frustrating to me as a scientist is the fact that so little information has been publicly released about data-fusion systems in actual use. It hearkens back to the cryptography debates of the 1990s, when the U.S. government argued that there were good reasons for legally restricting the use of cryptography but that those reasons were so sensitive that discussing them in public would be a threat to national security. I suspect a similar debate is brewing over the government's use of data fusion, not to mention the applications of this powerful technology in business and even in political activities. It is a debate well worth having—and having in public. ■

MORE TO EXPLORE

Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism. Roger Clarke in *Information Infrastructure & Policy,* Vol. 4, No. 1, pages 29–65; March 1995. Available at **www.anu.edu.au/people/Roger.Clarke/DV/MatchCBA.html**

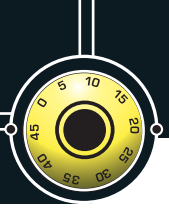
Database Nation: The Death of Privacy in the 21st Century. Simson Garfinkel. O'Reilly, 2000.

Forensic Feature Extraction and Cross-Drive Analysis. Simson L. Garfinkel in *Digital Investigation,* Vol. 3, Supplement 1, pages 71–81; September 2006. Available at **www.dfrws.org/2006/proceedings/10-Garfinkel.pdf**

Threat and Fraud Intelligence, Las Vegas Style. Jeff Jonas in *IEEE Security & Privacy,* Vol. 4, No. 6, pages 28–34; November/December 2006. Available at **http://jeffjonas.typepad.com/IEEE.Identity.Resolution.pdf**

Simson L. Garfinkel's Web sites are available at **www.simson.net** and **http://faculty.nps.edu/slgarfin**

MODERN CRYPTOGRAPHY can secure individuals' private information even as they collectively put it to work.



HOW TO KEEP SECRETS SAFE

A versatile assortment of computational techniques can protect the privacy of your information and online activities to essentially any degree and nuance you desire

By Anna Lysyanskaya

Zack has decided to try out the online dating service Chix-n-Studz.com. He signs up for an account at the Web site and fills in several screens of forms detailing his personal profile and what he is looking for in a potential partner. In no time at all, the service offers him a number of possible soul mates, among them the very exciting-sounding Wendy. He sends her his e-mail address and what he hopes is an engaging opening message. She replies directly to him, and a whirlwind e-romance begins.

Poor Zack. Soon he is also getting numerous unsolicited phone calls from political action groups and salespeople who seem to know things about him, and his health insurance company is questioning him about his extreme-adventure vacations; the unscrupulous owners of Chix-n-Studz have been selling client information. Then there is Ivan, a mischievous coworker to whom Zack foolishly showed one of Wendy's e-mails. Zack does not know that several subsequent recent messages supposedly from Wendy are fakes from Ivan.

Alice, in contrast, is on cloud nine, as is her new friend Bob. The two have met through SophistiCats.com, a matchmaking service that offers all the latest cryptographic tools. Alice logs on to its Web site protected by anonymous authorization, a system that ensures no one at the service can track who she is or when she is accessing the site. SophistiCats employs software that provides "secure function evaluation" to match her profile and partner criteria with Bob's, so no one at the service knows their information or even that she and Bob have been matched up. Imagine: a completely effective dating service that knows practically nothing about its clients!

Alice contacted Bob using a feature known as an anonymous channel, and he replied in kind—not even her Internet service provider (ISP) knows that Bob is her contact or what the messages say, and Bob's ISP is no better informed about her. Alice's roommate, Eve, however, *does* know, but only because Alice has talked about Bob and has pinned a printout of some messages above her computer. Eve could be trouble, because she is a die-hard practical joker fully capable of tapping into and altering the data flowing to and from Alice's computer (in fact, she controls the network that connects them both to the Internet). Never fear: encryption ensures that Eve can learn nothing beyond what Alice has shown her, and the coded "digital signatures" on Alice's and Bob's e-mails have made it a cinch for them to spot and ignore Eve's spoof messages.

Everything Crypto

Like Alice and Zack, most of us conduct many of our daily personal, business and government transactions electronically. We do so many things online—from staying in touch with friends to buying and selling everything, including the

KEY CONCEPTS

- Modern cryptography provides a variety of mathematical tools for protecting privacy and security that extend far beyond the ancient art of encrypting messages.
- You can keep eavesdroppers from knowing what you are saying or to whom you are saying it.
- You can remain anonymous even in online activities that require you to sign in and prove facts about yourself.
- Groups can compute virtually anything from their members' collective data (such as the winner of an election in which they are voting) without revealing any individual data.

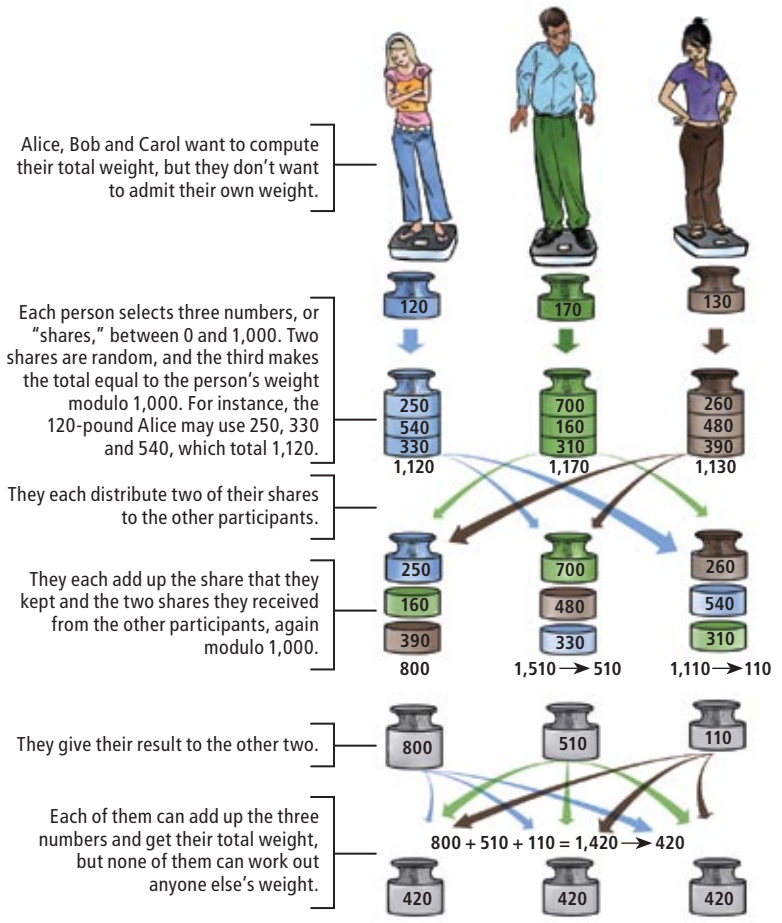
—The Editors

KENN BROWN *Mondolithic Studios*

[SECURE FUNCTION EVALUATION]

Computing Together

Secure function evaluation enables a group of people to compute anything they want from everyone's private data without revealing their own data in the process.



A more complicated procedure enables groups to multiply private numbers. By adding and multiplying bits, they can compute anything that could be evaluated from their data by a computer. The full system also safeguards against people deviating from the rules.

KEY DATES

Circa A.D. 800: Al-Kindi, an Arab scholar and mathematician living in Baghdad, writes *Manuscript for Deciphering Cryptographic Messages;* it has the first known description of frequency analysis and other cryptanalysis techniques.

1586: Thomas Phelippes uses frequency analysis to decrypt messages between Mary I of Scotland and conspirators against Elizabeth I of England. Mary and the conspirators are all executed.

kitchen sink—that getting comprehensive information about most people is as easy as logging, or recording, their online activities. And for various reasons, ISPs are already logging our activities, such as which sites we have visited and when. They are not alone. Many entities we interact with online—stores, newspapers, dating sites, and the like—keep close tabs on us as well. Thus, if we value privacy, we face the challenge of how to take advantage of everything the Internet has to offer without giving up our privacy.

An amazing discovery of modern cryptography is that virtually any task involving electronic communication can be carried out privately. Many people, including the editors of most dictionaries, mistakenly think that "cryptography" is synonymous with the study of encryption. But modern cryptography encompasses much more. It provides mathematical methods for protecting communication and computation against all kinds of malicious behavior—that is, tools for protecting our privacy and security.

Suppose, for instance, that all the members of a group connected by the Internet want to compute something that depends on data from each of them—data that each wants to remain private. The data could be their vote in an election, and they want to know the outcome without revealing their individual votes. A procedure known as multiparty computation or secure function evaluation (SFE) enables them to tally their votes in such a way that each participant learns the correct output and no one can learn anyone's individual vote—not even a coalition of malevolent insiders capable of intercepting messages on the network and substituting their own carefully crafted fake data. The SFE protocol can also provide each individual with a private output, as done by the fanciful SophistiCats service.

The basic idea behind SFE is that each participant's inputs are split into pieces, or shares, and distributed among the others in the group. Each participant then operates on the shares under his or her control (adding them, redistributing shares of the result, and so on). Finally, the group brings the pieces together again to get the final output. No one ever has the data needed to reconstruct another person's inputs [*see box at left for a simple example*].

It may not seem surprising that a function as simple as adding up votes can be evaluated securely, but recall what SophistiCats did for Alice: it worked out which members among its thousands of clients were good matches for her and gave her some limited information about those matches, all without itself learning anything about her profile or anyone else's. A Big Brother organization eavesdropping on the network traffic or combing through the data on SophistiCats's hard drives would be similarly incapable of learning anything.

SophistiCats is a fictional service, but cryptography investigators have shown how to turn it into fact. Indeed, this past January, SFE was used for the real-world problem (in Denmark, at least) of setting the price for sugar beet contracts to be traded among some 1,200 Danish farmers, based on bids that they inputted privately. Through SFE we can all have the best of both worlds: the functionality that we want over the Internet without sacrificing privacy.

MATT COLLINS

Although the SFE protocol makes possible a wide range of capabilities, its power and generality come at a price: it takes a large amount of computation and communication. The protocol is efficient enough for special tasks such as elections, yet it is too cumbersome to be pressed into service every time you click on a link to a secure Web page. Instead computer scientists have developed specialized protocols that are much more efficient than SFE for particular common tasks. These include:

Encryption. Neither Alice's ISP nor Eve can decipher the messages Alice sends to Bob. The traffic between Alice's computer and SophistiCats is secure as well.

Authentication. Alice can be sure messages come from Bob, not Eve.

Anonymous channels. Alice's ISP cannot tell to whom she has sent the messages or that she has ever visited the SophistiCats Web site.

Zero-knowledge proof. Alice can prove to someone else that something is true without revealing what her proof is.

Anonymous authorization. SophistiCats knows that she is a member when she accesses its Web site, but it cannot tell who she is. This protocol is a special case of a zero-knowledge proof.

Secret Messages

The oldest and one of the most fundamental problems studied in cryptography is that of encryption—the problem of how to communicate securely over an insecure channel (one on which an adversary can eavesdrop). Alice wants to send a message to Bob, but Eve has control over part of the channel (through the apartment's network) that Alice will use. Alice wants Bob, but not Eve, to be able to read the message.

In analyzing this problem, notice, first, that Bob must know something that Eve does not—otherwise Eve would be able to do whatever Bob can do. Bob's private knowledge is called his secret key (SK). Second, notice that Alice must know something about Bob's SK so that she can create a ciphertext—an encrypted message—specifically for Bob. If Alice knows the SK itself, the protocol is called secret-key encryption, the kind of encryption that has been known and practiced for centuries.

In 1976 Whitfield Diffie and Martin E. Hellman, both then at Stanford University, envisioned another possibility, called public-key encryption, in which Alice need not know the SK. All she needs is a public value related to the SK called Bob's public key (PK). Alice uses his PK to encrypt her message, and only Bob, with his SK, can decrypt the resulting ciphertext [*see box below*]. It does not matter that Eve also knows Bob's PK because she cannot use it to decrypt the ciphertext. Diffie and Hellman proposed the public-key idea but did not know how to carry it out. That came a year later, when Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, all then at the Massachusetts Institute of Technology, gave the first construction of a public-key cryptosystem: the RSA algorithm.

