



Notes from the Community

Editors: Mary Baker ■ HP Labs ■ mary.baker@hp.com
Justin Manweiler ■ IBM T. J. Watson Research Center ■ jmanweiler@us.ibm.com

From Nifty Gadgets to Dire Warnings

Mary Baker, HP Labs

Justin Manweiler, IBM T.J. Watson Research Center

Thank you for reading this quarter's edition of Notes from the Community. Recent contributions to our Reddit community include stories about cool new gadgets, displays, and nostalgic and whimsical projects, yet we also received some ominous warnings. These warnings indicate that not all of society is comfortable with the current directions of the Internet of Things (IoT) and pervasive technologies. As an industry, we need to understand and address these concerns.

WEARABLE WONDERS

Enthusiasm for wearables continues, but our contributors now focus on articles about wearables for specific applications and demographics.

Tagging the NFL

For the 2015 season, all players in the National Football League (NFL) will have real-time location technology embedded in their shoulder pads.¹ Zebra Technologies' MotionWorks real-time locating system has an accuracy of ± 4 to 12 inches (depending on the amount of averaging in the

system). This allows tagging of players, officials, flags, chains, and other important elements of the game. Receivers in the stadium (that is, RF receivers—not wide receivers!) send the sensed location data to the cloud for processing, with real-time results providing the speed of each player at each moment of a play, the player's accumulated yardage, coverage heat maps, and more.

Last year, the NFL tested this technology in selected stadiums, and this year they are using it in their NFL app for Xbox One and Windows 10. In a high-light clip available almost immediately after the live play, viewers can watch the play unfold with each player tagged with his speed and other information.

Cool Toys for Middle School Girls

According to Kyle Vanhemert, teen girls have the “coolest wearable out there” with Jewelbots (www.jewelbots.com),² which take the idea of friendship bracelets to the extreme. The bracelets look like a colorful elastic hairband with a plastic flower that can light up or vibrate when another Jewelbot-wearing

friend is nearby. The bracelets use Bluetooth to sense proximity.

A smartphone app (or a computer with Arduino software) lets kids program the bracelets' behavior. The programmer can assign different colors to different friends and cause the bracelets to flash or vibrate in various ways. Kids can also send haptic messages to each other or to groups of friends using their own codes by pressing the button on the flower charm. The company founders wanted a way to encourage young girls to take up programming. If my own (now high-school aged) daughter's reaction to the idea of Jewelbots is any indication, the founders have succeeded. My daughter (also known as the “focus group”) feels the bracelets would have been terrific fun at that age.

Yet could this increased visibility of friendship connections also add to social angst and hurt feelings? The bracelets take advantage of the idea that in middle school “the enmities and allegiances that form and dissolve in a single day rival anything that might be taught in European history class. What's more, teens and preteens crave ways to make these connections visible.”² Depending on the fluidity of haptic messaging, the bracelets could also be a great way to cheat with other students on multiple-choice exams.

Wearables for Unmentionables

An unsuccessfully funded Kickstarter project offers a somewhat less

JOIN OUR SUBREDDIT

This column offers a summary of interesting news and research in pervasive and mobile computing, with content drawn from submissions to a shared community on the social news site Reddit, at www.reddit.com/r/pervasivecomputing. We encourage you to join our subreddit and spread the news of this site to others, so that together we can build a sustainable online community for all aspects of pervasive and ubiquitous computing.

—Mary Baker and Justin Manweiler

savory wearable. As CNET’s Eric Mack reports, “we may just have hit peak wearable” with this gadget,³ which would keep track of and help analyze the wearer’s flatulence so the wearer can adjust his or her diet in appropriately gas-reducing ways. The user enters food information on a smartphone app and wears the sensor on his or her rear-end or in a back pocket. The Kickstarter page (www.kickstarter.com/projects/963861855/keep-track-of-your-gases-with-ch4) includes an almost charming video portraying cartoon figures suffering gaseous embarrassments that should vanish given sufficient time with this wearable and its app.

