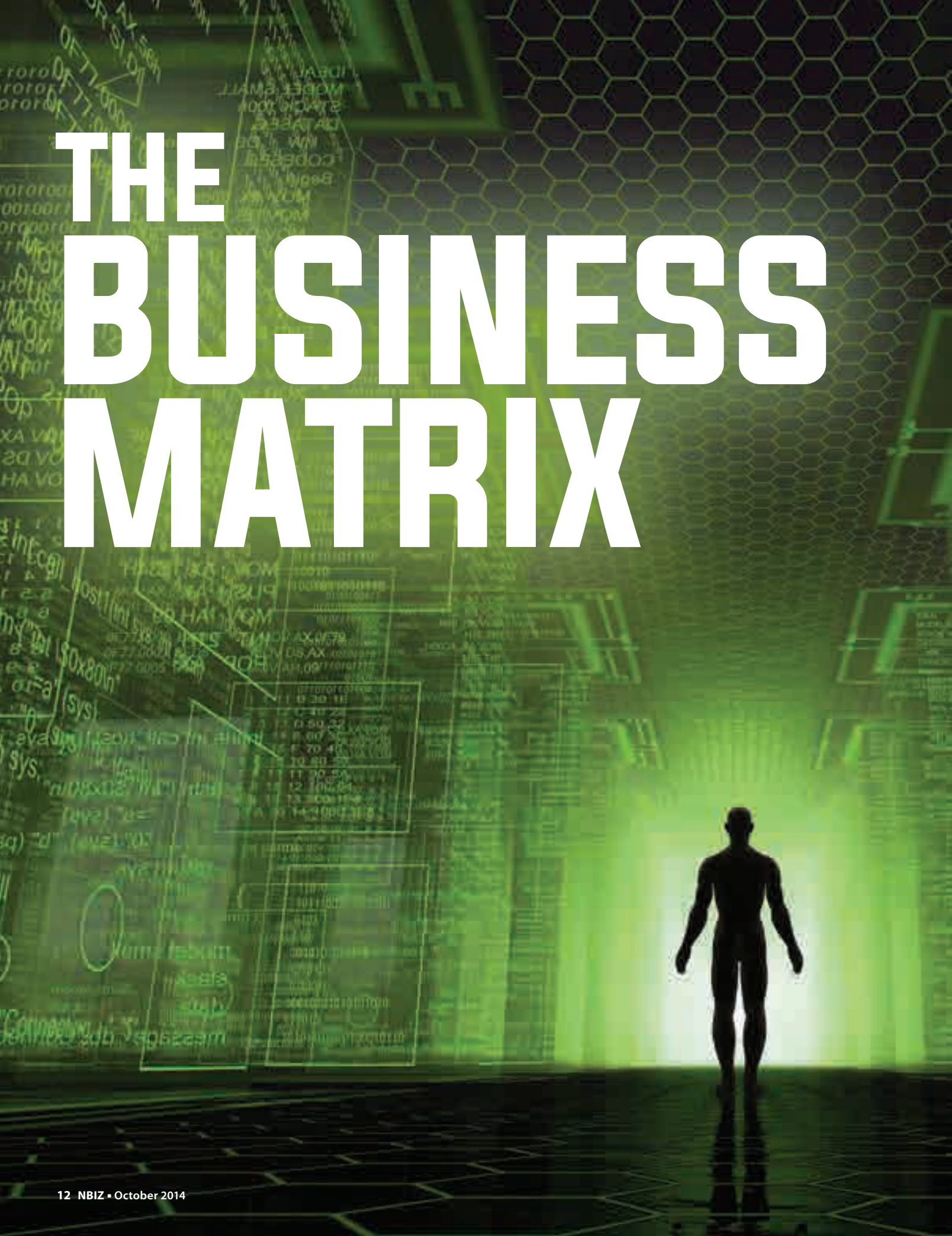
THE BUSINESS MATRIX



Science Fiction Becomes Reality

By Troy Anderson

In the Academy Award-winning film *The Matrix*, Thomas Anderson, played by actor Keanu Reeves, discovers that the world he thought was real is actually an illusion—a simulated reality created by an artificial intelligence system known as the "The Matrix." In this dystopian, future world, highly-advanced computers have tapped into people's brains and created an alternate reality in order to use their bodies' heat and electricity for energy. While *The Matrix* is a fictional film, Google's director of engineering, Ray Kurzweil, a futurologist and author of the *New York Times* bestseller *The Singularity Is Near*, recently announced that he expects computers to outsmart their makers by 2029.