Their algorithm works for public-key encryption because it involves a so-called trapdoor function. Such a function is easy to compute, to produce the ciphertext, yet hard to invert, to recover the plaintext, unless a special "trapdoor" is used. The trapdoor serves as the secret key. The RSA algorithm was the first example of a function with a trapdoor property. For this work they won the 2002 A. M. Turing Award, the most prestigious prize in computer science.

KEY DATES

1918: Major Joseph O. Mauborgne of the U.S. Army and Gilbert Vernam of AT&T Bell Laboratories invent the one-time pad, in which the random, secret key is as long as the message itself and is only ever used once.

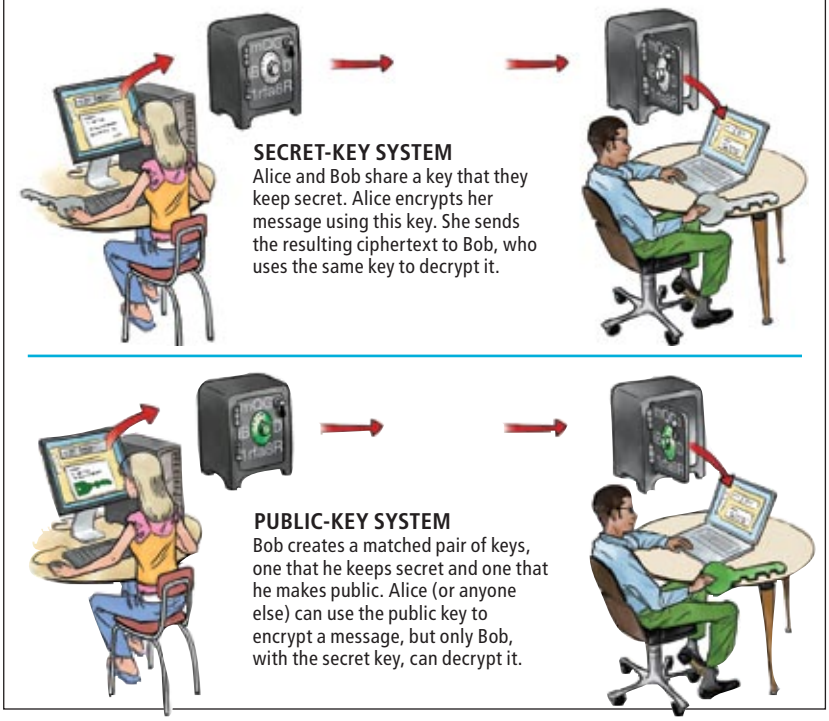
1944: At Bletchley Park in England, Colossus (the first vacuum-tube-based, programmable computing machine) decrypts German High Command messages, providing invaluable information prior to the D-day invasion of Normandy.

1945: Claude Shannon of AT&T Bell Laboratories proves that the one-time pad is unbreakable even against an adversary with unlimited computational power. This definition of secrecy is so strong, however, that he also proves that the one-time pad is the only possible cryptosystem satisfying it.

[ENCRYPTION]

Concealing Content

Modern techniques for encrypting information come in one of two types: secret-key encryption and public-key encryption.



SECRET-KEY SYSTEM
Alice and Bob share a key that they keep secret. Alice encrypts her message using this key. She sends the resulting ciphertext to Bob, who uses the same key to decrypt it.

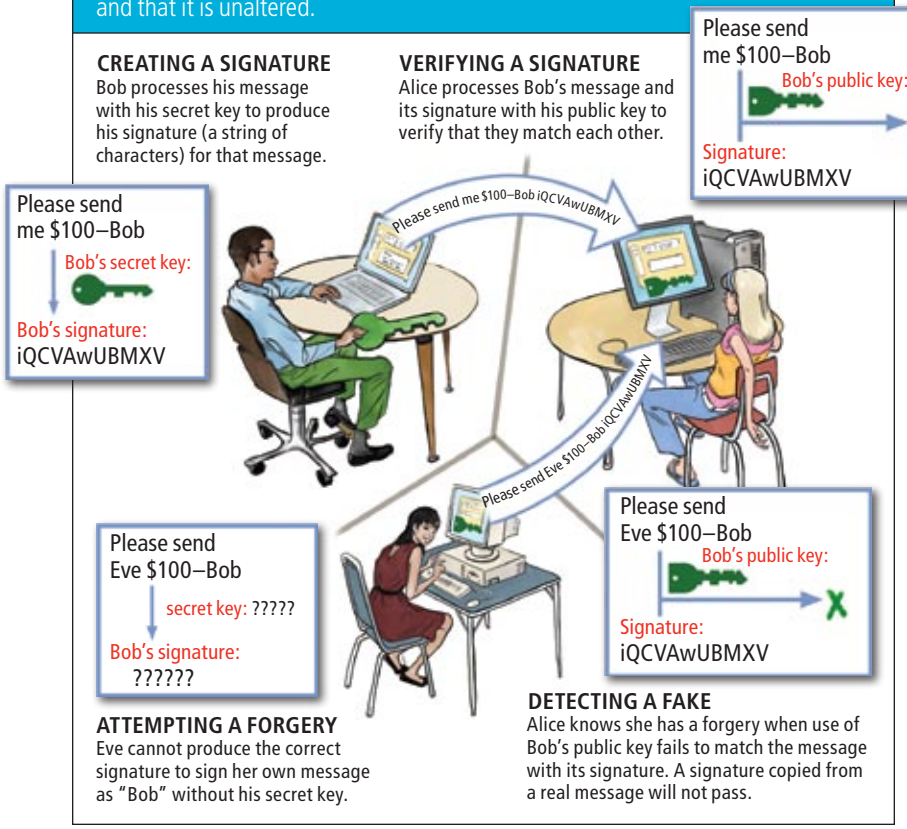
PUBLIC-KEY SYSTEM
Bob creates a matched pair of keys, one that he keeps secret and one that he makes public. Alice (or anyone else) can use the public key to encrypt a message, but only Bob, with the secret key, can decrypt it.

MATT COLLINS

[AUTHENTICATION]

Signing a Message

A digital signature guarantees that a message comes from a specific person and that it is unaltered.



KEY DATES

1976: Whitfield Diffie and Martin E. Hellman, both at Stanford University, propose public-key encryption and authentication.

1977: Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, all at the Massachusetts Institute of Technology, construct the first public-key cryptosystem, the RSA algorithm.

August 1977: In Martin Gardner's *Scientific American* column, Rivest et al. challenge readers to decrypt a message encrypted by the RSA algorithm with a 129-digit key (RSA-129). They estimate that doing so may take 40 quadrillion years.

The RSA discovery, hailed as a fundamental cryptographic breakthrough, fueled years of subsequent research in encryption and in cryptography more generally. Much hard work on encryption still remains, from finding new trapdoor functions, to studying the mathematical assumptions that underpin the security of a specific function, to defining precisely what is required for an encryption system to be considered secure.

Public-key encryption makes it possible to purchase things online without sending sensitive information such as credit-card numbers openly on the Internet. The customer's Web browser plays the role of Alice and the Web site the role of Bob. More generally, https, a protocol that most browsers now support, uses public-key encryption to provide Web browsing over an encrypted channel—look for "https://" in the URL (the address of the Web site) and an icon such as a closed padlock on the browser's status bar.

Many people also use public-key encryption for secure e-mail. Plenty of free software exists for that purpose, including the GNU Privacy Guard package (available at www.gnupg.org) first released by the Free Software Foundation a decade ago. If you do not encrypt your e-mail, it travels across the Internet in a form that is easy to read and may remain in that form on various hard drives along the way for some time afterward.

Hi, It's Me!

Closely associated with the problem of encryption is that of authentication. Suppose Alice receives the message "Alice, please send Eve $100. Love, Bob." How does she know that it really came from her boyfriend Bob and was not in fact fabricated by Eve?

Just as in the encryption scenario, Bob must know something that Eve does not so that he, but not Eve, can produce a message that Alice will accept. Thus, Bob again needs a secret key. Moreover, Alice needs to know something about Bob's SK to be able to verify that the message is from Bob. Once again, two varieties of protocol exist: secret-key authentication, more commonly known as a message authentication code, and public-key authentication, frequently referred to as a digital-signature scheme. Diffie and Hellman first envisioned digital-signature schemes at the same time that they proposed public-key encryption, and a scheme using the RSA algorithm was the first one constructed.

The chief idea is that Bob uses his SK to compute a "signature" that he appends to his message and that Alice or anyone else then uses his PK to verify that it matches the message itself [*see box at left*]. Alice knows the message must be from Bob because no one else has the SK needed to produce the valid signature.

Currently it is easy to trick an e-mail client into thinking that a message came from Bob when in fact it came from Eve. A spoofed e-mail may include fake news reports and incorrect stock quotes, tricking people to act against their best interest. But if all e-mail communication were authenticated, such an attack would be impossible: your e-mail client would digitally sign all outgoing messages and would verify the digital signatures of all incoming messages. Authentication could also combat spam by having servers reject incoming e-mail that is not authenticated by its sender. Authentication protocols did not exist when e-mail was developed in the 1970s, and many conventions from that era still prevail.

Software that everyone can use to sign their e-mail and verify signatures is freely available, for instance, as a part of the GNU Privacy Guard package mentioned earlier.

MATT COLLINS

Onion Routing

By encrypting your messages, you can prevent ISPs (or any other eavesdropper) from discovering what you send and receive, but not to whom you are communicating. For example, Alice's ISP will know if she browses an Alcoholics Anonymous Web site. Imagine if the ISP were to sell this information to car insurance companies. People would be less likely to seek help online because they would be worried that it would increase their insurance premium.

This problem could be solved with SFE: Alice's private input would be the URL she wants to look at, and her private output would be the contents of the Web page she wants to see. Using SFE, however, would be highly inefficient. In 1981 David Chaum, then at the University of California, Berkeley, proposed a much simpler solution called anonymous channels, now also known as onion routing.

As the name suggests, Alice wraps her message in layers. She encrypts each layer (and everything inside it) with a different person's public key and then adds that person's address to the outside of the layer. A message from Alice to Bob could travel as follows: Alice sends the onion to Mark, who can peel off the outermost layer by decrypting the onion with his secret key. Inside, Mark finds a smaller onion and Lisa's address. He forwards that onion to Lisa, who can decrypt it with her key, and so on. Finally, Bob receives the onion core from someone, and he decrypts it to find Alice's message.

In practice, the intermediaries are part of a network of computers set up to handle the decryption and forwarding automatically. Ideally, each intermediary continually receives lots of onions and forwards them in random order. Even if an ISP is watching all the intermediaries at all times, it cannot tell where Alice's message went or where Bob's came from, provided there is enough onion traffic on the network.

Bob himself does not know who sent the message, unless Alice chooses to reveal her identity in the message. Yet even if she remains anonymous to him, he can still send her an

KEY DATES

1982: Shafi Goldwasser and Silvio Micali, then Ph.D. students at the University of California, Berkeley, develop the definitional foundations of modern cryptography, including a practical definition of security.

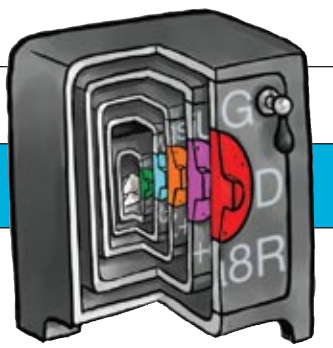
1985: Goldwasser, Micali and Charles Rackoff of the University of Toronto invent zero-knowledge proofs. A year later Oded Goldreich of Technion–Israel Institute of Technology in Haifa, Avi Wigderson of the Hebrew University of Jerusalem and Micali devise the zero-knowledge proof for graph three-colorability.

