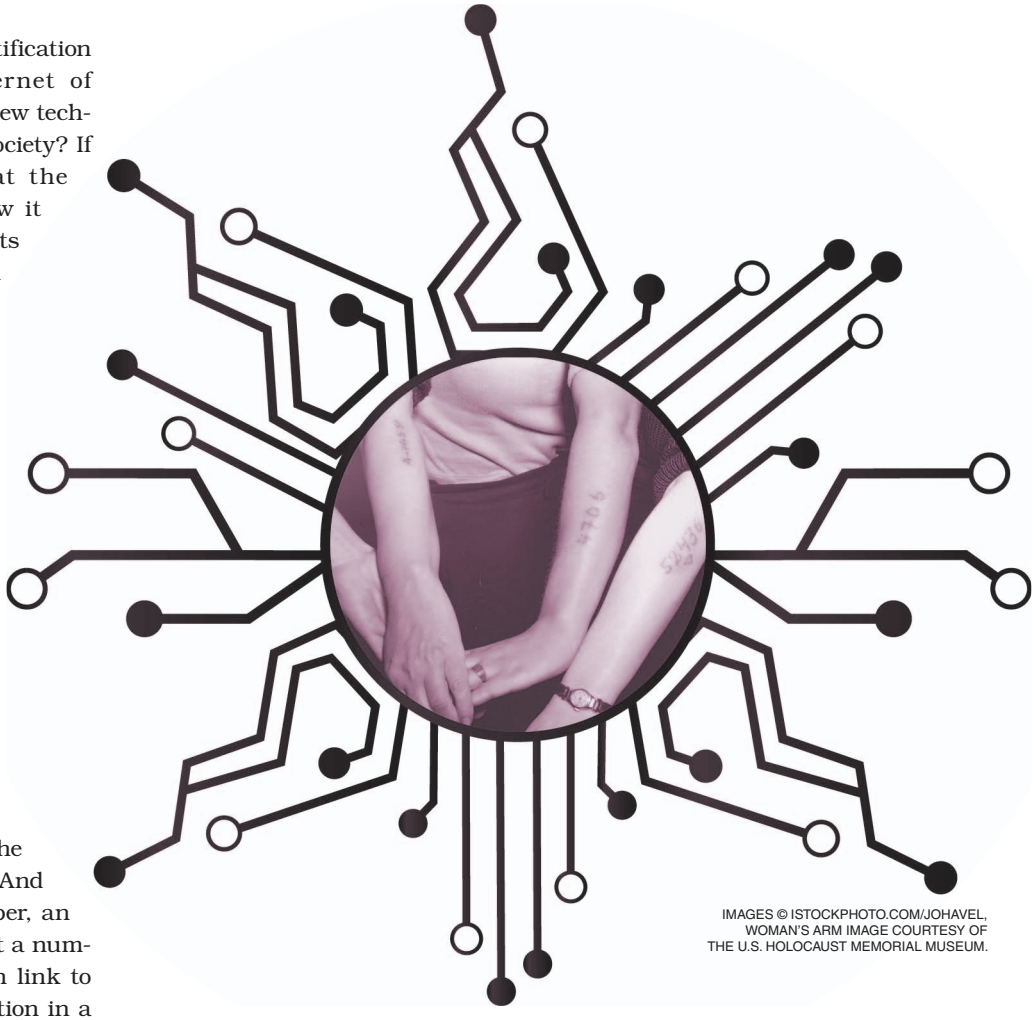
RFID: Helpful new technology or threat to privacy and civil liberties?

Liz McIntyre, Katina Michael, and Katherine Albrecht

Is radio frequency identification (RFID) and the Internet of Things (IoT) a helpful new technology or a threat to society? If you understand what the technology is and how it works, it's easy to see how its widespread implementation could sound the death knell for privacy and civil liberties.

As you likely know, RFID is a tag and tracking technology that uses tiny microchips hooked up to miniature antennas to track items from a distance. This chip and antenna combination is called an RFID tag (Fig. 1). Each tag contains an ID number that is like a Social Security number for things because it uniquely identifies the item to which it is attached. And like a Social Security number, an RFID tag number is not just a number—it's a number that can link to virtually unlimited information in a computer database.



