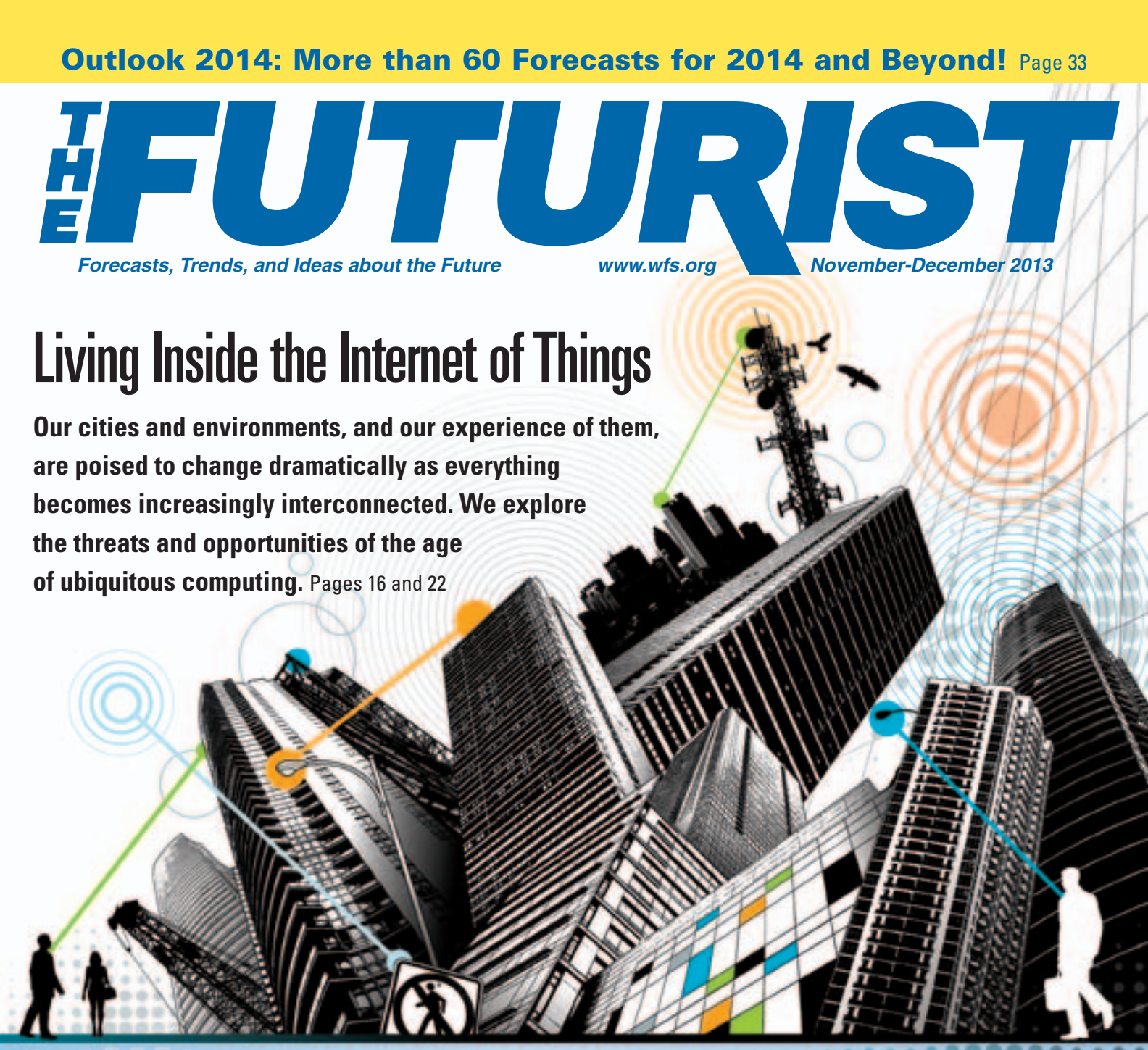
Outlook 2014: More than 60 Forecasts for 2014 and Beyond! Page 33

THE FUTURIST

Forecasts, Trends, and Ideas about the Future *www.wfs.org* *November-December 2013*