PEOPLE WITH TOO MUCH FREE TIME

One of the most enjoyable aspects of the pervasive computing and DIY community is the zany variety of projects that people work on just for the fun of it. At least, we hope they are having fun, because these inventions aren’t likely to make anyone rich.

Listen to the Tortilla

In response to a previous video’s depiction of a tortilla slapped onto a phonographic turntable, UpgradeTech decided to see if they could produce an actual song-playing tortilla. Not only did they succeed, but you can do it too by following their instructable at www.instructables.com/id/Make-a-Working-Playable-Tortilla-Record-with-a-Las. You’ll need a laser cutter and uncooked flour tortillas (apparently, corn tortillas are too lumpy and cooked tortillas shred too easily). I’m not sure how many phonographs will play this tortilla, but UpgradeTech uses a Numark PT-01 with a spare 78 diamond needle (see Figure 1). We are also cheerfully informed that the tortilla remains edible but tastes burnt. Enjoy watching and listening to the tortilla play Jarabe Tapatío (The Mexican Hat Dance) at www.youtube.com/watch?v=rdzCv_9eaoM.



Figure 1. UpgradeTech’s song-playing tortilla. (Source: UpgradeTech; used with permission.)

Watch the Microwave

We also received a link to an oldie-but-goodie. In 2011, a team of four University of Pennsylvania students won the 2011 PennApps Hackathon by modifying a microwave to play YouTube videos, where the length of the video matched the cooking time of the food. Forty-one teams competed that year, with most teams predictably writing smartphone apps. The winning team decided it would be more interesting to hack a microwave, because it is “outdated, kind of like TI calculators.”⁴ A tablet attached to the microwave played the video while the food was cooking, and when finished, the microwave sent a tweet (see Figure 2).

The challenge for the students was that there is no API for programming a microwave. The team couldn’t even get through the cover of their first microwave and had to use another in the hackathon. “We were lucky enough to see how the pieces were put together; we were able to take it apart slowly, and we were lucky we didn’t kill ourselves with the capacitor inside it.”⁴ See Brian Dzenis’ article

at <http://technical.ly/philly/2011/09/21/pennapps-fall-2011-hacked-microwave-driven-video-player-wins-2500> for more information about this IoT microwave, created long before the term “IoT” became fashionable.

IT’S NOT ALL FUN AND TOYS

With new gadgets come new attack paths, and it’s getting scary. Sadly, we can’t even keep our old toys running.

Your Smartwatch Tells Time (and Secrets)

The Open Web Application Security Project (OWASP) IoT Top 10 Project (www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project) grew from concern on HP’s Fortify on Demand team that many security and privacy issues are overlooked or insufficiently understood in the IoT space. The team’s most recent report focuses on smartwatches and associated smartphone apps and cloud components (<http://go.saas.hp.com/fod/internet-of-things>).⁵

It probably surprises no one that all of the 10 watches analyzed exhibited

NOTES FROM THE COMMUNITY

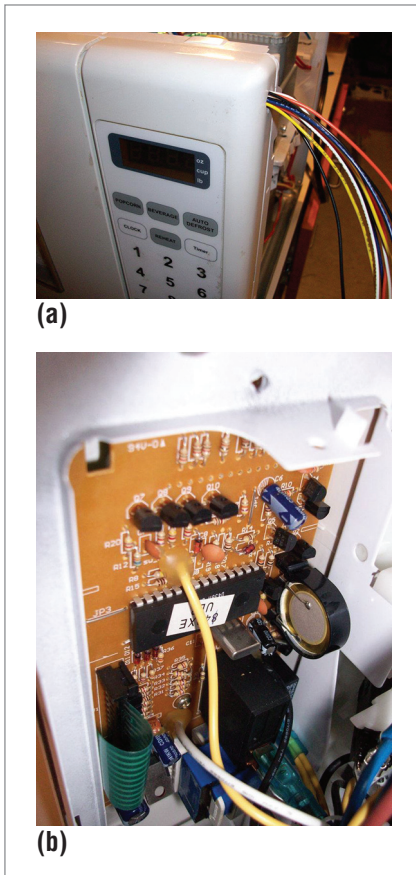


Figure 2. The (a) outside and (b) inside of the contest-winning hacked microwave. (Source: Kevin Conley; used with permission.)

problems, such as insufficient user authentication, broken transport encryption, or APIs that let hackers determine valid user account names. Given that many of these watches garner personal information about location, weight, workouts, and user activities, one hopes that the guidelines offered in the report will help developers fix and avoid some of these pitfalls.