IMAGES © ISTOCKPHOTO.COM/JOHAVEL, WOMAN'S ARM IMAGE COURTESY OF THE U.S. HOLOCAUST MEMORIAL MUSEUM.

RFID tags are tracked and "read" by RFID reading devices (Fig. 2). These RFID readers gather information from the RFID tags via radio waves, similar to the radio waves that allow you to listen to your favorite FM station. RFID radio waves, like FM radio waves, travel invisibly through solid objects like purses, backpacks, wallets and shopping bags—and can even travel through walls and people.

Because RFID tags don't require batteries and can communicate information right through solid objects

Digital Object Identifier 10.1109/MPOT.2015.2410392
Date of publication: 8 September 2015

silently and invisibly, it means they can be easily hidden. For example, they can be inserted into the soles of shoes, embedded in clothing labels, or molded into plastic and still share the unique ID numbers and any other information that might be stored on their chips.

RFID readers can also be hidden in public and quasipublic spaces, so people might never see them at all. We've seen applications where they are inserted under floor tiles, embedded in doorways, hanging from ceilings, and even hidden in everyday objects like garbage cans, store mannequins, and park benches. It's this X-ray-like ability to identify and track objects silently and invisibly that makes this technology so useful—and potentially threatening at the same time.

Granted, RFID power could be used in positive ways. It could help reduce waste, allow for just-in-time inventory, and quickly identify whether needed products are in stock and available for consumers (Fig. 3). It can also be a boon for employee safety and truck (and driver) location determination in places like open pit mines. For example, active RFID tags embedded in helmets and clothing could help locate miners trapped under rubble.

On the other hand, RFID could also be deployed in less altruistic ways by marketers eager to track consumer behavior and rogue governments interested in secretly monitoring political dissidents. Unfortunately, such plans are widespread, and most consumers are unaware of the looming threat of ubiquitous surveillance that M.G. Michael has termed "überveillance."

Because RFID tags don't require batteries and can communicate information right through solid objects silently and invisibly, it means they can be easily hidden.

FIG1 An RFID tag. (Image courtesy of Katherine Albrecht.)

Stealthy abuse potential of "spychips"

Some industry proponents defend widespread tagging and tracking of everyday items and dismiss privacy concerns by pointing out that RFID technology has limited read ranges, especially the passive tags planned for consumer goods. It's true that passive tags do not contain batteries, have a relatively short read range of up to 6 m, and can only read and transfer sensor values when the tag is powered by an external reader. However, this shorter range and absence of batteries is precisely why these tags can be so invasive.

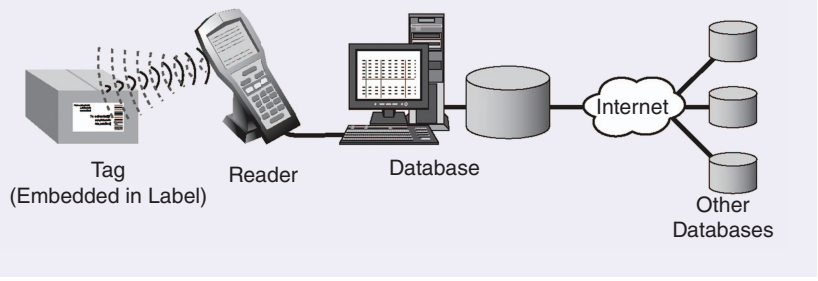


FIG2 Components of an RFID system. (Image courtesy of the U.S. Government Accountability Office.)

One risk associated with passive tags is their virtually unlimited life since their function is not dependent upon an onboard battery. This means that goods to which they are attached could be tracked whenever they come in range of a compatible reader device, potentially for decades. Since developers have talked about installing RFID readers not only in stores but other public and private spaces, it's easy to see how certain tagged objects, like shoes, clothes, and other items could act as long-term proxies for the location and identity of people wearing and carrying them.