Living Inside the Internet of Things

Our cities and environments, and our experience of them, are poised to change dramatically as everything becomes increasingly interconnected. We explore the threats and opportunities of the age of ubiquitous computing. Pages 16 and 22



Governments Confront Their Pension Deficit Disorder, page 28

Game Plan for a Future-Ready Workforce, page 43

Futurists Explore the Next Horizon, page 47

Evolution or Extinction? Humanity's Future Legacy, page 64

PLUS: WORLD TRENDS & FORECASTS

When the Bots Can Read Your E-mail, page 8

How the Brain Grieves Lost Futures, page 10

Impacts of Humanity's Madding Crowds, page 12

Connecting with Our Connected World

We can only really communicate with a tiny fraction of our personal and global environment. But our world and our experience of it are poised to change dramatically as everything becomes increasingly interconnected. Here's what we can expect in the coming era of the "Internet of Things."

By Richard Yonck

Whether it's biological cells, electronic systems, or communities of people, networks increase in value as the number of nodes and connections grow. As Metcalfe's law suggests, increased connectedness can lead to increased value and usefulness.

For many millennia, our ability to communicate was limited to those people with whom we could physically meet and interact. Writing and the ability to create records transcended this limitation, allowing us to communicate with others separated from us by physical space and even time. With the telegraph and telephone, near real-time two-way communication with nearly anyone, anywhere on the planet, became possible.

Our growing interconnectivity has allowed us to share knowledge and ideas, which in turn has advanced society even further. But it was the development of the Internet that really accelerated this process.

Perhaps equally important, our inventions made it possible to improve our communication with the physical world in the form of remote sensors and other telemetry. As computers process more input from satellites, sensors, radio-tagged devices, and so on, it's been estimated more than 40% of all data will be entirely machine-generated by 2020; that is up from 11% in 2005, according to the 2012 IDC Digital Universe report. This trend will likely continue for some time.

With ever more devices coming online, people will become less directly involved in the vast majority of communications. Information will be exchanged solely by devices in what's referred to as M2M or machine-to-machine communication. In certain respects, this is just as well, since much of this data will be transferred and acted upon at speeds many orders of magnitude faster than human thought.

Such increased connectivity will undoubtedly have unintended consequences and repercussions. Our challenge will be to maintain control of something that we haven't directly created ourselves, that makes the world run faster, and that is even more intricately connected than our own brains.

Impacts of Increased Connections

Since the 1980s, Internet Protocol version 4 (IPv4) has provided unique numeric addresses for each of the world's Internet-linked devices. This protocol has the potential for 2^{32} or some 4.29 billion addresses—a number that seemed inexhaustible at a time when the Internet was just taking off.

As early as the 1990s, it was already becoming apparent that IPv4's 32-bit address space was going to be inadequate for future growth. So work was begun on what would

eventually become IPv6, a 128-bit protocol. This allows for 2^{128} unique addresses or 340 trillion trillion trillion—28 orders of magnitude greater than IPv4! Even with the explosive growth that will continue with the Internet of Things (IoT), this protocol should be usable for many decades, if not centuries to come.

In the meantime, following the principles stated by Moore's law, computation devices are getting smaller, cheaper, and more powerful. The Michigan Micro Mote, or M^3, for example, is an ultra-low-power prototype designed by researchers at the University of Michigan. Less than a cubic millimeter—about the size of a grain of sand—it includes a processor, data storage, sensors, and wireless communication, and it harvests its power via a solar cell. Though still in the lab, M^3 demonstrates that we're rapidly approaching a new era of computing.

As a result of these advances, we can foresee a day not very many years off when such chips will shrink to the size of a speck of dust. "Smart dust," as it is often called, will follow economies of scale similar to earlier processors, with unit production costs plummeting toward zero.

These tiny circuits will give rise to a world that is connected in ways that would have been difficult to imagine not that many years ago. Everything from roads and bridges to household appliances and food products will soon be able to communicate via the Internet. Information about stresses and deformation will let us anticipate infrastructure failure before it happens. Even hillsides and streams—the natural environment—will be connected. Flow rates and measurements of soil movement will aid us in understanding and protecting our natural resources. Devices in the home will be able to order their own supplies, schedule their own repair, or restock pantries.