Don't Try This in Traffic

Contributors submitted several links about attacks on cars. Wired.com's Andy Greenberg writes about his participation in an experiment in which Charlie Miller and Chris Valasek wirelessly took over the controls of the Jeep Cherokee Greenberg was driving

on a St. Louis freeway (www.wired.com/2015/07/hackers-remotely-kill-jeep-highway).⁶ The hackers blasted the radio, air conditioning, windshield wipers, and wiper fluid, making it hard to see or hear. Then they turned off the accelerator while Greenberg was stuck heading up an overpass. The jeep slowed to a crawl on a part of the interstate with no shoulder. Then, as he aimed for a ditch, they cut his brakes. The hackers could determine the jeep's position and speed, so they could pick where and when to cause the most havoc. Miller and Valasek shared their work with Chrysler, which issued a patch before the code for the hacks was made public at a Black Hat conference.

In a subsequent article (www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget),⁷ Greenberg describes another wireless attack path through a dongle plugged into dashboards so that insurance companies and owners of vehicle fleets can have access to vehicle speeds, locations, and other information. Demonstrating the hack with a Corvette, a team from the University of California at San Diego sent SMS messages to a dongle to disable the car's brakes. Metromile, a distributor of the dongles, has issued a patch.

As if all of this isn't scary enough, Sean Gallagher of *Ars Technica* writes that we're only just entering the era of car hacking, with many new exploits on the way, some of which are hard to patch (<http://arstechnica.com/security/2015/08/highway-to-hack-why-were-just-at-the-beginning-of-the-auto-hacking-era>).⁸ Some car manufacturers have been willing to work with the hackers to fix the exploits as quickly as possible, while others have taken the approach of suing the security researchers instead. Read more of Gallagher's article for an in-depth explanation of the state of automotive security.

Don't Try This in the Air—Or Anywhere Else

Many readers will already have seen this story in one form or another. As reported

by James Vincent of *The Verge* (www.theverge.com/2015/7/16/8976337/drones-quadcopters-handguns-legal)⁹ and others, a drone hobbyist with a history of "drone rage" mounted a semiautomatic handgun on a homemade drone and posted a videotape of it firing four times.

This comes at a bad time for the drone industry and hobbyist community, given that it occurred not long after the Federal Aviation Administration decided to be more flexible about approving commercial drone flights and to ease up on sending pulldown requests for videos of people flying drones where they shouldn't. And while people are already uncomfortable about drones' capabilities for remotely spying on them (see below), this evidence of the feasibility of do-it-yourself remote-controlled airborne weapons is even more worrisome.

Looming Extinction

One of the more unusual submissions to our Reddit site this quarter is a video presenting the repercussions of Sony's decision to stop repairing its Aibo robotic dogs (<http://digg.com/video/the-people-trying-to-save-their-robot-dogs-from-extinction>).¹⁰ In our industry's rush to create new technologies, we often don't think about what it means to lose the older technology. Sony produced approximately 150,000 of these toys from 1999 to 2006, and for some Japanese households, these delightful interactive toys were as close as they could come to having a family dog.

The video focuses on one couple in particular, whose Aibo toys are truly a part of their family. Unfortunately, the toys break down over time, and the owners are wondering how they will keep their pets "alive" when they can no longer salvage parts from some toys to fix others. In fact, the video opens with an Aibo funeral ceremony. As one of the owners laments, "One day all [Aibo's] parts will be gone, and Aibo will die."