Consider, too, that the shorter read range of passive RFID could better pinpoint exactly where a tagged object and the person wearing or carrying it is located for certain applications. For example, if a consumer has a passive RFID tag in his shoe, the shorter read range of just a few inches could be a better position indicator than a tag with a longer read range. If a reading device is set up to figure out who is standing in a particular spot, say in front of a store advertisement, this would reduce the chances of interference or confusion with RFID tags in other shoes that might be a short distance away.

Of course, read range need not be limited in these ways. There are two other categories of RFID tags besides passive tags. These include active and semipassive tags. While passive tags have no internal power source, active and semipassive tags contain batteries, extending their read range to 100 m or more.

The toll tags many people have in their cars for automatic toll payment on highways are an example of semipassive RFID tags with onboard batteries (Fig. 4). Government agencies find the car toll tags useful for monitoring traffic flow on highways and following the travels of government employees and persons of interest (Fig. 5). Toll tag records have even been used in court and custody cases to establish a person's whereabouts or habits. While this interest could be legitimate, it's easy to see how this surveillance potential could be abused by a repressive government or police.

Another way RFID proponents have tried to downplay the surveillance potential of their systems is by pointing out the technology's limitations and weaknesses, particularly in harsh environments. Unfortunately, it is often these very weaknesses that make RFID even more problematic. For example, hackers have been able to siphon personal information from RFID-laced credit cards by walking through crowds with a handheld reader device. They've also demonstrated the insecurity of the RFID tags in U.S. passport cards, which could compromise the privacy and security of travelers.

Certain environments and the presence of liquid or metal used to pose insurmountable challenges for the technology, but now there are new tags that overcome these limitations by utilizing the unique properties of different frequency bands. RFID systems operate in low-frequency (LF), high-frequency (HF) and ultra-high-frequency (UHF) bands. Lower frequencies have a shorter read range with a slower data read rate but are ideal for objects made of metal or containing liquid, which used to be impossible to track with RFID. HF or UHF systems allow for a longer read range and a faster data rate, but have been prone to interference, depending on environmental conditions. Over time, systems have improved for applications that require higher speeds. In fact, the fastest growing RFID tag market segment is UHF Gen2 (standardized by EPCglobal) and is predominantly used for item-level tracking of apparel.

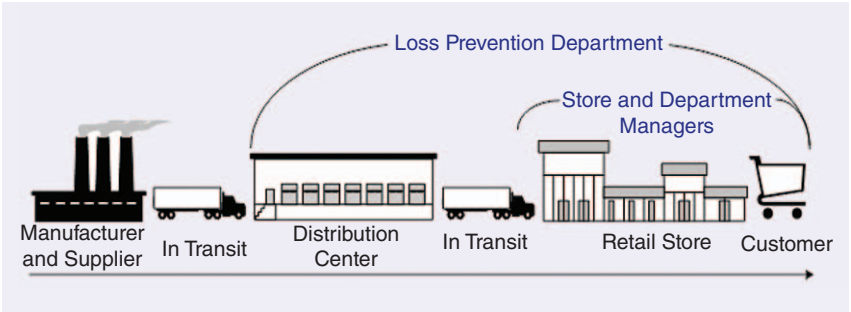


FIG3 RFID could be beneficial for tracking items from the point of manufacture to store shelves. However, RFID should never be used to track consumers without their knowledge and consent, inside or outside stores. RFID tags should be permanently disabled by retailers before consumers take possession of items they have purchased. (Image courtesy of Nicholas Huber and Katina Michael, 2007.)

FIG4 Sydney, Australia's, Cross City Tunnel e-tag. The Cross City Tunnel is a fully electronic toll road, and there are no toll booths for cash payment. As the vehicle passes one of the tolling points of the tunnel, the tag will transmit a signal to the toll gantry. This acknowledges and deducts the appropriate toll amount from one's toll account. (Photo courtesy of Jason Sargent.)

FIG5 Singapore's electronic road pricing (ERP) using RFID was launched by the Singapore Land Transport Authority in 1998. It was the world's first ERP system, an automated toll-collection system used to control and manage traffic volume in the city. (Photo courtesy of Katina Michael.)

One risk associated with passive tags is their virtually unlimited life since their function is not dependent upon an onboard battery.