All of this will be possible because of increased intelligence combined with increased connectivity.

Coined in 1999, the term *Internet of Things* refers to a world of interconnected physical objects, capable of sharing data about their state or the state of their environment. In a 2012 white paper, Cisco estimated that the

IoT will have a value of $4.4 trillion over the next decade. GE estimates the "industrial Internet" will add up to $15 trillion to global GDP over the next 20 years—approximately equivalent to the current size of the U.S. economy.

Obviously, these are the sort of numbers that attract a lot of attention as well as investment. Cisco is attempting to rebrand the concept as the *Internet of Everything* (IoE). With IPv6 only representing 1% of Internet traffic as of late 2012, there remains an enormous amount of supporting hardware to be sold as we transition to the new protocol.

True two-way connectivity is the goal, but in the meantime, different technologies are being used to close the gap. RFID tags (Radio Frequency IDentification) and QR codes are one approach to making individual items addressable, albeit in a passive, single direction. Ultimately, the optimal method of realizing IoT will be active, two-way communication that uses the Internet, along with an assortment of shorter-range technologies, such as Wi-Fi, ZigBee, and Bluetooth.

"So, what was so important that it took you out of your way that day? The data that the Internet of Things will make available could suddenly provoke many such questions. Who will be asking them?"

Hyperconnectivity's Benefits and Drawbacks

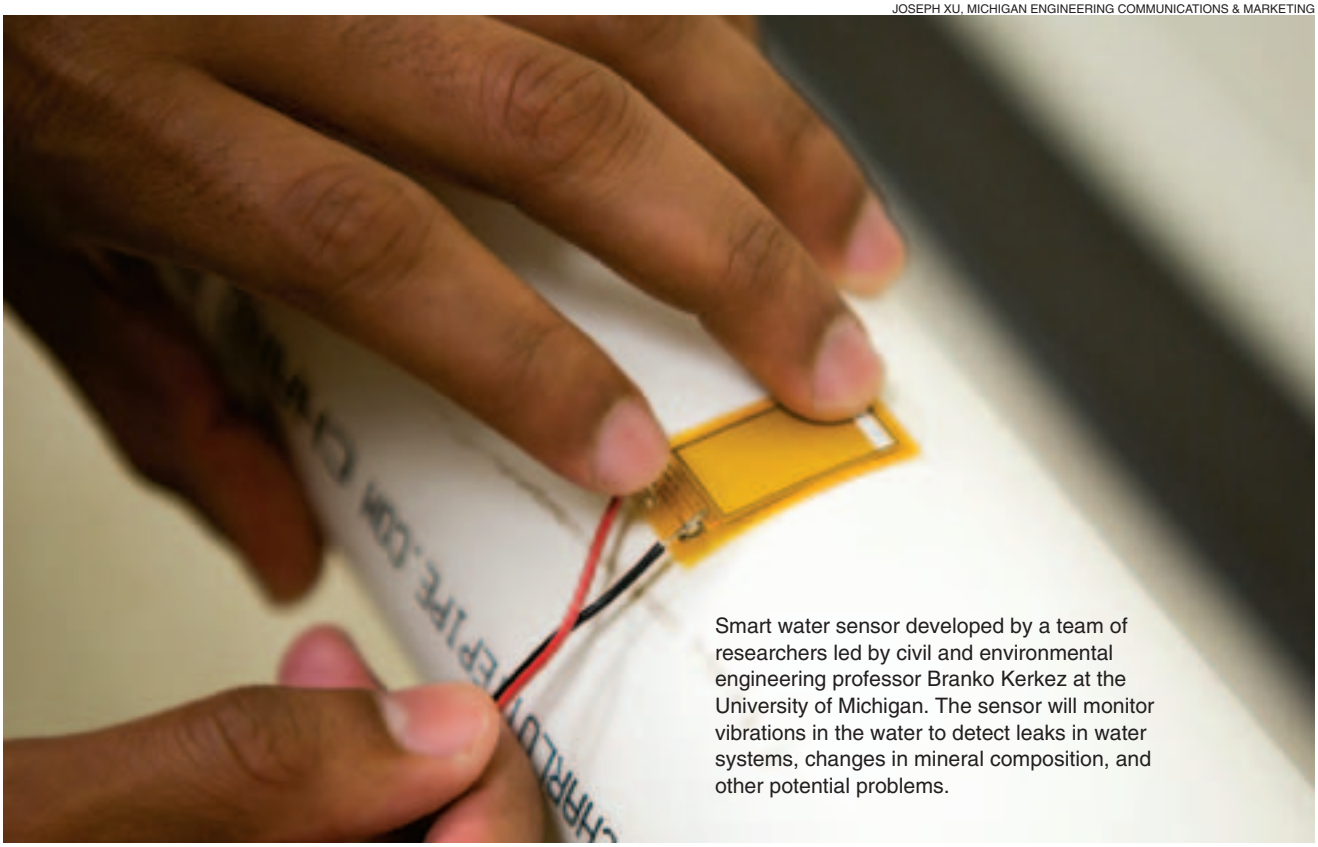
The benefits of the Internet of Things should be obvious to business, government, and individuals alike. The ability to know exactly where a product is in your inventory or supply chain can significantly improve efficiency and lower costs. Additionally, service and warranty issues could be handled much more readily and unintrusively.