INTERNET OF ANGST

Daily reports of new attacks and vulnerabilities don't go unnoticed, and society's worries grow accordingly. As a result, readers this quarter submitted an unusual number of articles depicting dystopian views of our technological future and our society's increasing concern.

Useless Things of the Internet

In *The Atlantic*, Ian Bogost writes about the difference between Mark Weiser's vision of ubiquitous computing, in which computers become invisibly embedded in our world, and what we are actually seeing with IoT, where computing becomes "more visible, brazenly visible, in fact" (www.theatlantic.com/technology/archive/2015/06/the-internet-of-things-you-dont-really-need/396485).¹¹ Bogost believes IoT is mostly about taking over previously "dumb" devices for no better reason than to say they're no longer dumb, because Silicon Valley wants to turn all other industries into the computer industry so a few technology companies can make more money.

He illustrates his disgust with amusing and fairly harsh commentary about particular examples drawn from the endless projects on crowdfunding sites, such as an app that checks how much propane is left in your grill's tank ("Look at me, using this app, it checks my propane. Isn't that cool? Look at me, running this Kickstarter. Aren't I cool?"). He even takes on established devices, such as the Nest Learning Thermostat (<https://nest.com>), claiming that "at best, it will probably still take a couple years to break even on the cost of the Nest device," plus what you'll have to spend on drywall work for the installation. Ominously, he states that "We already chose to forego a future of unconnected software. All of your devices talk constantly to servers, and your data lives in the cloud because there's increasingly no other choice. Eventually, we won't have unconnected things, either. We've made that choice too, we just don't know it yet."¹¹

Please Don't Look at Us List

It seems that for every positive article we see about drones, we encounter another describing what can go wrong, and now some people are trying to protect themselves from these problems. As of February 2015, according to Andrew Zaleski of *Fortune*, over 10,000 people had registered their properties' longitude and latitude at www.noflyzone.org as areas that drones should avoid (<http://fortune.com/2015/02/18/noflyzone-do-not-call-list-drones>).¹² This list is the equivalent of the "Do Not Call List" for phone numbers.

The main concern for registrants seems to be privacy—they do not like the idea of drones spying on them, and that was even before the incident with the drone-mounted handgun. The service maintainers claim that "We coordinate

Complicated information-rich visual overlays are particularly hazardous when people need to react physically and quickly to events to remain safe.

with participating drone manufacturers to automatically prevent drones from flying over your property." While partners will supply the no-fly-zone information to users, some partners and drone manufacturers will even use the data to program physical geo-fences and will maintain the information via software updates. Apparently, future updates will allow exceptions for delivery drones. However, the whole system is voluntary—there really is no current way to enforce the no-fly-zones for homeowners. The list maintainers hope that hobbyists and the drone industry will voluntarily "do the right thing."

Aggravated Reality

A recent *Ars Technica* column investigates both positive and dangerous applications of augmented reality ([\[arstechnica.com/science/2015/07/terminator-vision-and-the-complex-questions-behind-augmented-reality\]\(http://arstechnica.com/science/2015/07/terminator-vision-and-the-complex-questions-behind-augmented-reality\)\).¹³ The author points to many pleasant current uses, such as the first-down overlay on NFL games on TV, or a smartphone app that lets you point your phone at the sky to have it trace the constellations you can see. However, there are also many disturbing or potentially perilous applications of AR.](http://</p>
</div>
<div data-bbox=)

IEEE Spectrum's article on the dangers of augmented reality explains that humans' mental process of sensing the world visually and making decisions based on that input is not something to mess around with lightly (<http://spectrum.ieee.org/consumer-electronics/portable-devices/the-reallife-dangers-of-augmented-reality>).¹⁴ Complicated information-rich visual overlays are particularly hazardous when people need to react physically and quickly to events to remain safe. The author also warns us of a "hugely annoying future" of targeted advertising on every surface around us: "a dystopian future in which we all stumble around bathed in AR ads."