Claims versus evidence

Developers have dreamed up hundreds of invasive RFID applications, not only to profit from observed consumer behavior but also to enable governments to use such data for their own purposes. Here are just a few troubling proposals pulled from the U.S. Patent and Trademark Office.

Hidden, flexible RFID tags with fabric antennas

Philips Electronics is the assignee for U.S. Patent #6677917, "Fabric Antenna for Tags" (Fig. 6). According to the patent documentation, "...the RF tag may be obscured from view and attached to a product or person in a hidden location. The RF tags may be hidden for a variety of reasons... Accordingly, RF tags may be embedded in garment tags, product tags, and clothing."

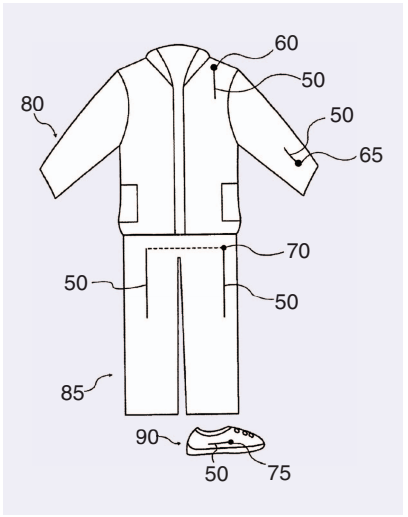


FIG6 From Philips Electronics U.S. Patent #6,677,917, "Fabric Antenna for Tags." Consumers might never suspect that their clothes and shoes contain tracking devices!

Bank of America's talking billboard

Bank of America is the assignee for U.S. Patent #6,708,176, "System and Method for Interactive Advertising" (Fig. 7). This patent envisions a world in which consumers

wear and carry live RFID tags that could be used to identify them or something about them for marketing purposes: "...[T]here is a need for a public advertising and announcement device that has the ability to identify specific individuals or groups of individuals who come into contact with the device, the ability to collect, gather and use personal information about those individuals or groups to select and present more interesting, targeted ads and announcements...."

FIG7 From Bank of America's U.S. Patent #6,708,176, "System and Method for Interactive Advertising." This patent drawing shows a random consumer in front of a smart billboard that scans for RFID tags.

A "person-tracking unit" that monitors people in public places

IBM is the assignee for U.S. Patent #7,076,441, "Identification and Tracking of Persons Using RFID-Tagged Items in Store Environments" (Fig. 8). This patent talks about not only tracking people in retail stores via live RFID tags they wear and carry to serve up targeted advertising. It goes further to claim the invention can be used to track people in "...other locations having roaming areas, such as shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, museums, etc...."

In Fig. 8, a "person tracking unit" tracks "RFID tags...integrated into items... Any item can include a RFID tag and may be a hat, watch, belt, shoes, scarf, purse, wallet, clothing, briefcase, jewelry, or any other item that can be 'carried' on or by a person...."

We've heard the RFID industry try to defend these kinds of creepy patent ideas, claiming that patents might not ever be used even though they actually work. So would they ever *really* track people like this? Yes! Well-known global corporations have already been caught using RFID systems to secretly monitor customers.

As far back as 2003, Gillette rigged an RFID "smart shelf" in a U.K. Tesco store in which the shelf sensors triggered a closed-circuit television camera to take mug shots of customers when they picked up packages of razor blades. Mug shots were also taken of consumers when they purchased the blades at checkout. At the end of the day, the store matched shelf photos with checkout photos. If there weren't matching photos, the people with only shelf mug shots were considered suspected shoplifters. When