On a personal front, individuals would be able to automate all sorts of routine, often mundane tasks, such as reordering supplies and groceries, or being reminded to service an appliance or vehicle, and remotely monitoring our homes. Every possession could be catalogued and instantly locatable. Misplacing your keys would become a thing of the past. The potential applications will be nearly endless.

But as with every new technology, there will be downsides. Security and privacy concerns will initially be among the most prevalent of these. As a growing number of our possessions become accessible via the Internet, the number of potential security holes will grow, as well. For example, you might experience a hacked Internet-connected appliance, such as a refrigerator or toaster oven, that results in unauthorized access to more financially or personally sensitive parts of your network and your life.

Regulation safeguards will also need to keep pace with the changes. Currently, stores track personal shopping habits using loyalty cards, then resell the data to marketers. A recent *Wall Street Journal* article confirms that this same data is now being purchased by insurance companies for the purpose of setting

JOSEPH XU, MICHIGAN ENGINEERING COMMUNICATIONS & MARKETING



Smart water sensor developed by a team of researchers led by civil and environmental engineering professor Branko Kerkez at the University of Michigan. The sensor will monitor vibrations in the water to detect leaks in water systems, changes in mineral composition, and other potential problems.

Scenario: Life with the Internet of Everything

Anya's smart clock woke her gently, the time determined by her sleep phase (as detected by her bed) and coordinated to her morning's schedule. Despite this, as she got up, she realized something wasn't quite right. There was a mild ache in her joints, and her head felt fuzzy.

Bringing up the Web on her nightstand (the nearest surface at hand), Anya quickly checked EpiCast and confirmed her suspicions: An H3N9 flu virus was moving through the city. Pathogen detectors had been tracking its progression for days.

Fortunately, her medicine cabinet spotted the trend nearly 36 hours ago and ordered the genetically targeted medicine for that exact flu bug. It had been delivered last night and was waiting for Anya downstairs. She swallowed two tablets and got ready for work, knowing she'd be feeling her normally healthy self again before she left the house.

On the way to the office, Anya's self-driving Prius navigated traffic as she reviewed a report in preparation for her first meeting. The cars around her maintained tight formation while speeding along at over 100 mph. Lightning-fast response times combined with car-to-car-to-road communication allowed for capacities and speeds far greater than in the dangerous old days when people drove themselves. It was difficult to believe that, at the turn of the century, traffic accidents and fatalities were hundreds of times more frequent than they were today.

Nevertheless, she noted her normally smooth commute was a few minutes slower than usual. Checking the navigation monitor, she saw why: Traffic was being routed away from the old Crosstown Bridge. Earlier that morning, sensors had determined that stress deformation in the structure had finally exceeded federal standards. Well, better a couple extra minutes in traffic than to be caught on a collapsing bridge.

At the last minute, Anya decided to make a quick detour to pick up some office treats from the new 3-D gastroprint chocolatier everyone had been raving about. Anyone could print their food these days, but these people were artisans. She paid for the confections with a swipe of her index finger, the minuscule chip embedded beneath her skin effortlessly debiting her bank account.