1987: Goldreich, Wigderson and Micali construct protocols for multiparty computation, or secure function evaluation, building on a two-party protocol developed by Andrew C. Yao of Princeton University.

[ANONYMOUS CHANNELS]

Hiding Connections

Data can be sent anonymously by using protocols such as onion routing, in which the data as well as the route it is to take are encased in multiple layers of encryption.



SENDING AN ONION

Alice first encrypts her message with a series of public keys belonging to randomly selected intermediaries, resulting in an "onion" with many layers of encryption. She also puts routing instructions in the layers.

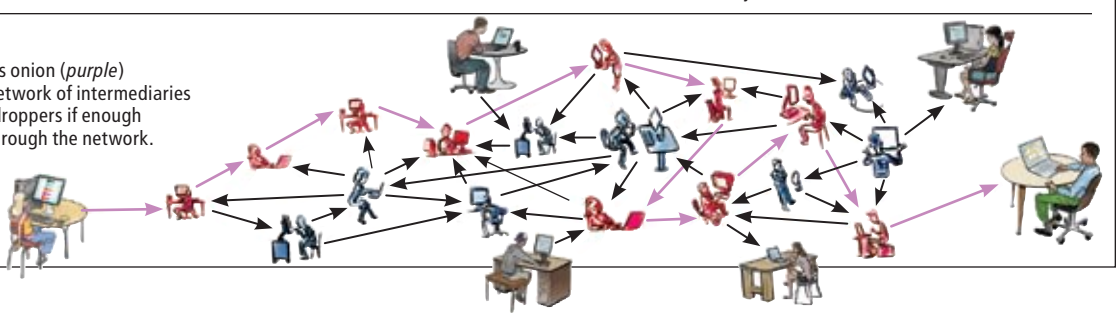
She sends the onion to Mark, whose secret key decrypts the outermost layer of encryption. "Inside" he finds an onion addressed to Lisa, which he forwards to her.

Lisa's secret key removes the next layer of the onion, and inside she finds another addressed onion, which she forwards, and so on.

Finally, Tom uncovers the core of the onion and sends it to Bob, who opens the core with his secret key to find the message. No one but Alice knows the complete route taken by the onion.

THE NETWORK

The route taken by Alice's onion (*purple*) on its way through the network of intermediaries is concealed from eavesdroppers if enough other data are passing through the network.



MATT COLLINS

[ANONYMOUS AUTHORIZATION]

Showing You Belong without Saying Who You Are

A subscriber to a Web site could sign on as a legitimate, registered user without revealing any identifying information by using anonymous authorization. The Web site would not even be able to associate the user with his or her previous visits. Such a protocol is an example of a zero-knowledge proof, in which one party proves a fact without revealing anything about the proof but its validity.

Imagine Alice and Bob play a game with a graph, three colored pens and some paper cups. The graph is a collection of dots, or vertices, connected by lines. Two vertices connected by a line are said to be adjacent. Only some graphs are three-colorable, meaning that three colors suffice to color in all the vertices without coloring any two adjacent vertices the same. Alice will prove to Bob that she has three-colored her graph without giving him any clues about how to three-color it.

The game begins with Bob out of the room. Alice draws six separate copies of the graph. Because she knows how to three-color the graph, she does so with the first copy. For the other five, she uses all of the six possible permutations of her colors. Thus, the six copies of the graph are three-colored in trivially different ways. She chooses one of the six copies at random, places it on the table and covers each vertex with a paper cup. Now Bob returns, and he gets to choose any two adjacent vertices and remove their cups. If the two vertices are the same color, he knows that Alice has been lying and that she has not drawn a valid three-coloring.

They keep repeating the inspection procedure—Bob leaves the room each time while Alice randomly chooses one of the six copies of the graph to place under the cups. From Bob's perspective, if Alice is cheating, she could be showing him many different invalid colorings, and the telltale matching adjacent vertices need not be in the same place on each one. But as he plays enough rounds, the probability that he will catch such cheating approaches 100 percent. Yet at the end of it all, he will not know how Alice has colored the graph. On each round, the two colors he sees on the chosen vertices are random; he might as well have picked the colors himself.

For any statement that has a reasonably short proof (such as "I have the credentials showing that I am an authorized user and over 18"), one can concoct a version of this game that would prove the statement without disclosing any extra information (such as "I am Alice" or "I am user #4790561").

KEY DATES

1994: Netscape Communications releases the Secure Sockets Layer protocol, which employs public-key encryption to provide security for transactions on the World Wide Web.

1994: Arjen K. Lenstra of Bell Communications Research and more than 600 volunteers on the Internet, using about 1,600 computers running recently developed factoring algorithms, take eight months to factor RSA-129. They reveal the message, "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE."

2008: An RSA key of recommended length (2,048 bits) would take more than a quadrillion years to break on a modern PC.

anonymous reply if she includes a "reply onion" containing the layers of addresses and public keys needed to route a message back to her.

Alice's and Bob's messages can remain untraceable even if some of the intermediaries leak information about what they are doing. As more participants use this system and volunteer their computers to serve as intermediaries, it becomes harder to figure out who is talking to whom.

As with encryption and digital signatures for e-mail, free software is available for anyone to communicate over anonymous channels or to participate as an intermediary. The Onion Router (Tor) project, for instance, can be found at www.torproject.org.

Private Log-ins

Let's say Alice has a subscription to the online magazine SophistiCat American. She connects to the magazine via an anonymous channel, logs on with her user name and password, and takes good care that all her incoming and outgoing messages are encrypted. Does that mean she can rest assured that no one will find out what she is doing online? Of course not—the magazine knows exactly what Alice is doing.

Alice might try to cover her tracks by using a pseudonym when she subscribes, but the reading habits of this pseudonymous user may quickly point to Alice's identity. She may reveal her zip code to look at a weather forecast, type in her birth date to check her horoscope and give away her likely gender by reading about topics such as breast cancer. Those three pieces of information—zip code, date of birth and gender—are enough to uniquely identify 87 percent of the U.S. population [see "Information of the World, Unite!" by Simson L. Garfinkel, on page 82].

Surprisingly, Alice's problem has a cryptographic solution called anonymous authorization. Alice can prove to the magazine that she is a valid subscriber each time she accesses its Web page. Yet this proof reveals nothing about which subscriber she is—not even, say, that she is the

MATT COLLINS

person who accessed it a few hours earlier. The protocol is a special case of the more general zero-knowledge proof protocol.

With a zero-knowledge proof, Alice can convince Bob that a statement is true without revealing why it is true or, in fact, without revealing any extra information at all. To prove the statement "I am an authorized user of SophistiCat American," the online magazine or a third-party service would issue a unique credential—something like a secret key—to Alice when she subscribed. Each time the magazine subsequently challenged her, she would use that key to prove she had a valid credential, without revealing the credential itself. With credentials from various authorities, Alice could provide a zero-knowledge proof of more complicated statements such as "I am an authorized user and over 18."

The basic idea of how a zero-knowledge proof works is illustrated by the scenario described in the box on the opposite page, in which Alice proves to Bob that she has colored a diagram in a special way (technically, that she has "three-colored a graph") without showing Bob how she colored it. Three-coloring a graph is a so-called NP-complete problem [see "The Limits of Quantum Computers," by Scott Aaronson; Scientific American, March]. For the present discussion, what is important about "NP-complete" is that you can pick any statement for which you have a reasonably short proof and concoct a version of Alice and Bob's game to give a zero-knowledge proof of your statement.

The three-colorability protocol demonstrates the principles that make zero-knowledge proofs possible, but it is not very efficient in practice—similar to the way that general secure function evaluation is inefficient. Fortunately, cryptography investigators have developed similar protocols for specific kinds of credentials that can serve for efficient anonymous authorization.

Breaking the Codes

How secure is secure? When Alice encrypts a message to Bob, just how difficult is it for Eve to decipher the message? And what if Eve has some inside knowledge or opportunities to try to game the system? For instance, she may already know something about the encrypted message—say, that it is the name of a local café where Alice and Bob are going to meet in person for the first time. Or if "Bob" is a secure Web server, Eve might send it carefully chosen gibberish in place of ciphertext and, from its responses, learn clues about its secret key. A widely accepted definition of security for public-key encryption covers all those bases and requires that Eve gain not even a little usable information. Among others, the GNU Privacy Guard package passes the test.

Analyzing the security of a cryptosystem is a highly developed science. Contrary to the common perception, cryptography is not a cat-and-mouse game in which a system is presumed to be secure merely because no one has shown how to break it. Instead many building blocks of cryptography rely on well-studied mathematics problems. Cryptographers cannot prove with absolute certainty that such a cryptosystem is unbreakable, but they do prove that any algorithm to break it would also answer a fundamental question that has stymied the best mathematicians and computer scientists.

Some protocols depend only on the existence of a particular kind of mathematical function. For instance, cryptographers know how to construct a public-key cryptosystem out of any trapdoor function. Thus, if someone breaks the functions used in RSA, others that were still standing could be substituted.

Only rarely is a scheme assumed secure on a more ad hoc basis. But that is done only after hundreds of leading researchers around the world have studied the algorithm for several years. The cryptography community can only afford to carry out that process for a few critical building blocks. They then prove the security of larger systems assuming the security of the building blocks. See www.SciAm.com/sep2008 for more on the assumptions behind the security of cryptosystems.

Cryptographic protocols can provide surprisingly versatile solutions to seemingly impossible privacy problems (such as anonymous authorization). But many of the privacy problems we face do not appear cryptographic in nature. If Alice is under constant surveillance in the physical world, it is small consolation that her online activities are secure. In London, cameras already watch public spaces in the interest of law enforcement. Perhaps, to protect privacy, building owners could administer the data from cameras on their property, and SFE could manipulate the data to, say, track suspects leaving a crime scene without storing everyone else's activities in a central database. More generally, when privacy is threatened by a system such as public surveillance, we should ask ourselves, What problems is the system trying to solve? And can we keep our privacy by using cryptography in solving them? ■

KATHLEEN DOOHER

[THE AUTHOR]

Anna Lysyanskaya is associate professor of computer science at Brown University, where she is a recipient of a National Science Foundation CAREER grant and a Sloan Research Fellowship. She earned her Ph.D. from the Massachusetts Institute of Technology, supervised by Ronald L. Rivest, the "R" of RSA encryption. Signature schemes and anonymous authorization protocols from her thesis are now a part of the Trusted Computing Group Standard. If you bought a new computer in the past couple of years, its microprocessor probably incorporates them.

MORE TO EXPLORE

Zero-Knowledge Sudoku. Lance Fortnow. (How to prove that you have a solution to a Sudoku puzzle without revealing your solution.) Available at **http://weblog.fortnow.com/2006/08/zero-knowledge-sudoku.html**

Introduction to Modern Cryptography. Jonathan Katz and Yehuda Lindell. Chapman & Hall/CRC, 2007. First chapter available at **www.cs.umd.edu/~jkatz/imc.html**

Multiparty Computation Goes Live. Peter Bogetoft et al. February 2008. Available at **http://eprint.iacr.org/ 2008/068**

IMPROVING ONLINE SECURITY

To protect against more numerous and sophisticated attacks by hackers, security professionals call for upgraded technology along with more attention to human and legal factors

THE PARTICIPANTS

Rahul Abhyankar
Senior director of product management, McAfee Avert Labs, McAfee

Whitfield Diffie
Vice president and fellow, chief security officer, Sun Microsystems

Art Gilliland
Vice president of product management, information risk and compliance, Symantec

Patrick Heim
Chief information security officer, Kaiser Permanente

John Landwehr
Director, security solutions and strategy, Adobe Systems

Steven Lipner
Senior director of security engineering strategy, Microsoft

Martin Sadler
Director, systems security lab, HP Labs, Hewlett-Packard

Ryan Sherstobitoff
Chief corporate evangelist, Panda Security US, Panda Security

QUIS CUSTODIET IPSOS CUSTODES? worries the classical Roman maxim: "Who watches the watchmen?" But the security vendors who stand guard over today's networked information systems are under considerable scrutiny from their competitors, their customers, hackers and, increasingly often, governments concerned about national security. SCIENTIFIC AMERICAN's editor in chief John Rennie sat down in Palo Alto, Calif., this past May with representatives from the security industry—and from some of the industries that will rely on the protections they provide—to discuss the challenges they will confront. What follows is an edited transcript of some highlights of those proceedings; a more complete version is available online at **www.SciAm.com/sep2008**

—The Editors

Who Is Responsible?