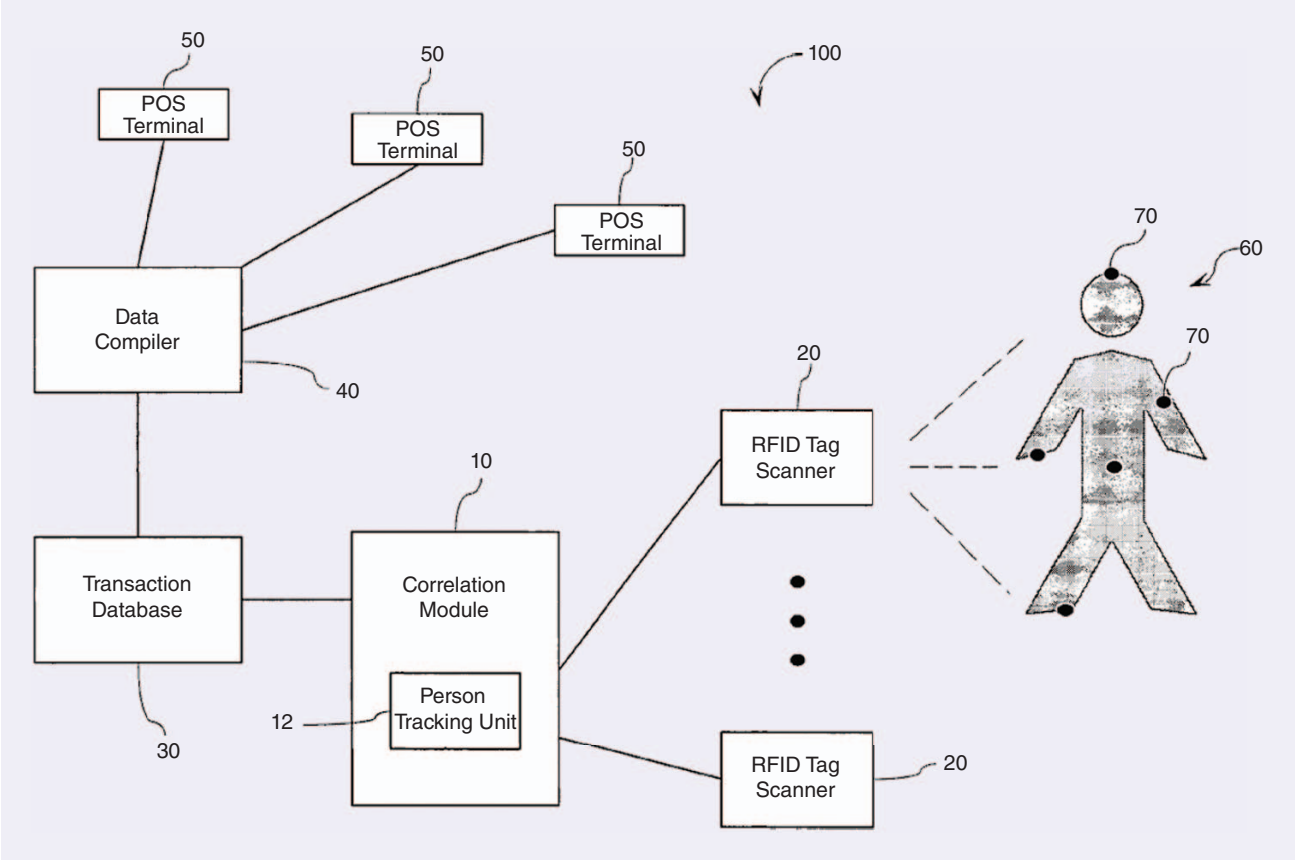


FIG8 IBM U.S. Patent #7,076,441, "Identification and Tracking of Persons Using RFID-Tagged Items."

reporters exposed the practice, the shelf quickly disappeared.

Procter & Gamble was caught in a similar scheme at a Walmart store in Broken Arrow, Oklahoma. When customers picked up Lipfinity brand lipsticks off the "smart shelf," an RFID sensor triggered a hidden camera to beam video of them interacting with the product back to Procter & Gamble headquarters in Ohio. It was never clear exactly who had access to the live feed of the product's predominantly female customers, which upped the creep factor.

More recently, in the summer of 2014, *Russia Today* reported that sportswear giant Adidas secretly inserted RFID tags into millions of German replica World Cup jerseys. Adidas refused to provide details about the deployment, and it's still unclear whether the RFID tags were used for tracking and if customers left the store with live RFID tags.

Because of the consumer backlash over RFID tests and general distrust of tracking technology, many retailers are keeping quiet about current trials and deployments in retail stores because they want to move forward despite consumer concerns.