"Ray Kurzweil said that by 2029, that they would fuse human minds with machines," says John W. Whitehead, a constitutional attorney and founder of The Rutherford Institute, a nonprofit civil liberties organization based in Charlottesville, Virginia. "If you've seen the movie *The Matrix*, that's where we're moving."

Once Science Fiction—Now Reality

Once the subject of science fiction novels and blockbuster films, new technologies such as biometrics, radio frequency identification (RFID), and even microchip implants are rapidly changing the world we live in, and a growing number of businesses are adopting these new technologies.

"These technologies, biometrics, smartcards and RFID chips, and their underlying technologies have all started to mature," says Stuart Lipoff, vice president for publications and a fellow at the Institute of Electrical and Electronics Engineers, a Parsippany, New Jersey-based global professional organization dedicated to advancing technology for the benefit of humanity. "These technologies have only started to get to the point where they are very reliable, work well with batteries, and can be incorporated into tiny devices like cell phones. As there are more and more instances of identity theft and fraud and we are doing more and more things with our cell phones, there is a reason why these new technologies are becoming more popular."

At one point, the Lone Star State, home to Texas Instruments, a Dallas-based company that designs and makes semiconductors, was a "hotbed for RFID development," says Mark Roberti, founder and editor of the *RFID Journal* in Hauppauge, New York. "That's probably a little less true now because Walmart sort of backed off their efforts a little bit," he says, "but companies in Texas are using these technologies just like everybody else."

Biometric Technologies Emerge in Business World

A number of businesses, including Six Flags Over Texas in Arlington, are using or are in the process of rolling out biometric scan systems. These biometric technologies use thumbprints and face recognition and have been utilized by the military and government for years. They are increasingly being employed in the business world. The new iPhones use these technologies as well as a few retailers whose workers log into their computers by fingerprint. Biometric technology, including fingerprint and retina recognition, are considered a more convenient and secure method of authenticating identity. Banks, government agencies, credit card companies, and mobile phone manufacturers are exploring biometrics and similar technologies.

"Some companies are adopting biometrics. The list is getting bigger by the day," says Keith Palmgren, an instructor at the SANS Institute, a cooperative research and education organization that is the largest source for world-class information security training and security certification. Palmgren is also the president of NetIP, Inc. in San Antonio. "The point will come when you are going to walk into Walmart, and when you are going through the checkout counter, you'll simply put your finger on the [biometric reader] to pay. That kind of thing is increasing. Disney was one of the earlier adopters of this kind of thing, along with some of the other amusement parks."

Barclays Leads the Way in Biometric Readers

In September, Barclays announced that it will become the first major bank in the western world to use biometric readers to allow customers to easily access their online accounts and authorize payments. This will all be done within seconds but without the need for PINs, passwords, or authentication codes. According to Barclays, the combination of vein biometrics and highly secure digital signature technologies in their biometric reader is "a first for the global financial sector." The device can read and verify a user's unique vein patterns in the finger. Unlike fingerprints, vein patterns are extremely difficult to spoof or replicate.

"This solution is at the leading edge of innovation and is in direct response to client concerns about the threat of online fraud while making our clients' lives easier through its convenience," Ashok Vaswani, chief executive officer of Barclays Personal and Corporate Banking, said in a prepared release. Proponents of these technologies say that they are designed to fight fraud and identity theft and to increase security, productivity, and profits for businesses.

Paul Donfried, the chief technology officer at Washington, D.C.-based LaserLock Technologies, a leader in protecting companies, industries, governments, and individuals from the rising threat of counterfeiting and fraud says business is booming. "Fortunately for us, but unfortunately for the general public, counterfeiting and fraud are increasing at alarming rates to the point where this year, it's estimated that about five percent of the global gross domestic product will be lost to counterfeiting and fraud," Donfried says. "That's close to $2 trillion."