Nine minutes later, Anya arrived at her office building. As she passed through the scanners and checkpoints, she was quietly taken aside for secondary questioning. Obviously, her detour had fallen enough outside her typical routine to trip one of the security algorithms. It was an inconvenience, but given the amount of crime and terrorist activity in the world, it seemed like a small price to pay.

—Richard Yonck

premiums and investigating claims. In a world of total connectivity, the rate at which a household consumes sugar, salt, tobacco, and alcohol would potentially be an open book to insurers seeking to control costs. Without adequate changes to consumer-protection laws, the IoT's impact on personal liberty and privacy will be significant.

Of course, individuals could opt to keep much of their life disconnected and off the grid, so to speak. But if this choice results in less profit for retailers, they are likely to charge a higher price, just as they currently do for those customers not using loyalty cards. Such costs will create an incentive for consumers to participate in this hyperconnectivity.

Privacy issues in such a truly connected world go far deeper than that, however. Objects with embedded intelligence would collect the digital traces of people interacting with smart environments; this information might be used to extract patterns of individual and group behavior:

- You routinely pass over a particular bridge every Tuesday.
- You enter a certain building between 2:00 and 3:00 p.m. with significant regularity.
- Despite opting out of a store's loyalty program, the timestamp on your credit-card transaction corresponded with those of several items as they were subtracted from the store's inventory.
- The smartcup containing your daily cappuccino with an extra shot of espresso (which you purchased with your smartphone coffee app) was tossed into a garbage can three blocks off of your usual route back to the office.

So, what was so important that it took you out of your way that day?

The data that the Internet of Things will make available could suddenly provoke many such questions. Who will be asking them?

The information that "big data" analysis provides and the detailed profiles that could be created from it are unprecedented in all of history. People are unlikely to accept such developments without at least some resistance. Individuals and groups could implement hacks, flash mobs,

and other activities just to generate false or misleading data that interferes with such analysis. Of course, measures would be taken to account for such disinformation-generating efforts.

The detail and granularity of the information that could be harvested from a smart environment will make Facebook's privacy settings seem like Fort Knox by comparison. Because there will be so much data generated, it makes statistical analysis increasingly accurate, both for individuals as well as in the aggregate. Automated forms of data mining will be able to ascertain everything from epidemiological information to commuter transit patterns to personal sex habits. Nothing will be exempt, sacred, or ignored, because all of it will ultimately have commercial value.

It's this potential value that makes all this data so attractive and, at the same time, so threatening. At one level, it's a pragmatic, socially useful technology: Corporate and personal efficiency will be increased and productivity enhanced. But in the end, all this data can also be utilized for other purposes. Ultra-personalized marketing, indirect surveillance, and even pre-crime forecasting all become possibilities.

This last is, of course, a reference to the film *Minority Report*, which was based on a Philip K. Dick novel. While the premise of this story relies on "precogs," a trio of precognitive operatives, much the same role could be performed by highly granular surveillance, combined with data mining and statistical analysis.

Anticipating the Unintended Consequences

As a general rule, the more complex something is, the more opportunity there is for it to operate in a manner other than we intended or expected. The more connected our world becomes, the greater the potential for all these sensors and devices to communicate in unforeseen ways, leading to unanticipated interactions and behaviors. Without adequate safeguards, it's entirely feasible that a series of unrelated events beginning from something innocuous could trigger a major incident—even an infrastructure shutdown.

An example of this is the Northeast blackout of 2003, which knocked out power to 55 million people in the United States and Canada. In this instance, unpruned trees coming in contact with overloaded transmission lines caused a transient current increase. A cascading failure occurred when software didn't properly redistribute the load but instead shut down power in succeeding areas, propagating the disturbance across the network.

As our systems begin communicating with each other in new ways, mostly without human oversight, the opportunity for such disturbances will grow.

Metcalfe's law states that networks increase in value as they grow. One outgrowth of this principle is that aggregations of cells in an organism can acquire capabilities beyond those of its individual cells. For instance, a single neuron is basically a chain of electrochemical potentiations. Networked together, these same cells may form a brain, along with its emergent property of mind.