The panelists agreed on certain priorities for maintaining or strengthening data security. Some of these were technological, but regulatory and legal frameworks were also crucial.

DIFFIE: The foremost influence on these things in the next decade is going to be Web services and what I call digital outsourcing. We're going into a world where there will be a million computational services that somebody else can do for you better than you can do for yourselves. Ten years from now you'll look around and see what we call secure computing today will not exist. So what is going to be needed is a legal framework that obliges contractors to protect the security of the information. But they cannot respond to the obligation unless the technical machinery can be developed to allow them to protect that information.

GILLILAND: Yes, but if you look at how customers are actually implementing technology today, they're already far behind what it can do. That's not necessarily the problem now. It's how do we make this technology practical so that customers can actually address their own privacy issues, their own auditing processes, and manage the protection of their data for themselves to current standards, which for the most part they're not doing today.

LIPNER: For the business customers, you want the sort of things that Art and Whit are talking about: assurance about what will be done with your data, ways to describe the restrictions on it, and so on. For the consumers, you want an environment that they trust and that just works—because a lot of the growth of the Internet and Internet business is based on consumer confidence. We need to increase that confidence and ensure that it's justified.

GILLILAND: The interesting balance that we have to figure out is, How do you enable businesses to continue to share information as rapidly as possible so they can make good decisions and yet make that sharing simple?

The Dangerous Human Element

Users themselves can be the Achilles' heel of security systems because of their propensities for error and their tendency (however unwittingly) to trade data safety for ease of use. As such, it falls to technology to compensate for the potential failings of users.

HEIM: We should not underestimate the human element. I liken it to driving. The reason we have controls in place such as driver's licenses is so that people at least have a basic understanding of the rules of the road and how to operate a vehicle safely, so that we can minimize those risks. I don't think there's been enough educational outreach to end users on how to use their systems safely. I'm not necessarily proposing there needs to be a "cyber driver's license," but you know, that probably wouldn't be a bad idea because we see that many, many of the observed problems are behavioral in nature.

DIFFIE: See, that's exactly what would be an utterly monstrous idea. Cyberspace is the world of the future. If you don't have a right to be there, you don't have a free society.

ABHYANKAR: The human element is something that we can't ignore. We recently celebrated the 30th anniversary of spam. E-mail continues to be something that gets exploited. There is a dark underbelly to technology, and the rate of innovation that the bad guys have and the social engineering techniques they have to steal your data are that much further ahead of what the good guys have. That's something that technology alone is not going to solve.

GILLILAND: If you look at the research that we've been doing, around 98 percent of the data loss is through mistakes of human error and process breakdown. Being in the security industry, we're always going to be fighting the bad guys. But the bad guys are less of the problem around data loss. Being able to steal information is always going to be a business for somebody, and you can't ever fight all of them 100 percent. But we can stop the large percentage that is human and process error.

HEIM: We see on a day-to-day basis that if the technology organization itself can't anticipate the needs of the individuals, in many cases they will enable themselves to get their jobs done using consumer-grade technologies.

Rahul Abhyankar
McAfee

Ryan Sherstobitoff
Panda Security

John Landwehr
Adobe Systems

Art Gilliland
Symantec

Patrick Heim
Kaiser Permanente

Martin Sadler
Hewlett-Packard

Steven Lipner
Microsoft

Whitfield Diffie
Sun Microsystems

GABRIELA HASBUN

SHERSTOBITOFF: Right. We can't keep your information secure if you're going to e-mail it to yourself over Gmail so that you can work from home.

HEIM: Sure, if individuals are not enabled through secure technology, they will compensate using consumer technologies, such as putting in a wireless access router or copying data to a USB drive. So there are technological challenges, but there are challenges on the economics, too. What does it take to do information technology right? To do it securely and in a manner such that people can get their jobs done and they don't have to backdoor the process?

DIFFIE: In short, lack of features is frequently a security problem. If the system doesn't offer you the ability to do what you need to do securely, you will do what you need to do anyway.

The Economics of Modern Hacking

Hacking is no longer the province of curious or bored programmers. The production of malicious software is now a business, and that fact profoundly changes the scope of the challenge.

ABHYANKAR: The economic model for hacking is so well established that if it were legitimate and you were a venture capitalist looking to put money into this business, you would get good returns, right? The cost of sending malicious e-mail just keeps getting driven down. And anonymity in the network makes it harder to track down the bad guys from a legal enforcement and prosecution perspective.

SHERSTOBITOFF: A lot of the activity is not really centered on the original hackers. They're using middlemen. When you actually investigate, you end up getting to individuals—what they call "mules"—who had no awareness or knowledge that they were becoming victims of this whole scheme. We're seeing that result as an upsurge from these Web sites that say, "I have a great job for you! Make $1,000 a week!" Law enforcement can't get to the hacker who created the malicious software; the hacker or the attacker is long gone. The hackers don't actually conduct the attacks; they sell these creations for money. There's an underground economy just on sales of these attacks. You can now purchase something for $1,200 and be a cybercriminal.

SADLER: So, given that we all understand how sophisticated the bad guys have become, what level of cooperation do you think we should be employing? Because, essentially, we still all compete. We're fragmented, and the bad guys are coordinated. And there's plenty of evidence that these different organized criminal elements are actually trading this stuff among themselves. We don't have that level of cooperation among ourselves.

SHERSTOBITOFF: That's why I would advocate a vendor-agnostic approach here. To circumvent this threat takes not only a technological approach but also a community-sharing response, with research labs working together to share what they've seen. Because already, not all the malware samples in our labs come from our customers. We do get them from others in the industry. At the top, we're not like bitter rivals. It's a common problem that the industry as a whole needs to respond to.

> **"The equivalent on the Internet now is, we walk out with our entire bank account into the most unsafe neighborhoods, and then we're surprised when we're mugged."**
>
> *—Martin Sadler*

Better Education? Or Better Design?

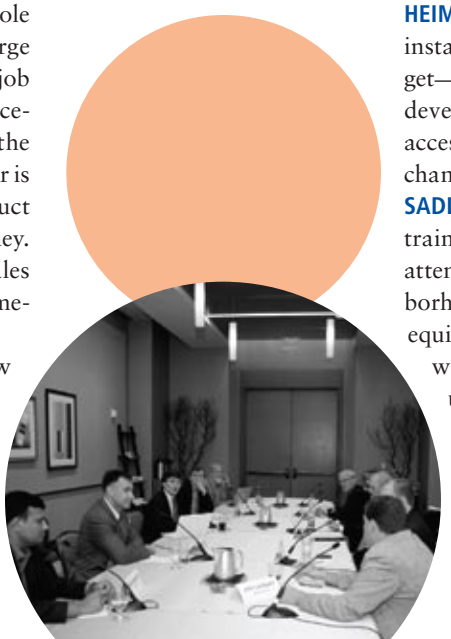
Perhaps surprisingly, the panelists generally foresaw few lasting improvements in data security from better educating end users: the nature of the threats changes too fast.

LIPNER: We need to take the burden of sophisticated education off the end user and get to the point where the technology is just helping the user be secure and you're not imposing pop-up fatigue on users, because it's counterproductive. A lot of building secure systems is about the user experience. And I think that's gotten short shrift across the industry.

SADLER: I don't think we should be putting emphasis on education at all. I think it's only education in extremely general terms that will last more than six months. You look at many of the education programs around the globe, and they're very, very short term in what they're telling people to do. Put in place the latest antivirus, that sort of thing.

HEIM: If people really knew the consequences of installing that free animated screen-saver widget—that in essence, they are saying, "I trust the developer of this little widget with complete access to my system and all my data"—it might change the way people behave online.

SADLER: I think there is an answer, though. You train young children, when they go out, to pay attention to the neighborhoods. "These neighborhoods are kind of safe; these are not." The equivalent on the Internet now is, we walk out with our entire bank account into the most unsafe neighborhoods, and then we're surprised when we're mugged. There has to be separation of concerns. You want people to be able to download the latest



GABRIELA HASBUN

screen savers, but in a part of their environment that doesn't affect their bank account.

HEIM: But when we're dealing with large-scale infrastructures, you need to be able to rapidly apply new patches and to maintain the stability of your environment. And it's not always clear-cut that if you apply a security patch, that you aren't going to come crashing down.

GILLILAND: I agree there shouldn't be some driver's license–like certificate for using the Internet. But why wouldn't we have basic end-user education when you walk into a company? "Here's your laptop, here's your PDA. I'm going to teach you the security principles for Symantec."

SADLER: And how long do you think those principles would last?

GILLILAND: Principles can last for a long time.

DIFFIE: It depends on what they are.

GILLILAND: "Don't open e-mail or don't open attachments from people that you don't know."

DIFFIE: That's a hopeless rule.

LIPNER: The only way you can address that is with underlying security and authentication. You give users a choice, but they have to know there are classes of things that are safe, whether it's Web sites or attachments or executables. If you tell a user, "You have to read the code, or you have to interpret the SSL dialogue boxes," that's too hard. For end users, you have to provide an authenticated infrastructure that allows them to know whom they're dealing with.

GILLILAND: End users will violate the trust, given the opportunity, without a certain amount of education. Even if a warning pops up and says, "Warning: this site appears to be dangerous," but the site says, "Click here to see Britney Spears naked," they will still do it. The most effective sort of virus dissemination is always social engineering. Always.

LANDWEHR: Isn't there another way we can look at solving this? Instead of focusing so much on how to educate users about malware, we can change the rules of the game for the hackers so they're less interested in attacking our computers, because we're better at protecting the information that's on them. Then if anybody steals the files that are on the disk, they're encrypted. If someone accidentally e-mails something, it's encrypted. If it goes anyplace that it shouldn't, they don't have the keys to open it.

SHERSTOBITOFF: Agreed. In the financial community, they're taking on the evolution of out-of-band authentication [joint authentication over two independent systems, such as a networked computer and a cell phone]. Some of the higher rolling traders are getting authentication devices: smart keys, RSA tokens. Some in the financial community are also putting anomaly detection in the back ends to detect suspicious patterns and localizations. Ultimately, financial institutions are adapting their technologies and authentication mechanisms so that they basically do not invite hackers.

LANDWEHR: We're seeing a lot of activity around smart cards. I've got my smart card badge here, and it's the same badge that I use to go into the buildings that we have around the world, but it also has a PKI [public-key infrastructure] credential on it that I can use to log on to applications, encrypt business documents and digitally sign PDF forms. There's also a PIN code that protects it, just like an ATM card. If you steal the card from me, you get a couple of guesses on the PIN code, and then it stops working.

The International Perspective

National perspectives on data security and privacy vary greatly. In many respects, the U.S. is lagging in its response to rising threats.

SADLER: I think there's a much greater effort in France, Germany and the U.K. to educate small businesses than in the U.S. So despite my arguing against education, I think the U.S. probably has to get some basics in place for small businesses here. Also, there's a much better dialogue among academia, government agencies and industry in Europe, particularly in the U.K. and in Germany, than in the U.S. I don't think the U.S. shows anything like enough common dialogue among those parties.

SHERSTOBITOFF: We're seeing task forces emerge in Europe that are dedicated to thwarting cybercrime. They're taking an initiative far in advance. But from our talks with the FBI, it is still not there yet in this country.