Donfried also notes, "On the digital side, it's hardly a day that passes where we don't learn about yet another cyber-security attack that has been successful. The most recent one was at Home Depot, and prior to that, Target was a high-profile one...we saw an attack on Apple that revealed salacious photographs of a bunch of well-known personalities. The good news is that as it becomes more widespread and a global problem, that it's causing a lot of companies to look for more effective ways to combat this kind of fraud and protect customers and their core business."

Barclays isn't the only company moving into biometric identification. Giant online Chinese retailing firm Alibaba also plans to start using fingerprint scanning in an effort to make transactions more secure. The company is integrating fingerprint scanning into its Alipay Wallet app. Motorola has developed a "digital tattoo" to help ensure that only the owner can unlock its phones.

"Made of super thin, flexible materials based on VivaLnk's eSkin™ technology, each digital tattoo is designed to unlock your phone with just a touch of your Moto X to the tattoo, no passwords required," according to a Motorola statement. "The nickel-sized tattoo is adhesive, lasts for five days, and is made to stay on through showering, swimming, and vigorous activities like jogging. And it's beautiful, with a shimmering, intricate design. It's another step in making it easier to unlock your phone on the go and keep your personal information safe."

Thomas Way, an associate professor of computing sciences at Villanova University in Philadelphia says people are overwhelmed by the sheer number of user names and passwords they are required to remember to navigate in today's digital world. He describes this as the "tyranny of the password."

"Our online existence is being overwhelmed by the need to have all these different passwords to login with," Way says. "That has led us to come up with shortcuts, so it's pretty typical nowadays to keep a file on your computer that stores all your passwords. But this solution leaves us open to someone who might be an adept computer hacker who is able to gather up this treasure trove of passwords and use them in nefarious ways.

"There are at least 7 billion passwords out there encoded on people's fingers. So biometrics should work. It used to be that fingerprint readers were pretty expensive, but we're now at the point where we can incorporate them into cell phones and laptops and at grocery stores. The technology has become cheap enough that it can be everywhere."

Clayton Locke, the chief technology officer at Intelligent Environments, an international provider of innovative mobile and online solutions for financial service organizations based in Kingston upon the Thames in the United Kingdom, says the use of biometrics is relatively new, but their research shows a growing appetite. Eight in 10 British consumers have said they're ready to ditch their passwords in favor of biometric security measures, while 53 percent of British banking customers said they want their banks to integrate fingerprint scanners into their digital banking services.

Locke says these technologies are changing the banking experience for customers. For instance, biometric measures such as voice verification technology can make banking services easier and more convenient for customers. USAA Bank has started incorporating voice commands into its mobile banking app, allowing users to pay bills, make transfers, and check their balance simply by talking to the system, simplifying the process of managing finances while on the go.

"The possibilities here are endless," Locke says. "Consumers could check how much they have spent on groceries in the last month while in the supermarket simply by asking their smartphone, allowing them to make more informed shopping decisions."

BIOMETRICS ARE BEST REGARDED AS AN EXTRA LAYER OF AUTHENTICATION TO BE USED ALONGSIDE OTHER SECURITY MEASURES RATHER THAN AS A SILVER BULLET ON THEIR OWN.

BIOMETRICS SECURITY ISSUES

Although biometrics offer security and other benefits, there still are concerns. For example, hackers may find a way to steal biometric files. For fingerprint scanning to work, the computer has to have a biometric file on record that it compares with the user's scanned fingerprint. This operates like a password: when a user enters his or her password, the computer keeps it on file for later comparison.

"If someone hacks your password, you can change it," Locke says. "If someone hacks your biometric file, you can't change your fingerprints. Biometrics are best regarded as an extra layer of authentication to be used alongside other security measures rather than as a silver bullet on their own. They should be part of a progressive security framework where the levels of security required increase as the sensitivity of the information being accessed increases."

RFID TECHNOLOGIES GROWTH

In addition to biometrics, a growing number of companies are using Radio Frequency Identification (RFID) chips and tags. RFID chips are about the size of a grain of rice and include a microchip with an

antenna that transmits information about an individual to a reader via radio waves. "One of the hottest areas right now in using RFID is to track apparel items in retail," Roberti says. "Apparel stores have a really hard time managing complex inventories. When you think about how a polo shirt may come in five or six sizes and as many as 10 colors, that's 50 or 60 stocking units. You need to make sure you have the right amount of each of those 60 units. It's very difficult to do. You'll know what I mean if you've ever gone into an apparel store and it seems they have every size except yours."