We have been speakers at international conferences and have recently witnessed many RFID industry proponents practically giddy at the possibilities of tracking people. They see the god-like ability to monitor consumers as they purchase products in real time as an irresistible opportunity to increase market share and their profits. They've even gone so far as to envision RFID connected sensors that would enable those with control of the technology to "watch" closely as people handle and interact with products in their own homes and observe how they feel based on the interpreted behavior being monitored.

We fear that the ultimate trajectory of this technology could lead to renewed calls for the microchipping of people. While this may seem far-fetched, former U.S. Secretary of Health and Human Services Tommy Thompson called for people-chipping in 2005 on the news program *CBS MarketWatch*, recommending the technology for medical identification purposes. Thompson even sat on the board of the Verichip Corporation (renamed Positive ID Corporation) after he left his government office, and Alzheimers patients have already been chipped in a trial in a Florida nursing home. (These trials were quietly cancelled in 2007 about the same time it was revealed that implanted microchips were causing cancer in pets and laboratory animimals, as documented at http://www.antichips.com/cancer/index.html.)

All of these tagging and tracking plans are truly concerning, but it gets worse. The RFID industry has a plan to systematize all of this tracking and monitoring, with the ultimate goal of tracking and monitoring every item on planet earth 24/7. You may have heard of this planned system, dubbed the IoT.

Developers have dreamed up hundreds of invasive RFID applications, not only to profit from observed consumer behavior but also to enable governments to use such data for their own purposes.

IoT was coined back in 1999 by Kevin Ashton, cofounder and executive director of the then Auto-ID Center at M.I.T., a consortium of industry and government RFID proponents hoping to make ubiquitous RFID tracking a reality.

Recently, Cisco Systems has ratcheted up the original language of the Auto-ID Center's vision. Rather than simply call it the IoT, they now enthuse that we are headed toward an *Internet of Everything*. In light of this, we should perhaps now be considering the Internet of All Things, in other words, the Web of Things and People.

It is true that the "connectedness" offered by the IoT is extremely powerful, and has tremendous potential, but as far as people are concerned, there are two fundamental, and potentially fatal, flaws to the IoT vision. The first flaw is that people are not "things." However, as soon as they are incorporated into the IoT, they become things, at least in the eyes of the system. In addition, people potentially become prey, as well, as we have seen from recent events—prey for marketers, for overzealous security teams and arms of government, and for a whole lot more.

People are not mere objects. Placing numbers on individuals directly or indirectly through the things they wear and carry debases them to the same status as cans of cola and bags of dog food. It is simply dehumanizing—and living in such a world is demoralizing and creates huge power imbalances.

The second flaw is that linking objects to subjects en masse may someday spell the end of our privacy, which is already under considerable attack. And once our privacy is gone, our civil liberties will quickly vanish too. Once people are tracked, they can be monitored. Once people can be monitored, they can be controlled. The mere fear of ubiquitous surveillance has a way of forcing changes in behavior. The end result of self-imposed restraint under this kind of scrutiny could effectively gut critical freedoms like the right of free speech and press, which are essential to a democratic society. The terrible evidence for this is still with us from our not too distant past (Fig. 9).

FIG9 Women display their tattoos that were marked onto their skin at Nazi concentration camps for the purpose of identification and dehumanization. (Photo courtesy of the U.S. Holocaust Memorial Museum.)

As far back as 2003, Gillette rigged an RFID "smart shelf" in a U.K. Tesco store in which the shelf sensors triggered a closed-circuit television camera to take mug shots of customers when they picked up packages of razor blades.

While RFID may hold potential for good, we hope you now see that the master plan of developers has frightening downsides that you should know about as a consumer. You should also be aware of them as an engineering professional because one day you may be called upon to help develop an RFID project that could be used to track you, the people you care about, and ultimately all of society, with potentially devastating consequences.