LIPNER: Because there are usages and national purposes specific to Europe and the U.S. government, additional standards will be needed. I think they'll have to be international.

GILLILAND: Obviously, there's a ton of different privacy regulations that go on throughout Europe. Companies are trying to figure out how to adhere to some process or some policy framework that allows them to follow as many of the rules as they can. That's the challenge that we haven't spent a lot of time talking about here. How do people and companies that have been trying to comply with the privacy regulations prove that they have been doing it? ■

"We can change the rules of the game for the hackers, so they're less interested in attacking our computers."

—John Landwehr

ONLINE

A full version of the edited transcript of this discussion is available online at www.SciAm.com/sep2008

THE END OF PRIVACY?

Young people share the most intimate details of personal life on social-networking Web sites, portending a realignment of the public and the private

By Daniel J. Solove

He has a name, but most people just know him as "the Star Wars Kid." In fact, he is known around the world by tens of millions of people. Unfortunately, his notoriety is for one of the most embarrassing moments in his life.

In 2002, as a 15-year-old, the Star Wars Kid videotaped himself waving around a golf-ball retriever while pretending it was a lightsaber. Without the help of the expert choreographers working on the *Star Wars* movies, he stumbled around awkwardly in the video.

The video was found by some of the boy's tormentors, who uploaded it to an Internet video site. It became an instant hit with a multitude of fans. All across the blogosphere, people started mocking the boy, making fun of him for being pudgy, awkward and nerdy.

Several remixed videos of the Star Wars Kid started popping up, adorned with special effects. People edited the video to make the golf-ball retriever glow like a lightsaber. They added *Star Wars* music to the video. Others mashed it up with other movies. Dozens of embellished versions were created. The Star Wars Kid appeared in a video game and on the television shows *Family Guy* and *South Park*. It is one thing to be teased by classmates in school, but imagine being ridiculed by masses the world over. The teenager dropped out of school and had to seek counseling. What happened to the Star Wars Kid can happen to anyone, and it can happen in an instant. Today collecting personal information has become second nature. More and more people have cell phone cameras, digital audio recorders, Web cameras and other recording technologies that readily capture details about their lives.

For the first time in history nearly anybody can disseminate information around the world. People do not need to be famous enough to be interviewed by the mainstream media. With the Internet, anybody can reach a global audience.

Technology has led to a generational divide. On one side are high school and college students whose lives virtually revolve around social-networking sites and blogs. On the other side are their parents, for whom recollection of the past often remains locked in fading memories or, at best, in books, photographs and videos. For the current generation, the past is preserved on the Internet, potentially forever. And this change raises the question of how much privacy people can expect—or even desire—in an age of ubiquitous networking.

Generation Google

The number of young people using social-networking Web sites such as Facebook and MySpace is staggering. At most college campuses, more than 90 percent of students maintain their own sites. I call the people growing up today

KEY CONCEPTS

- Social-networking sites allow seemingly trivial gossip to be distributed to a worldwide audience, sometimes making people the butt of rumors shared by millions of users across the Internet.
- Public sharing of private lives has led to a rethinking of our current conceptions of privacy.
- Existing law should be extended to allow some privacy protection for things that people say and do in what would have previously been considered the public domain.

—The Editors

HARRY CAMPBELL

FAST FACTS

Every day people post more than **65,000** videos on YouTube.

In 2006 MySpace surpassed **100 million** profiles.

Since 1999 the number of blogs has grown from **50** to **50 million**.

More than **50 percent** of blogs are written by children younger than **19**.

"Generation Google." For them, many fragments of personal information will reside on the Internet forever, accessible to this and future generations through a simple Google search.

That openness is both good and bad. People can now spread their ideas everywhere without reliance on publishers, broadcasters or other traditional gatekeepers. But that transformation also creates profound threats to privacy and reputations. The *New York Times* is not likely to care about the latest gossip at Dubuque Senior High School or Oregon State University. Bloggers and others communicating online may care a great deal. For them, stories and rumors about friends, enemies, family members, bosses, co-workers and others are all prime fodder for Internet postings.

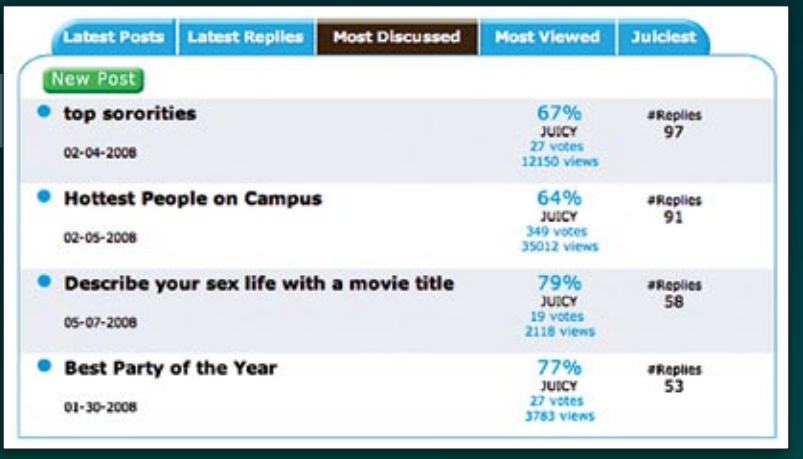
Before the Internet, gossip would spread by word of mouth and remain within the boundaries of that social circle. Private details would be confined to diaries and kept locked in a desk drawer. Social networking spawned by the Internet allows communities worldwide to revert to the close-knit culture of preindustrial society, in which nearly every member of a tribe or a farming hamlet knew everything about the neighbors. Except that now the "villagers" span the globe.

College students have begun to share salacious details about their schoolmates. A Web site called JuicyCampus serves as an electronic bulletin board that allows students nationwide to post anonymously and without verification a sordid array of tidbits about sex,

[CAMPUS GOSSIP SITES]

Blabbing to the World

No detail is too intimate for Web sites that reveal misdeeds, lascivious exploits and other assorted gossip about college life.



JUICYCAMPUS is a popular electronic bulletin board where students can anonymously post gossip and rumors about other students. The site declares that it was created with the "simple mission of enabling online anonymous free speech on college campuses." The gossip on JuicyCampus is a mix of sex, drugs, drunkenness, disease and other topics involving the dirty underbelly of college life.

DON'T DATE HIM GIRL is a site that lets women post concerns about men they have dated. Their narratives about these wayward men often include men's real names and pictures. Unverified complaints sometimes claim that the men have sexually transmitted diseases or that they are abusive.

TOMMY MOORMAN; SOURCES: JUICYCAMPUS AND DON'T DATE HIM GIRL (*screen shots*)

drugs and drunkenness. Another site, Don't Date Him Girl, invites women to post complaints about the men they have dated, along with real names and actual photographs.

Social-networking sites and blogs are not the only threat to privacy. As several articles in this issue of *Scientific American* have already made clear, companies collect and use our personal information at every turn. Your credit-card company has a record of your purchases. If you shop online, merchants keep tabs on every item you have bought. Your Internet service provider has information about how you surf the Internet. Your cable company has data about which television shows you watch.

The government also compromises privacy by assembling vast databases that can be searched for suspicious patterns of behavior. The National Security Agency listens and examines the records of millions of telephone conversations. Other agencies analyze financial transactions. Thousands of government bodies at the federal and state level have records of personal information, chronicling births, marriages, employment, property ownership and more. The information is often stored in public records, making it readily accessible to anyone—and the trend toward more accessible personal data continues to grow as more records become electronic.

The Future of Reputation

Broad-based exposure of personal information diminishes the ability to protect reputation by shaping the image that is presented to others. Reputation plays an important role in society, and preserving private details of one's life is essential to it. We look to people's reputations to decide whether to make friends, go on a date, hire a new employee or undertake a prospective business deal.

Some would argue that the decline of privacy might allow people to be less inhibited and more honest. But when everybody's transgressions are exposed, people may not judge one another less harshly. Having your personal information may fail to improve my judgment of you. It may, in fact, increase the likelihood that I will hastily condemn you. Moreover, the loss of privacy might inhibit freedom. Elevated visibility that comes with living in a transparent online world means you may never overcome past mistakes.

People want to have the option of "starting over," of reinventing themselves throughout their lives. As American philosopher John Dewey once said, a person is not "something complete, perfect, [or] finished," but is "something moving, changing, discrete, and above all initiating instead of final." In the past, episodes of youthful experimentation and foolishness were eventually forgotten, giving us an opportunity to start anew, to change and to grow. But with so much information online, it is harder to make these moments forgettable. People must now live with the digital baggage of their pasts.

This openness means that the opportunities for members of Generation Google might be limited because of something they did years ago as wild teenagers. Their intimate secrets may be revealed by other people they know. Or they might become the unwitting victim of a false rumor. Like it or not, many people are beginning to get used to having a lot more of their personal information online.

What Is to Be Done?

Can we prevent a future in which so much information about people's private lives circulates beyond their control? Some technologists and legal scholars flatly say no. Privacy, they maintain, is just not compatible with a world in which information flows so freely. As Scott McNealy of Sun Microsystems once famously declared: "You already have zero privacy. Get over it." Countless books and articles have heralded the "end," "death" and "destruction" of privacy.

[A PUBLIC LIFE]

The Internet Never Forgets

A post on YouTube can provoke global ridicule with the press of a return key. When a young man applied for a job at a U.S. investment firm, he sent along a video with his résumé. Called *Impossible Is Nothing,* it showed the student engaging in a variety of physical feats, from bench-pressing 495 pounds to doing a ski jump to breaking bricks with a karate chop. Throughout the clip, the student bragged about his athletic accomplishments and his overall success in life.

Needless to say, the video was not particularly appropriate for the job he was seeking, and his arrogance was so over the top that the video was quite funny. Apparently, someone at the investment firm leaked the video, and it was posted online. It became an instant hit and has been viewed hundreds of thousands of times. Throughout the Internet, the student has been mocked and parodied. His job prospects have diminished substantially. Although he certainly made a mistake and may have learned a lesson, his youthful bravado and misjudgment are now forever preserved in cyberspace.

[THE AUTHOR]

Daniel J. Solove is a professor of law at the George Washington University Law School and author of *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, 2007) and *Understanding Privacy* (Harvard University Press, 2008).

SOURCE: VEOH (*video clips*); GEORGE WASHINGTON UNIVERSITY LAW SCHOOL (*Solove*)

Those proclamations are wrongheaded at best. It is still possible to protect privacy, but doing so requires that we rethink outdated understandings of the concept. One such view holds that privacy requires total secrecy: once information is revealed to others, it is no longer private. This notion of privacy is unsuited to an online world. The generation of people growing up today understands privacy in a more nuanced way. They know that personal information is routinely shared with countless others, and they also know that they leave a trail of data wherever they go.

The more subtle understanding of privacy embraced by Generation Google recognizes that a person should retain some control over personal information that becomes publicly available. This generation wants a say in how private details of their lives are disseminated.

The issue of control over personal information came to the fore in 2006, when Facebook launched a feature called News Feeds, which sent a notice to people's friends registered with the service when their profile was changed or updated. But to the great surprise of those who run Facebook, many of its users reacted with outrage. Nearly 700,000 of them complained. At first blush, the outcry over News Feeds seems baffling. Many of the users who protested had profiles completely accessible to the public. So why did they think it was a privacy violation to alert their friends to changes in their profiles?

Instead of viewing privacy as secrets hidden away in a dark closet, they considered the issue as a matter of accessibility. They figured that most people would not scrutinize their profiles carefully enough to notice minor changes and updates. They could make changes inconspicuously. But Facebook's News Feeds made information more widely noticeable. The privacy objection, then, was not about secrecy; it was about accessibility.