SEEING THE FUTURE

Fortunately, there are also much more attractive views of our future, courtesy of new displays and more benign virtual and augmented reality systems.

Tents of the Future

Researchers at Brown University have taken your basic yurt in a whole new direction. The interior surfaces (domed ceiling, curved walls, and floor) of their new \$2.5 million immersive 3D virtual reality space are all displays—adding up to about 100 million pixels projected by 69 stereo projectors (see Figure 3a). Users don 3D glasses and employ their head tracking functionality as well as a wand to control the system (see Figure 3b). A *Boston Globe* article describes a series of amazing visual experiences, including moving along the surface of the moon, viewing a 260-foot-long antique scroll, and participating in students' video games

NOTES FROM THE COMMUNITY

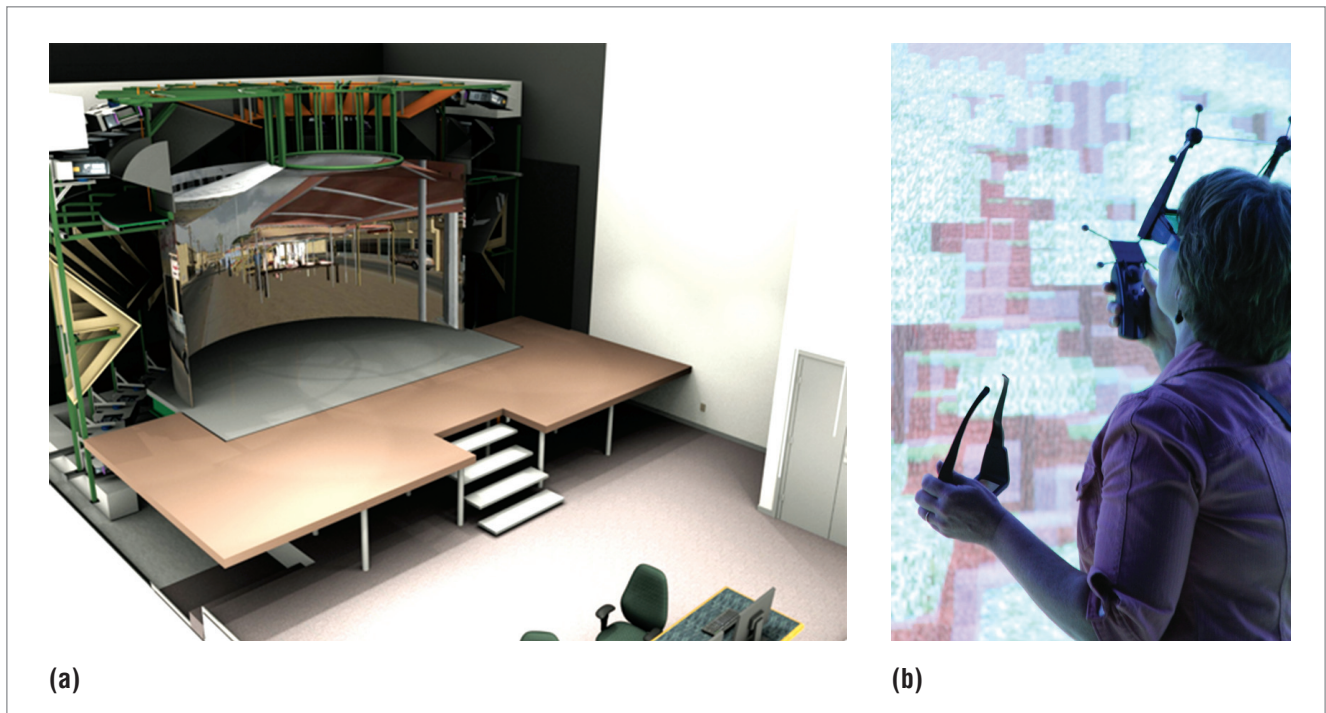


Figure 3. Brown University's YURT (*y-shaped ultimate reality theatre*): (a) The domed ceiling, curved walls, and floor are all displays in this new immersive 3D virtual reality space, where (b) users wear 3D glasses with head-tracking functionality and use a wand to control the system. (Source: Brown University Department of Computer Science; used with permission.)