Read more about it

- K. Albrecht and L. McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*. New York: Penguin Group, 2006.
- K. Albrecht and L. McIntyre. (2014). Protect yourself from RFID, eHow. [Online]. Available: http://www.ehow.com/ehow-tech/blog/protect-yourself-from-rfid-really-frightening-id-technology/
- K. Albrecht and L. McIntyre, "RFID: The big brother bar code," *Alec Policy Forum*, vol. 6, no. 3, pp. 49–54, Winter 2004.
- K. Albrecht and K. Michael, "Connected: To everyone and everything," *IEEE Technol. Soc. Mag.*, vol. 32, no. 4, pp. 31–34, 2013.
- K. Albrecht, "RFID tag—You're it," *Sci. Amer.*, vol. 299, no. 3, pp. 72–77, 2008.
- W. A. Herbert and A. K. Tuminaro. (2008). The impact of emerging technologies in the workplace: Who's watching the man (Who's watching me)? *HofstraLabor Employment Law J.* [Online]. *25(2)*, article 1. pp. 355–393. Available: http://scholarlycommons.law.hofstra.edu/hlelj/vol25/iss2/1
- K. Michael and M. G. Michael, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*. Hershey, PA: IGI Global, 2009,
- K. Michael, G. Roussos, G. Q. Huang, R. Gadh, A. Chattopadhyay, S. Prabhu, and P. Chu, "Planetary-scale RFID services in an age of uberveillance," *Proc. IEEE*, vol. 98, no. 9, pp. 1663–1671, 2010,
- K. Michael, and K. W. Miller, "Big data: New opportunities and new challenges," *IEEE Comput.*, vol. 46, no. 6, pp. 22–24, 2013.
- M. G. Michael and K. Michael, *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies*. Hershey, PA: Information Science Reference, 2014.
- M.G. Michael, K. Michael, and C. Perakslis, "Uberveillance, the Web of Things, and People: What is the culmination of all this surveillance?" *IEEE Consumer Electron. Mag.*, vol. 4, no. 2 pp. 107-113, 2015.
- A. Gilbert. (2003). 'Smart shelf' test triggers fresh criticism. *CNET News*. [Online]. Available: http://news.cnet.com/Smart-shelf-test-triggers-fresh-criticism/2100-1017_3-5107918.html
- A. Jha. (2003). Tesco tests spy chip technology. *The Guardian*. [Online]. Available: http://www.theguardian.com/business/2003/jul/19/supermarkets.uknews
- Russia Today. (2014). Tags with a price: Adidas RFID tracking could be used to spy on clothes' owners. [Online]. Available: http://rt.com/news/183604-adidas-rfid-tag-privacy/

About the authors

Liz McIntyre (liz@startmail.com) is an award-winning investigative writer and former bank examiner with a flair for exposing corporate shenanigans and bureaucratic misdeeds. She is also an internationally known privacy expert, consumer advocate, and coauthor with Katherine Albrecht of the bestselling expose on RFID technology, *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*. She currently works to promote privacy-friendly consumer services, like StartPage.com, and coauthors an online security and privacy column for eHow with Katherine Albrecht.

Katina Michael (katina@uow.edu.au) is the editor-in-chief of *IEEE Technology and Society Magazine* and the senior editor of *IEEE Consumer Electronics Magazine*. She is the associate dean international of the Faculty of Engineering and Information Sciences at the University of Wollongong, New South Wales, Australia, where she specializes in the socioethical implications of emerging technologies. Her most recent book, coedited with M.G. Michael, is *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies*. She holds a Ph.D. degree in automatic identification and location-based services and a master's degree in transnational crime prevention from the University of Wollongong and a bachelor of information technology degree from the University of Technology, Sydney.

Katherine Albrecht (kma@post.harvard.edu) is is an internationally known privacy researcher, consumer advocate, bestselling author, and nationally syndicated radio host. She is also a senior executive with the private search engine StartPage and is on the team behind the new privacy-protecting e-mail program StartMail. She holds a doctorate in human development and consumer education from Harvard University, has studied at the MIT Media Lab, and received a master's degree from Harvard in technology, innovation, and education. She has authored pro-privacy legislation, testified before the U.S. Federal Trade Commission and numerous state legislatures, and was appointed as a consumer technology expert by former New Hampshire Governor John Lynch. She coauthored the bestseller *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move* with Liz McIntyre. She is currently serving as an associate editor of *IEEE Technology and Society Magazine*.