In 2007 Facebook again encountered another privacy outcry when it launched an advertising system with two parts, called Social Ads and Beacon. With Social Ads, whenever users wrote something positive about a product or a movie, Facebook would use their names, images and words in advertisements sent to friends in the hope that an endorsement would induce other users to purchase a product more than an advertisement might. With Beacon, Facebook made data-sharing deals with a variety of other commercial Web sites. If a person bought a movie ticket on Fandango or an item on another site, that information would pop up in that person's public profile.

Facebook rolled out these programs without adequately informing its users. People unwittingly found themselves shilling products on their friends' Web sites. And some people were shocked to see their private purchases on other Web sites suddenly displayed to the public as part of their profiles that appeared on the Facebook site.

The outcry and an ensuing online petition called for Facebook to reform its practices—a document that quickly attracted tens of thousands of signatures and that ultimately led to several changes. As witnessed in these instances, privacy does not always involve sharing of secrets. Facebook users did not want their identities used to endorse products with Social Ads. It is one thing to write about how much one enjoys a movie or CD; it is another to be used on a billboard to pitch products to others.

Changing the Law

Canada and most European countries have more stringent privacy statutes than the U.S., which has resisted enacting all-encompassing legislation. Privacy laws elsewhere recognize that revealing information to others does not extinguish one's right to privacy. Increasing accessibility of personal information, however, means that U.S. law also should begin recognizing the need to safeguard a degree of privacy in the public realm.

In some areas, U.S. law has a well-developed system of controlling information. Copyright recognizes strong rights for public information, protecting a wide range of works, from movies to software. Procuring copyright protection does not require locking a work of intellect behind closed doors. You can read a copyrighted magazine, make a duplicate for your own use and lend it to others. But you cannot do whatever you want: for instance, photocopying it from cover to cover or selling bootleg copies in the street. Copyright law tries to achieve a balance between freedom and control, even though it still must wrestle with the ongoing controversies in a digital age.

The closest U.S. privacy law comes to a legal doctrine akin to copyright is the appropriation tort, which prevents the use of someone else's name or likeness for financial benefit. Unfortunately, the law has developed in a way that is often ineffective against the type of privacy threats

STRATEGIES TO PROTECT PRIVACY

The U.S. has less stringent privacy laws than do many other countries. The desire to shield people's private lives on the Internet has prompted new thinking about how to balance openness with a need to restrict release of personal details.

Appropriation Tort
A name or likeness—Angelina Jolie's face, for example—cannot be used for financial benefit in an advertisement without consent. To deal with online abuses, this common-law tort could be expanded to protect against the posting of photographs online without consent.

Breach of Confidentiality Tort
Private information disclosed in privileged relationships—to doctors, lawyers and clergy, among others—is protected. This tort law could be strengthened to cover other relationships, such as spurned lovers, former friends or ex-spouses.

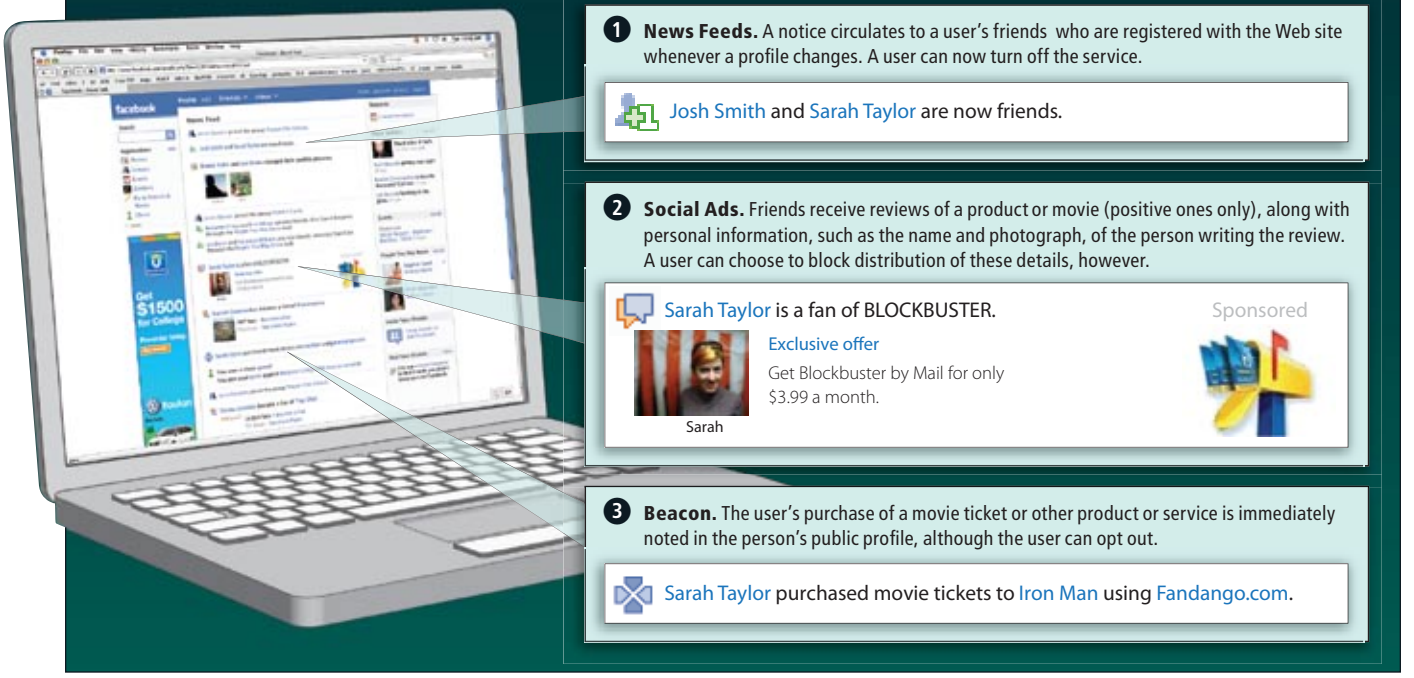
Privacy in Public
Under U.S. law, a person does not retain any privacy rights when information becomes public. In Canada and many European countries, these disclosures do not imply the loss of all such rights. The U.S. should recognize that a person does not sacrifice all privacy rights when appearing in public. *—D.J.S.*

TOMMY MOORMAN

[SOCIAL-NETWORKING SNAFUS]

My Life Is Your Life

Facebook users demanded more privacy protection after three services sent information to "friends" without asking their permission.



now cropping up. Copyright primarily functions as a form of property right, protecting works of self-expression, such as a song or painting. To cope with increased threats to privacy, the scope of the appropriation tort should be expanded. The broadening might actually embody the original early 20th-century interpretation of this principle of common law, which conceived of privacy as more than a means to protect property: "The right to withdraw from the public gaze at such times as a person may see fit … is embraced within the right of personal liberty," declared the Georgia Supreme Court in 1905. Today, however, the tort does not apply when a person's name or image appears in news, art, literature, or on social-networking sites. At the same time the appropriation tort protects against using someone's name or picture without consent to advertise products, it allows these representations to be used in a news story. This limitation is fairly significant. It means that the tort would rarely apply to Internet-related postings.

Any widening of the scope of the appropriation tort must be balanced against the competing need to allow legitimate news gathering and dissemination of public information. The tort should probably apply only when photographs and other personal information are used in ways that are not of public concern—a criterion that will inevitably be subject to ongoing judicial deliberation.

Appropriation is not the only common-law privacy tort that needs an overhaul to become more relevant in an era of networked digital communications. We already have many legal tools to protect privacy, but they are currently crippled by conceptions of privacy that prevent them from working effectively. A broader development of the law should take into account problematic uses of personal information illustrated by the Star Wars Kid or Facebook's Beacon service.

It would be best if these disputes could be resolved without recourse to the courts, but the broad reach of electronic networking will probably necessitate changes in common law. The threats to privacy are formidable, and people are starting to realize how strongly they regard privacy as a basic right. Toward this goal, society must develop a new and more nuanced understanding of public and private life—one that acknowledges that more personal information is going to be available yet also protects some choice over how that information is shared and distributed. ■

MORE TO EXPLORE

Privacy and Freedom. Alan Westin. Atheneum, 1967.

Philosophical Dimensions of Privacy: An Anthology. Ferdinand Schoeman. Cambridge University Press, 1984.

The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. Daniel J. Solove. Yale University Press, 2007.

Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy. Lawrence M. Friedman. Stanford University Press, 2007.

Understanding Privacy. Daniel J. Solove. Harvard University Press, 2008.

TOMMY MOORMAN; SOURCE: FACEBOOK (*screen shot*)

Safety Dance over Plastic

Just how harmful are baby bottles, eyeglasses and other bisphenol-A plastics? Patricia Hunt, who helped to bring the issue to light a decade ago, is still trying to sort it all out BY ADAM HINTERTHUER

On the day Patricia Hunt's career veered into an entirely different field, her graduate students at Case Western Reserve University were grumbling, itching to use some exciting new data in their own experiments, but were told to wait while Hunt (just one last time) checked on her subjects.

Hunt, a geneticist, was exploring why human reproduction is so rife with complications. She had a hunch the chromosomally abnormal eggs that plague human pregnancies were tied to our hormones. A paper outlining the results of Hunt's experiments on the hormone levels of female mice was ready for publication. All she needed was to ensure that her control population, the mice left alone in the study, was normal. Instead Hunt stumbled on a disturbing result—40 percent had egg defects.

Hunt shelved hopes of publication and scrutinized every method and piece of lab equipment used in her experiment. Four months later she finally fingered a suspect.

It was the janitor. In the laboratory. With the floor cleaner.

A single breach in protocol had turned the rodents' safe environs into acutely toxic habitats. A maintenance worker had used an abrasive floor cleaner, instead of the usual mild detergent, to wash out cages and water bottles. The acidic solution scarred the hard, polycarbonate surface of the plastic and enabled a single chemical culprit to leach out—bisphenol-A (BPA).

Hunt's unnerving discovery, in 1998, led her to speak out on the possible human health threats of BPA; she and Frederick vom Saal, a biologist at the University of Missouri–Columbia, have become prominent scientists sounding the alarm. To critics, however, Hunt and vom Saal have been alarmists; they argue that there have been no documented cases of BPA-based plastic harming humans and that fears of the chemical are overblown.

First synthesized in 1891, bisphenol-A came into use as a synthetic estrogen in the 1930s. Later, chemists discovered that, combined with phosgene (used during World War I as a toxic gas) and other compounds, BPA yielded the clear, polycarbonate plastic of shatter-resistant headlights, eyeglass lenses, DVDs and baby bottles.

But during the manufacturing process, not all BPA gets locked into chemical bonds, explains Tim A. Osswald, an expert in polymer engineering at the University of Wisconsin–Madison. That residual BPA can work itself free, especially when the plastic is heated, whether it's a Nalgene bottle in the dishwasher, a food container in the microwave, or a test tube being sterilized in an autoclave.

In recent years dozens of scientists around the globe have linked BPA to myriad health effects in rodents: mammary and prostate cancer, genital defects in males, early onset of puberty in females, obesity and even behavior problems such as attention-deficit hyperactivity disorder.

For her part, the 54-year-old Hunt, now at Washington State University, focuses on aneuploidy, or an abnormal number of chromosomes in eggs that causes birth defects and miscarriages. Last year she co-authored a paper in *PLoS Genetics* that, she says, makes her original discovery look like "child's play." Hunt exposed pregnant mice to BPA just as the ovaries in their developing female fetuses were producing a lifetime supply of eggs. When the exposed fetuses became adults, 40 percent of their

DAN LAMONT

PATRICIA HUNT

THE ACCIDENTAL TOXICOLOGIST: A geneticist by training, she discovered that bisphenol-A (BPA), an estrogen mimic, was leaching from polycarbonate plastics, which harmed her lab mice and ruined her experiments.

BIG ISSUE: In 2004, 6.4 billion pounds of bisphenol-A were created for compact discs, eyeglasses, baby bottles and other consumer products. Production grows 10 percent every year.

