

cut State University. "It's all very well and good, but they forgot to mention that they can now track you anywhere you go. If you go through a toll booth anytime, anywhere, they will know that you have been there."

Bynum raises similar concerns about wearable devices for kids that let parents track them via GPS. "That's great if they are kidnapped or lost. That's wonderful," Bynum says. "On the other hand, they can now be tracked everywhere within 50 feet of where they are going. Tell that to a teenager who is out on a date and see what he or she says."

The general argument here is clear enough to understand. You can make a chunk of wood into a violin or a very effective club. Objects can be used outside their intended purposes, and this is no less true for high-tech devices created for a very particular purpose.

At Dartmouth College, philosophy professor James H. Moor discusses the potential use of wearable devices that would let military commanders track their soldiers in the field. Use them to track civilians at home, "and it could certainly begin to encroach upon freedom," he says.

Of course, this is only true if civilians are compelled to wear the devices, or in the case of implanted chips, to "Get Chipped," as Applied Digital Solutions' tagline urges.

"Who would decide who gets the chip?" wonders Frances Grodzinsky, a professor of computer science at Sacred Heart University who has written extensively on the intersection of ethics and technology. "Would it be voluntary? Who is doing the monitoring? Will there be a GPS system? Who would have access? Where would the chip information be located? Is this analogous to an implanted national identity card? What about the autonomy of the individual: Could he or she opt out? Would this become a way to monitor and track people without their consent? You can see that this raises a multitude of questions."

VeriChip's maker dismisses suggestions of a future police state. "If I use

my credit card at the gas station and the grocery store, that is already creating an electronic record," says Matthew Cossolotto, spokesman for Applied Digital Solutions. "There is nothing that the VeriChip does that is different from what happens electronically."

Yet it was Applied Digital Solutions CEO Richard Sullivan who raised this specter when he suggested in an interview that non-US citizens might be involuntarily implanted with microchips to make it possible to track their whereabouts. This kind of talk raises images of



WE PUT OUR BEST INTO GRADUATE DISTANCE LEARNING SO YOU CAN GET THE MOST OUT OF IT.

Wireless Communications • High-Tech MBA

Worcester Polytechnic Institute gives you nothing less than our best: the same professors that teach on campus; the same material; the same degree or certificate. In short, you get the same high-quality, practical education that made us a leading science, technology, and management university—but on your schedule, wherever and whenever you choose, with no campus-based requirements at all. Move your career ahead... without interrupting it. Call or click today for more information.



The University of
Science and Technology.
And Life.sm

508-831-5220 www.wpi.edu/+ADLN/IEEE

in brief.

Listen Up: Intelligent Fabrics March Forward

By Terry Costlow

Sleeping soldiers dreaming of the day when they don't have to worry about enemies slipping past dozing sentries might not have long to wait. Researchers are working on fabrics that the military could use to create smart tents that would listen for approaching noises, waking soldiers when suspicious sounds were detected.

Researchers involved in a joint project at Virginia Tech and the University of Southern California have devised a fabric that holds a cluster of microphones and processors. While many other programs look at intelligent clothing, this one looks at other places where fabric is used.

"We're trying to advance the science of electronic textiles, looking not just at wearables but putting sensors into tents, parachutes, or camouflage netting," says Mark Jones, an electrical computer engineer at Virginia Tech.

By spreading the microphones over a fair-sized piece of cloth, such as a tent's surface, the researchers can use triangulation to determine a sound's direction and distance. As the technology develops, algorithms will determine what the sound is and whether it's something that bears sounding an alert. Among other tasks, these fabrics could serve as monitoring systems that won't be subject to the diversionary tactics enemies often use to draw the attention of human sentries.

The initial prototype has a few computing clusters comprised of seven microphones linked to a 16-bit Analog Devices digital signal processor chip. In the prototype, a rigid circuit board houses the DSP chip and supporting circuitry, although flexible substrates will be used in later versions.

"Woven into the fabric are wires that link the microphones to the microprocessors, allowing the clusters to talk to each other and distribute power," Jones says.

In the prototype, two dozen wires were woven within three layers of cotton thread. One layer of wires ran horizontally, another ran vertically, and a buffer separated the two to prevent short circuits.

The first test, in which a truck drove past the fabric, showed mixed results. The fabric's components communicated with each other, but the truck noise was not as loud as expected, so little sound was detected. However, Jones remains optimistic. "We've got the hard part done—everything worked. Now it's just a matter of adjusting the gain so we can hear softer noises," he says.

As the hardware evolves, the focus will shift to software. Jones is devising concepts for the necessary algorithms, and he's also looking at an operating system.

The Virginia Tech-USC program is one of several developments in intelligent fabrics. Although the concept might seem a bit like science fiction, developers are certain that fabrics will some day handle part of a person's daily computing chores, doing tasks such as monitoring position or health conditions.