and 3D poetry (www.bostonglobe.com/lifestyle/style/2015/06/19/brown-university-unveils-virtual-reality-room/QoTO-Op66NpPZeGMF0bapjO/story.html).¹⁵

The article also compares different types of virtual reality—head-mounted displays that block out actual reality, and “caves” like Brown's YURT (a *y-shaped ultimate reality theatre*) that let users see their own bodies but immersed in a different reality. Both types have their different uses but are also vastly different in cost, as spaces such as the YURT require “unbelievable” amounts of money, while head-mounted displays can be consumer devices. Researchers anticipate many experimental and scientific uses for the YURT, including space-mission planning and astronaut training.

Displaying the Invisible


What would your screen tell your camera if it could talk? Dartmouth College research, recently presented at MobiSys 2015, describes a new way for a

screen to communicate with a camera without disrupting displayed images with QR codes or other human-visible information (<https://now.dartmouth.edu/2015/05/researchers-create-new-form-smart-device-communication>).¹⁶ Instead of changing RGB values or otherwise interfering with existing content image layers, HiLight encodes data using pixel translucency changes in a separate (by default transparent) image layer. The pixel translucency change is only perceivable by cameras, not human eyes. HiLight provides one-way real-time communication from off-the-shelf displays to off-the-shelf cameras such as those on smartphones or smart glasses. HiLight thus provides a way to include context-dependent or personalized data alongside the images on the screen.

Through the Looking Glass

In contrast to invisible content on visible displays, see-through displays offer visible content on invisible displays.

Transparent displays and augmented mirrors have been around for a while, with many groups trying out different approaches. MIT researchers, for example, have been working on embedding light-reflecting silver nanoparticles in transparent material to avoid the need for transparency-blocking electronics in the display material (www.gizmag.com/mit-transparent-display-nanoparticles/30549).¹⁷

This quarter, a reader contributed a link about Samsung recently showcasing a 55-inch transparent OLED display combined with Intel's RealSense 3D camera-based gesture sensing (www.mirror.co.uk/news/technology-science/technology/samsung-makes-see-through-computer-screens-5861734).¹⁸ In addition, Samsung has released a display that functions as a mirror that can also present information over the reflection. Some of us feel that tidying up our own images is an excellent application of augmented unreality. 