CAUSE FOR ALARM? When Hunt's first report came out, other scientists took note. Says colleague Frederick vom Saal: "In the field one thing people say is, 'Pat does not get it wrong.'"

Page Intentionally Blank

eggs were corrupted, which spelled trouble for *their* offspring. BPA's effects, it seemed, were not confined to the mouse receiving the dose. "With that one exposure," Hunt says, "we're actually affecting three generations simultaneously."

Although experts debate whether mice make good models for human effects, the crux of the argument over BPA is that experimental results have not been reproduced. A 2004 report from the Harvard Center for Risk Analysis found "no consistent affirmative evidence for low-dose BPA effects." According to I. Glenn Sipes of the University of Arizona, a co-author of that paper, it is this inconsistency that bothers skeptics. "I've never had a problem saying that we can see biological effects in these low-dose studies," he says. "But why are we seeing these studies that can't be repeated?" A onetime result in a rodent model, Sipes argues, cannot be extrapolated to mean negative impacts for human health.

But Hunt counters that there is plenty of corroboration to consider BPA a problem. In response to the Harvard study, she helped to produce a "state of the evidence" paper for *Reproductive Toxicology* in 2007. Along with 36 other researchers, led by vom Saal, the group analyzed hundreds of government-funded studies and found that 90 percent had concluded BPA was a health risk. It was the dozen or so industry-funded studies, vom Saal says, that failed to replicate other BPA research.

More important than these conspiratorial undertones, Hunt says, is one of communication between toxicology (the way skeptics look at BPA) and endocrinology (the way she looks at it). For instance, according to a statement on www.bisphenol-a.org, a Web site created by the American Chemistry Council (which represents dozens of companies engaged in plastics manufacturing), the toxicology of BPA is "well understood," and "BPA exhibits toxic effects only at very high levels of exposure." Current U.S. Food and Drug Administration guidelines, based partly on these findings, set a safe daily exposure to BPA at 50 micrograms per kilogram of body weight.

But according to Hunt, treating BPA like a traditional toxin is dangerous because it "doesn't play by the rules." Standard toxicology states that if a chemical is bad, "then higher doses are worse and an even higher dose is even worse," Hunt explains. But with hormones (and estrogen mimics like BPA), she says, high doses can sometimes "shut down" the body's response, and low doses are enough to exert effects.

Indeed, her lab rodents show BPA effects at just 20 micrograms per kilogram; other labs have found similar thresholds, making them one-half to one-third the FDA levels. These experiments yield bodily concentrations of BPA in ranges of parts per million, but some recent studies have even found that when BPA interacts with hor-

mone receptors on cell membranes, concentrations of one part per *trillion* can stimulate physiological responses.

That means basically any exposure to BPA could have consequences, an alarming conclusion, considering that in 2004 the Centers for Disease Control and Prevention found unmetabolized BPA in the urine of 93 percent of more than 2,500 human subjects. According to the National Toxicology Program of the U.S. Department of Health and Human Services, BPA has also been detected in human blood and breast milk.

With such ubiquitous exposure, one might expect to see numerous problems already afflicting humans. And perhaps this lack of any definitive effects most bothers skeptics. "Why do we have to work so hard to try to replicate and show these low doses really have an effect?" Sipes asks. "Why don't [reactions to BPA] stand out in black and white?"

Hunt is asking the same question. She is now working on a paper about how diet can alter responses to the chemical. It is one of many unstudied facets of the issue that, she says, may be making it difficult for scientists to reproduce their research: "There's a lot of complexity and a lot of things we just don't understand."

Treating bisphenol-A like a traditional toxin is dangerous because, Hunt says, it "doesn't play by the rules."

While scientists grapple to get a better handle on BPA, the public domain has made up its mind. On April 17 the National Institutes of Health raised concerns about BPA's established "safe" levels. Four days later Health Canada, the Canadian version of the FDA, announced a ban on polycarbonate baby bottles, citing concerns over BPA. The moves rattled the industry, as consumer outcry led stores such as Wal-Mart and CVS to announce they would phase out some polycarbonate products. And Nalgene, a company synonymous with its popular shatter-resistant bottles, decided to pull them from shelves.

The actions may seem premature given the need to solve the mysteries surrounding BPA. But recalling past hazards with mercury and lead in consumer products, Hunt feels caution is justified. "It's not like this has never happened before," she notes. "Now what we have to do is raise awareness and start looking at these products differently—and ask questions about whether they should be making their way into our everyday environment." ■

Adam Hinterthuer is a freelance writer based in Madison, Wis.

Dry Dyes

By Mark Fischetti

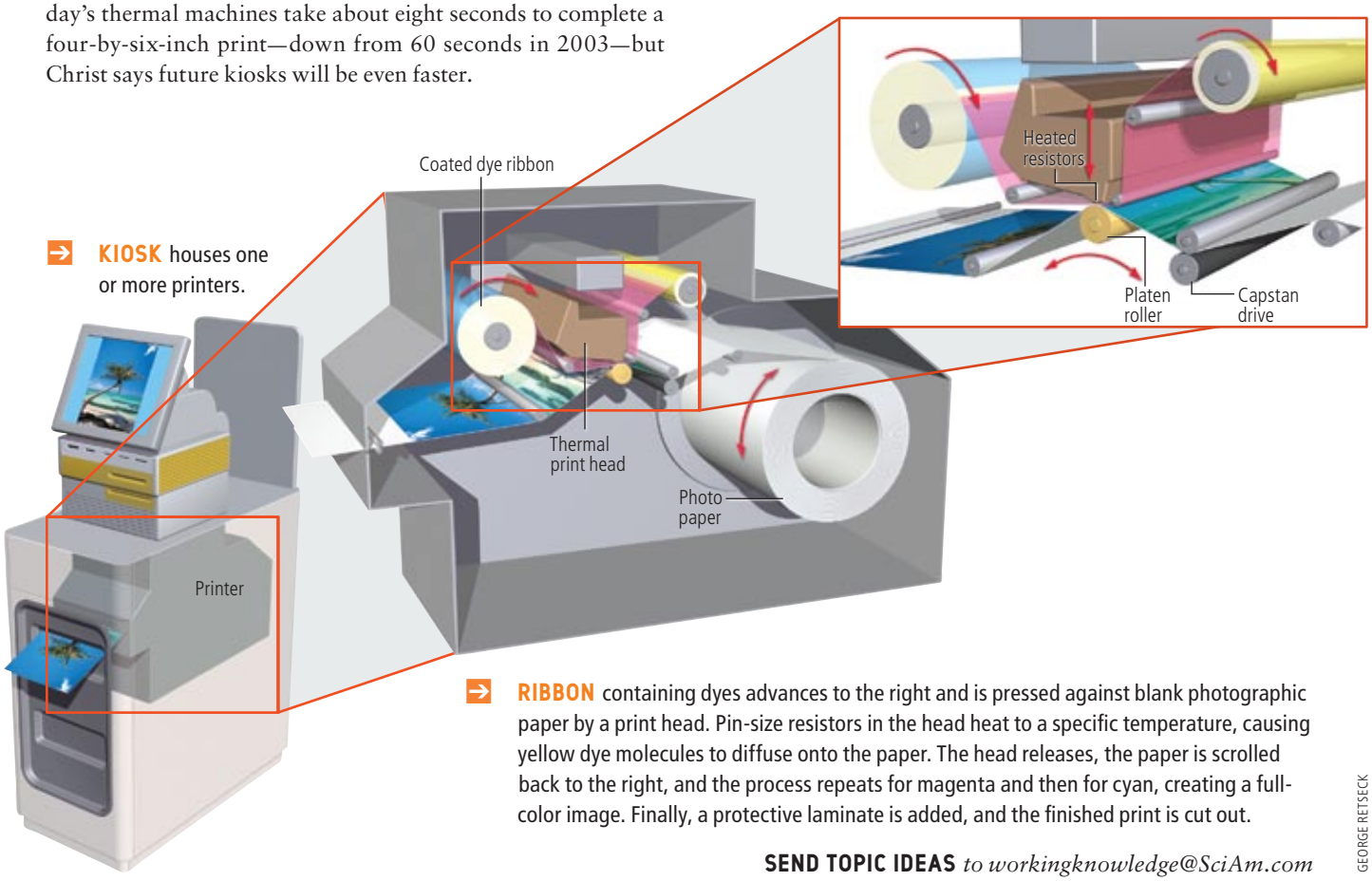
The steady rise of digital cameras has prompted the rapid growth of a new industry: instant photographic developing. A shutterbug brings her camera's memory stick to a store, inserts it into a kiosk, selects the photographs she wants, and moments later prints drop into a chute. The machines seem to be everywhere. "In five years the number of digital kiosks has skyrocketed to 85,000 worldwide," says Charles S. Christ, Jr., thermal systems director at Eastman Kodak in Rochester, N.Y.

The printers use a "dry" processing technique known as thermal dye transfer (as opposed to the traditional "wet" process of bathing exposed film in liquid chemicals). As the photographic paper scrolls past a print head, tiny resistors aligned in a row each heat up to specific temperatures, transferring minute amounts of yellow, magenta or cyan dye from a ribbon onto the paper. Together the dots form color pixels [*see illustration below*].

Larger machines in full-service stores also use processes such as electrophotography but typically for two-sided jobs such as printing custom greeting cards or calendars because the resolution is not as high as that created by the thermal approach. Today's thermal machines take about eight seconds to complete a four-by-six-inch print—down from 60 seconds in 2003—but Christ says future kiosks will be even faster.

An extreme form of dry processing is also bringing the "instant photo" back into vogue. In July, Polaroid introduced PoGo, a portable, pocket-size instant printer that makes two-by-three-inch prints from a digital camera, either over a wireless Bluetooth link or a USB cable. Start-up company Zink Imaging in Bedford, Mass., devised the process, the basic chemistry of which was invented by Stephen Telfer, now senior research fellow at the company.

In the system, colorless crystals are embedded in the photography paper. When resistors in the print head heat them to certain temperatures, they turn yellow, magenta or cyan [*see illustration on opposite page*]. PoGo can produce an image in 60 seconds, run on batteries and be used anywhere: parties, vacations, company events, all of which Polaroid is targeting. The first products sold for about $150, and 30 sheets of paper were around $10. Telfer says that larger print sizes are already being prototyped. And because no ink is involved, a unit could be housed in electronic devices such as televisions to make prints of imagery on the screen.