"This is definitely going to happen. First, in the military and industries where people wear uniforms," Jones says. For example, sensors in a uniform could monitor air quality in a chemical plant or battlefield, he adds. In other forms, hospital bed sheets could help monitor patients.

a Big Brother society that some might find incredible. But others note that in George Orwell's vision, technology lay at the heart of the mind-control culture,

and they worry that an unexamined technological evolution could lead us in that direction.

"We are building the infrastructure for

totalitarian control," says Deborah Johnson. A professor of applied ethics at the University of Virginia, Johnson works specifically in the technology, culture, and communication arena. She suggests that the public has so far been willing to accept new pervasive devices or applications without question because of a too-enthusiastic faith in the present commercial and political systems. "Right now, people are not afraid of it because it is not being built by the government. It's being built by the market and by commercial interests," she says. Those commercial interests tout the technology for particular uses, "but once it is all set up in place, it will only take a slight shift in political ideology for it to be used in other ways."

And more concerns exist than just the totalitarian threat. On a deeper level, Johnson worries about the fundamental transformation that pervasive computing could bring to human existence.

On the one hand, we are "making a world in which it is easier and easier for people to do things," she says. But can things get too easy? Could we phase out the need for our own bodies, building "a world in which I sit in my chair and make very small movements and literally everything would come to me?" she asks.

Take it one step further. What if we could embed a device to extend perception beyond the ultraviolet or embed elasticity "so we can jump higher, be more like kangaroos or something," says Herman Tavani, a philosophy professor with expertise in computer ethics at Rivier College in New Hampshire. "It's inevitable with the way things are going that those types of possibilities will be there, and this convergence of biotechnology and nanocomputing ultimately will threaten the whole sense of what it means to be human."

Society might be heading that way faster than we suppose. Bynum points to recent efforts in which computers have been used successfully to "read" a paralyzed man's thoughts—in effect, to convey messages based solely on his mental activities. "That sounds terrific," Bynum says, "but it also means

that if someone could gain control of the computers that are hooked to your brain, they could gain control of you in all sorts of ways that you wouldn't know about."

Before we reach that point, there are the more imminent threats of spying, snooping, and, ultimately, controlling. Grodzinsky suggests that given these manifold risks, it would be a mistake to let these pervasive technologies evolve "without designing policy that is fair, just, and well-reasoned."

There's supposed to be policy here?

THE POLICY LAG

In May 2002, Florida family Jeffrey, Leslie, and Derek Jacobs volunteered to receive the VeriChip identity chip. The procedure went forward with Applied Digital Solutions' support—and without the Food and Drug Administration's approval; the FDA must still determine whether the chip is a regulated device.

In fact, considerable confusion has surrounded the chip's status. In response to a letter from the FDA, Applied Digital Solutions put out a press release saying the FDA had determined the chip was not regulated because it was not intended as a medical device. The FDA responded that it had made no such determination; it warned the company to stop marketing the product and even temporarily halted trading of the company's stock.

With so much at stake, this hardly seems like an ideal way to make policy—which is why some observers say they are wary of leaving things in the hands of lawmakers.

"I would not feel secure with a legislative fix," says Johnson. If the issue here concerns ensuring that technology is used for its intended purpose, you need look only as far as Napster's much-touted use of file-sharing technology to see how difficult it is for the law to keep pace with reality. "We know that legislative fixes have not worked in the case of intellectual processes. It's too easy for technology to bypass legislation."

Some say the alternative lies with the

intellectual community. To set meaningful policy, "there would have to be a committee that was made up of computer ethicists as well as policymakers and bioethicists in order to ensure that there would be an ethical policy for implementing" new pervasive devices, says Grodzinsky.

Others say there must first be a comprehensive public dialogue in which new technologies' risks and rewards are examined and debated to give voice to whatever consensus might emerge. "This is not just for computer professionals. This is not just for philosophy professors like me. This is a social obligation for everybody," says Bynum.

But for the sake of argument, let's start with computer professionals.

THE ENGINEER'S ROLE

Although potential dangers are certainly inherent in pervasive devices, the devices' designers will justly declare their innocent intentions. They have good and positive uses in mind, after all. Yet the threat of these technologies lies not in their appropriate use but in their potential misuse. Some say engineers can and should be held responsible for those misuses. They say pervasive technology makers have a responsibility to build their devices so as to make them impervious to malicious adaptation.

"I don't think the engineers are off of the hook. Those who produce the device do bear some responsibility for whatever the consequences might be," Moor says. While the risk might never be eliminated in creating a particular device, "it seems to me that there is a positive duty on the part of the engineer to make it safer."

This might mean designing a device that requires the user's willing participation. Many of pervasive computing's ethical concerns center on the fear that people might be compelled to use, wear, or have implanted in themselves a particular device. An engineer who sees that potential would, therefore, have an ethical responsibility to minimize that risk, says Moor.