Similarly, large groups of individuals form societies, along with all their attendant behaviors, communications, and institutions. This is not to say that we aggregate into a "group mind," though as our communications become more continuous and interconnected, some similarities will appear. However, in both brain formation and society formation, the process of aggregation results in emergent properties that couldn't be fully predicted based solely on their constituent parts, whether cells or individuals.

The IoT could manifest similar complexities in response to the growing connectedness of its components. While it's unlikely that the network will simply wake up one day as a functioning, conscious mind, there's a significant possibility that it will perform actions, even exhibit behaviors, that are different from those for which it was originally designed.

This is the nature of complexity. Once a system reaches a particular threshold of complexity, we can no longer be certain about specific cause-and-effect relationships; rather, we must think in terms of probabilities. Instead of being 100% certain that A will lead to B, we might assign a likelihood of, say, 99.98%.

For some events, this probabilistic approach works fine, but for others it could be disastrous: Power plants, automated weapons systems, and freeways full of self-driving cars all could experience catastrophes if operating on erroneous information. So these and other systems will need to be designed with greater safeguards and redundancies than they have today.

Of course, these scenarios assume that the network has no volition. That could change. Over time, as the relative intelligence of individual components is upgraded and the methods of intercommunication increase in complexity, something akin to a mind or minds could emerge.

These wouldn't resemble any bio-

Data and Determinism

With hyperconnectivity and big data come the possibility of *anticipatory analysis*, à la *Minority Report*. This moves us to the borderland between free will and determinism. What happens when nearly all of our actions can be predicted with near-perfect accuracy? For one thing, it could make us question what it means to be human.

The matter of determinism has been argued by philosophers for millennia. Do we as humans have free will, or are we merely cogs on a great wheel of the universe, our every action already set in motion from the first flicker of the Big Bang?

The irony will be if we have had free will all along and it's only at this stage in our progress—at this cusp of our evolutionary and technological development—that we end up stripping it from ourselves.

—*Richard Yonck*

VIDEO SCREEN CAPTURES VIA CISCO TECHNOLOGY NEWS SITE, NEWSROOM.CISCO.COM

Left: Cisco Chairman and CEO John Chambers (right) and Chief Demonstration Officer Jim Grubb demonstrate the principles of the "Internet of Everything," or machine-to-machine communication, in an agricultural setting. Sensors could be tilled directly into the soil of a cornfield, for instance (below). When one part of the field finds itself in favorable conditions, the sensors could order the irrigation system to be activated.

logical mind that has ever existed, but in some ways that would make them potentially even more problematic. A system that set its own priorities based on its own motivations would be worse than useless if not harnessed and properly directed. Such a situation might be analogous to working with a domesticated animal. We can train a horse and even make some assumptions about its motivations, but in the end, if it insists on heading down one path when we need to take another, we're left with little choice but to dismount.

Whether or not such behavior should ever become an issue with our connected technologies remains to be seen, but it is prudent to anticipate unintended performance.

Rather than thinking of these unexpected behaviors as malfunctions, we should view them as the results of complex interactions that we have yet to understand. This is often what happens with software. As programs grow to hundreds of thousands, even millions, of lines of code, unanticipated values are passed and stored, and logic takes paths that were never intended. The result may be incorrect output, or the program crashes, or even the entire system halts.

Software developers perform considerable testing and debugging to ensure that such occurrences are kept to a minimum, but this simply won't be possible in a vast ad hoc network with uncounted interconnected sensors. The future Internet of Things (or Internet of Everything) will demand entirely new approaches to exception and fault handling to ensure the continued, healthy operation of our infrastructure.

Our world today is more connected than it has ever been, but a bare fraction of how connected it will become. As nearly every object in our personal, professional, and external worlds becomes addressable and programmable, much will change. We will change.

The Internet of Things will increase knowledge of our environment, bringing with it new functionality and efficiency. But it also holds the potential for new security holes, invasions of privacy, and possibly even a challenge to our sense of what it means to be human. The goal now is to ensure that these changes actually improve our lives. ❑

About the Author
Richard Yonck is a foresight analyst for Intelligent Future LLC in Seattle and is the Computing/AI contributing editor for THE FUTURIST. His article "Are You Smarter Than a Sixth-Generation Computer?" appeared in the September-October 2012 issue.