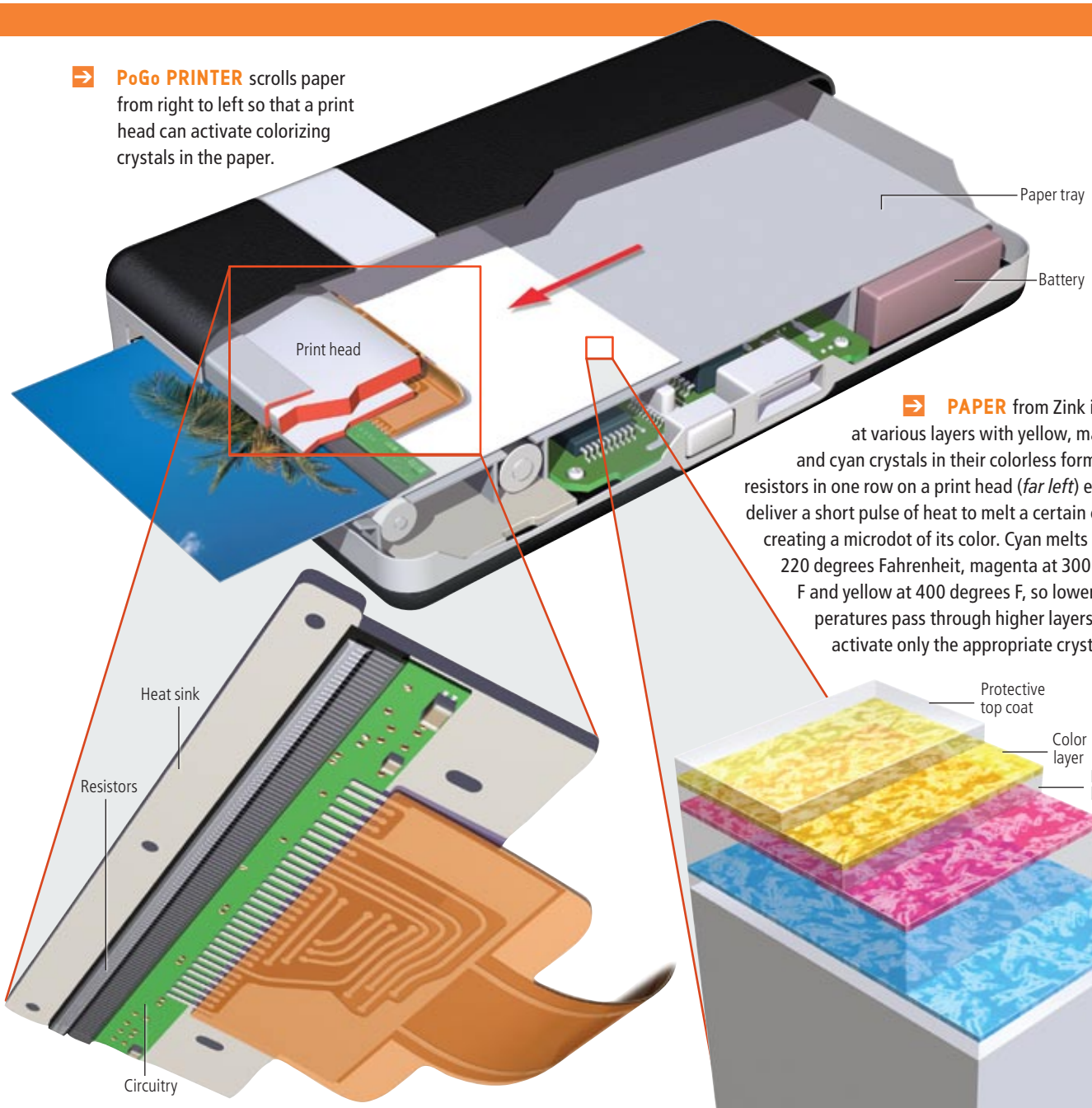
KIOSK houses one or more printers.

RIBBON containing dyes advances to the right and is pressed against blank photographic paper by a print head. Pin-size resistors in the head heat to a specific temperature, causing yellow dye molecules to diffuse onto the paper. The head releases, the paper is scrolled back to the right, and the process repeats for magenta and then for cyan, creating a full-color image. Finally, a protective laminate is added, and the finished print is cut out.

GEORGE RETSECK

SEND TOPIC IDEAS *to workingknowledge@SciAm.com*

PoGo PRINTER scrolls paper from right to left so that a print head can activate colorizing crystals in the paper.



PAPER from Zink is infused at various layers with yellow, magenta and cyan crystals in their colorless form. Tiny resistors in one row on a print head (*far left*) each deliver a short pulse of heat to melt a certain crystal, creating a microdot of its color. Cyan melts at about 220 degrees Fahrenheit, magenta at 300 degrees F and yellow at 400 degrees F, so lower temperatures pass through higher layers to activate only the appropriate crystals.

DID YOU KNOW ...

INSTANT GRATIFICATION: Polaroid introduced its familiar "instant camera" and color film in 1963. In 2007 it stopped making the camera, and it will stop selling the film in 2009. But its new portable PoGo printer for digital cameras keeps the tradition alive.

TOOTHY PICTURE: A capstan inside a kiosk printer grabs the backside of the photographic paper with tiny teeth, like sprockets on a gear, to move the paper back and forth to keep different colors in registration. The teeth indentations are hard to see, but rubbing a marker along the backside edge of a finished print, then wiping it away, will leave marked holes where the teeth sunk in.

GLOSS OR MATTE? Most photographs from kiosks have a glossy finish, created by the protective laminate. Kodak has developed a print head that can create different degrees of gloss at each laminate microspot, producing a pattern that looks like a matte finish.

Math Fix for Unfair Elections ▪ Physics Fix for Uninformed Voters

BY MICHELLE PRESS

GAMING THE VOTE: WHY ELECTIONS AREN'T FAIR (AND WHAT WE CAN DO ABOUT IT)

by William Poundstone. Hill and Wang, 2008 ($25)

This book will not reassure you: the U.S. has the worst of all possible voting systems. Known as plurality voting, it awards the prize to the candidate who gets the most votes among several contenders. The problem is vote splitting, the phenomenon in which two candidates split the support of like-minded voters and put someone who is not the most popular choice in office. Most of us will flash back to Ralph Nader in 2000. But the author reminds us of other cases—William Howard Taft and Teddy Roosevelt, for example, who split the Republican vote in 1912, leaving Democrat Woodrow Wilson to win. By Poundstone's calculation, in 45 presidential elections since 1828, at least five have been won by the second most popular candidate. "That's over an 11 percent rate of catastrophic failure," he writes. "Were the plurality vote a car or an airliner, it would be recognized for what it is—a defective consumer product, unsafe at any speed."

Often such vote-splitting "spoilers," the author points out, are financed by those who oppose their politics: in 2004, for example, Republicans paid for Nader signature drives, but it's a sad bipartisan practice. Poundstone, a writer who is fascinated with how scientific ideas—those of mathematics, in this case—play out in everyday life, recommends something called range voting as the least unfair of all voting methods. In this system, voters assign rankings to candidates, and the one with the most points wins. If the 2000 election had used range voting, for example, instead of having to cast a single vote for Al Gore, George W. Bush or Nader, voters could have rated each candidate on a scale of one to five, and the candidate with the highest ranking would have won.

ELECTRONIC ELECTIONS: THE PERILS AND PROMISES OF DIGITAL DEMOCRACY

by R. Michael Alvarez and Thad E. Hall. Princeton University Press, 2008 ($29.95)

Will the machine lose your vote? Will it be hacked? Political scientists Alvarez and Hall provide a rigorous analysis of electronic voting, and they come down heavily in favor of the benefits of the new technologies, arguing that media coverage has emphasized the problems while downplaying the potential for empowering more citizens to vote.

EXCERPT

PHYSICS FOR FUTURE PRESIDENTS: THE SCIENCE BEHIND THE HEADLINES

by Richard A. Muller. W. W. Norton, 2008 ($24.95)

Many public policy decisions today have a high-tech component. Muller, a professor of physics at the University of California, Berkeley, believes not only presidents but also the citizens who elect them need to understand the science behind the concerns our nation faces—terrorism, global warming, nuclear threats. He lays it out in lively, nontechnical language:

"A terrorist interest in crop dusters makes sense if you think about the physics. An Air Tractor 502 crop duster airplane is far smaller than a 767, but it is also a flying tanker. It has fertilizer containers that hold roughly 320 gallons of liquid, plus a 130-gallon fuel tank. It flies close the ground, where it cannot be detected by most radar technologies. Fill 'er up with 450 gallons of gasoline, and you are carrying roughly 2.1 to 2.4 tons of fuel—the energy equivalent of 32 to 36 tons of TNT.

"What could a single suicide pilot do with a full crop duster? He could crash into Yankee Stadium during the World Series. Or into the Super Bowl, or into the Olympics opening ceremony. The deaths, including trampling, might exceed those at the World Trade Center, with everything broadcast on international TV. (I virtually held my breath during those events in 2002.)"

TO INFORM VOTERS ON CLIMATE CHANGE

1 **The Bridge at the Edge of the World**
by James Gustave Speth. Yale University Press, 2008 ($28)

This distinguished environmentalist goes way beyond climate change to talk about the degradation of the planet caused by American-style consumerism—and to propose solutions large enough to make a difference.

2 **Fixing Climate: What Past Climate Changes Reveal about the Current Threat—and How to Counter It**
by Wallace S. Broecker and Robert Kunzig. Hill and Wang, 2008 ($25)

Cutting carbon emissions alone will no longer stem the warming tide: we must recapture carbon dioxide from the atmosphere.

3 **Climate Change 2007: Impacts, Adaptation and Vulnerability**
Working Group II Contribution to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press, 2008 ($165; paperbound, $85)

The ultimate source.

MICHAEL HEINZ *AP Photo (crop duster)*; CARR CLIFTON *Minden Pictures (beached glacial ice)*

Q *Why does **organic milk** last so much longer than regular milk?*

Craig Baumrucker, professor of animal nutrition and physiology at Pennsylvania State University, pours out an answer:

This longevity disparity actually has little to do with whether or not milk is organic. Rather organic milk frequently lasts longer—as long as a month, compared with about a week for regular milk—because producers use a different process to preserve it. According to the Northeast Organic Dairy Producers Alliance, organic milk needs to stay fresh longer because it is produced in fewer dairies and generally has to travel farther to reach store shelves.

The process that gives the milk a longer shelf life is called ultrahigh-temperature (UHT) processing or treatment. UHT-treated milk is heated to 280 degrees Fahrenheit (138 degrees Celsius) for two to four seconds.

Compare that with pasteurization, the standard preservation process. There are two types of pasteurization: "low temperature, long time," in which milk is heated to 145 degrees F (63 degrees C) for at least 30 minutes, or the more common "high temperature, short time," in which milk is heated to roughly 160 degrees F (70 degrees C) for at least 15 seconds.

The difference in temperatures hints at why UHT-treated milk lasts longer: pasteurization does not kill all the bacteria, just enough so that you do not get a stomachache. UHT, on the other hand, wipes out everything.

Retailers typically give pasteurized milk an expiration date of four to six days after delivery to the store. Before delivery, however, there was up to six days of processing and shipping, so the total shelf life after pasteurization is usually up to two weeks. Milk that undergoes UHT, if packaged properly, does not need to be refrigerated at all and can sit unopened at room temperature for up to six months.

Regular milk, like organic milk, can undergo UHT; much of the milk in Europe, for instance, is UHT-treated. So why isn't all milk produced this way?

One reason is that UHT destroys some of milk's vitamin content—not a significant amount—and affects some of its proteins, rendering milk unusable for cheese. More important, though, UHT-treated milk tastes different. UHT sweetens the flavor of milk by burning, or caramelizing, some of its sugars. Many Americans find this flavor offensive—just as they are leery of buying unrefrigerated milk.

Q *How long does **cellular metabolism** persist after death?*

Arpad Vass, a forensic anthropologist at Oak Ridge National Laboratory, examines this morbid mystery:

As best as anyone can gauge, cell metabolism continues for roughly four to 10 minutes after death, depending on the ambient temperature around the body.

During this interval, oxygenated blood, which normally exchanges carbon dioxide with oxygen, is not circulating. The buildup of carbon dioxide produced by cell respiration lowers the pH level of the cells, creating an acidic intracellular environment.

The acidic environment causes intracellular membranes to rupture—including those around the cells' lysosome, which contains enzymes for digesting everything from proteins to fats and nucleic acids. The burst membranes release the enzymes, which begin to digest the cells from the inside out—a process known as autolysis, or self-digestion.

The rate of autolytic spread depends on the local density of enzymes; the dispersion in liver tissue, which is rich in these proteins, is likely faster than in lung tissue, which has a smaller reserve. Autolysis also progresses more quickly in water-rich tissues such as those of the brain.

Environmental temperature is even more critical to regulating autolytic spread. Warm surroundings speed up the self-digestive process, whereas cold conditions retard it. For this reason, people who have drowned in very cold water can sometimes be revived even after relatively long periods. In such cases, the cold has slowed the autolytic process enough to prevent permanent tissue damage. ■

HAVE A QUESTION?... *Send it to experts@SciAm.com or go to* **www.SciAm.com/asktheexperts**

HENRIK SORENSEN (*glass of milk*); DAVID MCCARTHY *Photo Researchers, Inc.* (*liver cells*)