IEEE Computer Society Publications Office

10662 Los Vaqueros Circle, PO Box 3014
Los Alamitos, CA 90720-1314

STAFF

Associate Lead Editor
Shani Murray
smurray@computer.org

Group Managing Editor
Crystal Chweh
cchweh@computer.org

Senior Editor
Dale Strok

Associate Editor
Dennis Taylor

Assistant Editor
Denise Kano

Editorial Assistants

Rebecca Deuel, Joan Hong, and Ty Manuel

Magazine Assistant
Pauline Hosillos
pervasive@computer.org

Contributing Editors

**Cheryl Baltus, Kirk Kroeker, Anne Lear,
Keri Schreiner, Joan Taylor, and
Margaret Weatherford**

Design Director
Toni Van Buskirk

Layout & Technical Illustrations
Carmen Flores-Garvey and Alex Torres

Production Assistant
Monette Velasco

Publisher
Angela Burgess

Assistant Publisher
Dick Price

Membership & Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Assistant Advertising Coordinator
Debbie Sims

Submissions: Submit two copies of all articles and track proposals to *IEEE Pervasive Computing*, Magazine Assistant, 10662 Los Vaqueros Circle, Los Alamitos, CA 90720-1314; phone +1 714 821 8380; pervasive@computer.org. Manuscripts should be approximately 5,000 words long, preferably not exceeding 10 references. Visit <http://computer.org/pervasive> for editorial guidelines.

Editorial: Unless otherwise stated, bylined articles as well as products and services reflect the author's or firm's opinion; inclusion does not necessarily constitute endorsement by the IEEE Computer Society or the IEEE.



in brief...

Sonic Flashlight

By Danna Voth

George Stetten is an MD who doesn't practice medicine. One of the reasons is that he doesn't like to stick needles into people. "You can't see what you're going to hit under the skin, and I've always been bothered by that," he says.

So Stetten invented a device he calls the Sonic Flashlight. It uses a half-silvered mirror to project an ultrasound image's virtual reflection onto the same physical location the image is taken from. This lets the viewer "see" features under the skin. Stetten calls his new visualization method *real-time tomographic reflection*.

The Sonic Flashlight could be very useful to doctors trying to insert catheters into veins, especially deep ones that are harder to hit. The device could also be used for breast, kidney, and liver biopsies. Ernest Manders, a plastic and reconstructive surgeon who tested the device, says it would be a boon to emergency medical technicians on ambulances, medical staff in operating rooms, and soldiers on a battlefield. "I think it is a nifty idea that will help people manipulate needles in a much safer and expeditious fashion," Manders says.

Stetten's version improves on present methods because it's small and portable, you don't have to wear it, and it lets you look directly at the actual area of the patient's body you are manipulating. Current clinical ultrasound use requires the physician to look away from the patient to view the onscreen ultrasound image. First developed three and a half years ago, the latest model of the Sonic Flashlight is a foot-long portable device. Stetten says the next one, due out this spring, will be about six inches long.

The device has not been tested on live humans. Stetten and his colleagues have used it in phantoms, such as a butchered turkey breast with an olive inserted inside it, and in human cadavers. They also tested it on live pigs, and Stetten hopes to get a grant from the National Institutes of Health to extend the studies on animals. Roberta Klatzky, chairman of psychology at Carnegie Mellon University, started research designed to test how well people can use the device to hit something under the skin with a needle at various angles and in different lighting.

"The idea is that this would be a kind of tool like a stethoscope that you carry around with you, and whenever you need to put something into a vein, you just flip it open and then look right inside [the body]," Stetten says.



A hand as seen through the Sonic Flashlight's mirror.

"It is a myth that technology is ethics-neutral," Bynum says. "The idea that you can make, design, and sell this stuff

and then let someone else worry about the ethical implications is a complete ethical irresponsibility."

However, others take the opposite view, placing the responsibility not with the engineers but with those who commission their work.

Engineers "are being paid to determine the proper methodology and engineering functions," Lakhanpal says. "I think it's the person requiring that application who has to consider those ethical implications. Unless it is something very clear cut, unless it is the Manhattan Project, I don't think you can place that burden on the person who creates a particular piece of technology."

Whether or not an engineer accepts ethical responsibility for a technology's uses, some would argue that engineers' willingness to address these issues ultimately leads to a better end product.

Johnson says that when ethics concerns are raised, engineers too often dismiss the issue by declaring the technology's many useful aspects. "It's a kind of deflection of the criticism on the grounds that 'technology has benefits.' But we should not deflect the criticism," she says. "Instead, why not rethink the technology and what we are trying to do with it in order to avoid these negative side effects?"

That said, you might still wonder about the mark of the beast and the dozens of Web sites that identify the VeriChip as Satan's delivery mechanism of choice.

Applied Digital Solutions spokesperson Cossolotto says he is well acquainted with the phenomenon. Neither he nor any of the ethicists I spoke to could come up with a reason why the VeriChip in particular has drawn fundamentalist Christian concern. Biometrics in general has raised such concerns among readers of the Book of Revelation, but only this device appears to have assumed such centrality.

Cossolotto sees a surface similarity between his device and the mark described in Rev. 13:16-18, but he says that perhaps the Christian community is taking the passage a little too loosely. "I don't want to question anyone's religious beliefs," he says, "but I would ask them to look at the words." ■