Roberti says RFID technologies can help businesses with extensive inventories save a great deal of money. RFID tags allow retailers to identify items, pallets, and cases in a similar way that barcodes do but wirelessly. "With RFID, you can take the inventory of an entire store with 10,000 items in an hour," Roberti says. "With barcodes, that would take two people two days. So you can use RFID and increase your inventory accuracy from 65 percent today up to 95 percent easily, and, if you work at it, up to 99.99 percent if you really want. This boosts sales and profit margins for retailers."

FOR SOLDIERS AND JOURNALISTS IN WAR ZONES, AN IMPLANT COULD BE THE DIFFERENCE BETWEEN LIFE AND DEATH. A TRACKER COULD ALSO HELP LAW ENFORCEMENT QUICKLY LOCATE A KIDNAPPED CHILD.

Many companies, including ones in the oil and gas sector, also use RFID technologies for evacuation purposes. "You have an oil refinery where it's a dangerous environment," Roberti says. "If there is an incident, you need to get everyone out. How do you know if you got everyone out? If you didn't get everyone out, how do you know where someone is in the facility? There is a battery-powered system employees wear as an ID-badge, and it lets you locate them and lets you know when they got out and didn't get out."

Implantable Microchips

Among these new technologies, implantable microchips have raised the most concerns. In a recent FoxNews.com article, "Is There a Microchip Implant in Your Future?" John Brandon wrote that these microchip implants offer a number of benefits, allowing people to easily pass through a security checkpoint, buy groceries at a supermarket, or "if you are kidnapped in a foreign country, for example, it could save your life."

"Microchip implants like the ones pet owners use to track their dogs and cats could become commonplace in humans in the next decade," Brandon notes in the article. "Experts are divided on whether they're appropriate for people, but the implants could offer several advantages. For soldiers and journalists in war zones, an implant could be the difference between life

and death. A tracker could also help law enforcement quickly locate a kidnapped child."

Amy Zalman, the chief executive officer at the Washington, D.C.-based World Future Society, the largest and oldest membership organization in the world for futurists, observes that "these technologies are clearly afoot."

"Futurists are watching a trend in which chips move ever close to us: from our clothing into our phones and, ultimately, into our bodies," Zalman says. "The World Future Society prides itself on its neutrality, so we would not take a position on whether this is good or bad. We will ask what this trend and these technologies mean for human society. There will be questions about technology, ethics, surveillance, privacy, and our public selves. These technologies are going to raise deep questions about who we are and what it means to be human."

Electronic Privacy Bill of Rights

In an effort to address some of these concerns, Whitehead has proposed an electronic privacy bill of rights to Congress. "The problem with the chips is how much access the government will have to them," Whitehead says. "The Fourth Amendment says before you do surveillance that you need probable cause. If you are going to search somebody through a chip, you need to get a warrant to have it done. But I think the future is chips, manipulated from a distance. Unless we get some protection from lawmakers, it will be very difficult to operate in society without someone knowing where you are."

Palmgren claims he doubts most people will "stand for it," though some people may decide to have implantable chips. "That is very intrusive," Palmgren says. "Just look at what the privacy advocates are saying. I think they would have a field day with this, and they would have a valid point. I don't want one embedded in me. If you look at the uproar over monitoring that is reportedly being done by the NSA, if you look at the Edward Snowden leaks, and then you turn around and say you are going to put a chip in people and track them 24 hours a day, seven days a week and monitor everything they are doing, I don't think they are going to swallow that. I like my privacy. I'm not a huge privacy advocate, but even I'm not going along with that one." **N**

An award-winning journalist at the Los Angeles Daily News, *the* Press-Enterprise, *and other newspapers for 20 years, Troy Anderson writes for* Reuters, Newsmax, Christianity Today, Bankrate Insurance, *and many other magazines and online publications. He lives in southern California. For more information, visit www.troyandersonwriter.com.*