REFERENCES

1. "Zebra MotionWorks Sports Solution," Zebra Technologies, 2013; www.zebra.com/content/dam/zebra/product-information/en-us/brochures-datasheets/location-solutions/motionworks-data-sheet-en-us.pdf.
2. K. Vanhemert, "Somehow Teen Girls Get the Coolest Wearable Out There," *Wired*, 22 July 2015; www.wired.com/2015/07/somehow-teen-girls-get-coolest-wearable.
3. E. Mack, "This Health-Tracking Device Sniffs Your Farts," *CNET*, 1 May 2014; www.cnet.com/news/this-health-tracking-device-sniffs-your-farts-ch4.
4. B. Dzenis, "PennApps Fall 2011: Hacked Microwave-Driven Video Player Wins \$2,500," *Technical.ly*, 21 Sept. 2011; <http://technical.ly/philly/2011/09/21/pennapps-fall-2011-hacked-microwave-driven-video-player-wins-2500>.
5. "Internet of Things Security Study: Smartwatches," HP, 20 July 2015; http://go.saas.hp.com/l/28912/2015-07-20/3251bm/28912/69038/IoT_Research_Series_Smartwatches.pdf.
6. A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, 21 July 2015; www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.
7. A. Greenberg, "Hackers Cut a Corvette's Brakes Via a Common Car Gadget," *Wired*, 11 Aug. 2015; www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget.
8. S. Gallagher, "Highway to Hack: Why We're Just at the Beginning of the Auto-Hacking Era," *Ars Technica*, 23 Aug. 2015; <http://arstechnica.com/security/2015/08/highway-to-hack-why-were-just-at-the-beginning-of-the-auto-hacking-era>.
9. J. Vincent, "Watch this Apparently Legal Drone Fire a Handgun," *The Verge*, 16 July 2015; www.theverge.com/2015/7/16/8976337/drones-quadcopters-handguns-legal.
10. Z. Canepari and D. Cooper, "The People Trying to Save their Robot Dogs from Extinction," *The New York Times*, 17 June 2015; www.nytimes.com/video/technology/100000003746796/the-family-dog.html?src=vidm.
11. I. Bogost, "The Internet of Things You Don't Really Need," *The Atlantic*, 23 June 2015; www.theatlantic.com/technology/archive/2015/06/the-internet-of-things-you-dont-really-need/396485.
12. A. Zaleski, "NoFlyZone, a 'Do Not Call' List for Drones," *Fortune*, 18 Feb. 2015; <http://fortune.com/2015/02/18/noflyzone-do-not-call-list-drones>.
13. L. Hutchinson, "Terminator-Vision and the Complex Questions Behind 'Augmented Reality,'" *Ars Technica*, 6 July 2015; <http://arstechnica.com/science/2015/07/terminator-vision-and-the-complex-questions-behind-augmented-reality>.
14. E.E. Sabelman and R. Lam, "The Real-Life Dangers of Augmented Reality," *IEEE Spectrum*, 23 June 2015; <http://spectrum.ieee.org/consumer-electronics/portable-devices/the-reallife-dangers-of-augmented-reality>.
15. A. Katz, "Brown University Unveils Virtual Reality Room," *The Boston Globe*, 20 June 2015; www.bostonglobe.com/lifestyle/style/2015/06/19/brown-university-unveils-virtual-reality-room/QoTOOp66NpPZcGMF-0bapjO/story.html.
16. J. Cramer, "Researchers Create New Form of Smart Device Communication," *Dartmouth Now*, 18 May 2015; <https://now.dartmouth.edu/2015/05/researchers-create-new-form-smart-device-communication>.
17. D. Quick, "MIT Researchers Clarify Things with New Transparent Display Technology," *Gizmag*, 21 Jan. 2014; www.gizmag.com/mit-transparent-display-nanoparticles/30549.
18. O. Solon, "Samsung Makes See-Through Computer Screens that Interact with the Viewer," *The Mirror*, 11 June 2015; www.mirror.co.uk/news/technology-science/technology/samsung-makes-see-through-computer-screens-5861734.

Mary Baker is a senior research scientist at HP Labs. Contact her at mgbaker@hp.com.

Justin Manweiler is a researcher at the IBM T.J. Watson Research Center. Contact him at jmanweiler@us.ibm.com.



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.



How to Reach Us

Writers

For detailed information on submitting articles, write for our Editorial Guidelines (pervasive@computer.org) or access www.computer.org/pervasive/author.htm.

Letters to the Editor

Send letters to

Brian Kirk, Lead Editor
IEEE Pervasive Computing
 10662 Los Vaqueros Circle
 Los Alamitos, CA 90720
pervasive@computer.org

Please provide an email address or daytime phone number with your letter.

On the Web

Access www.computer.org/pervasive for information about *IEEE Pervasive Computing*.

Subscription Change of Address

Send change-of-address requests for magazine subscriptions to address.change@ieee.org. Be sure to specify *IEEE Pervasive Computing*.

Membership Change of Address

Send change-of-address requests for the membership directory to directory.updates@computer.org.

Missing or Damaged Copies

If you are missing an issue or you received a damaged copy, contact membership@computer.org.

Reprints of Articles

For price information or to order reprints, send email to pervasive@computer.org or fax +1 714 821 4010.

Reprint Permission

To obtain permission to reprint an article, contact William Hagen, IEEE Copyrights and Trademarks Manager, at copyrights@ieee.org.