"RFID: There's Nothing To Fear Except Fear Itself"

Opening Remarks by Rob Atkinson at the 16th Annual Computers, Freedom and Privacy Conference*

May 4, 2006, Washington, DC

... The United States is the worldwide leader in information technology in part because Americans have accepted the benefits of innovation without trying to control the risks ahead of time.

Thank you. It's a pleasure to be here and to argue for the case that Radio Frequency Identification (RFID) is a beneficial technology with few privacy implications.

When Linda asked me to debate Katherine Albrecht (head of Consumers Against Supermarket Privacy Invasion and Numbering [CASPIAN] and author of the anti-RFID book *Spychips*), her email said that the conference organizers wanted someone to represent the RFID industry's view. I emailed her back saying that I would be happy to debate Katherine, but that I don't represent the industry's view; I represent the view of consumers in the sense that I can't wait until RFID is deployed widely, since the benefits to consumers will be significant.

In the PR world the war is won or lost by how things are branded. The debate over RFID is no different. Katherine has cleverly referred to RFID tags as *spychips*. Who wouldn't be opposed to "spychips?" I prefer the term: *consumer-value tags*. This is a much more accurate term, not only because the RFID won't enable spying, but more importantly because it enables significant consumer value (see Box 1).

Perhaps I should mention that I am a card-carrying consumer value tag user. I have lots of CVT's on me. My cell phone. My RFID key to my office building. My Metro Card to ride on the subway. My Mobil speed pass. By the way, if anyone has a rogue scanner, feel free to scan me and extract any info you need.

* Opening remarks from debate with Katherine Albrecht at CFPC conference (www.cfp2006.org/progthurs.html).

RFID Benefits:

In her remarks, Katherine largely dismissed the benefits of RFID and vastly overstated the risks and costs. I am sure some will say I am doing the opposite, but let me highlight just a few of the potential benefits of RFID technologies. RFID could:

- Lower costs in the supply chain, enabling consumers to benefit from lower prices. For example, RFID could reduce standing inventories by 5 percent, warehouse labor by 7.5 percent, and theft by 1 percent of sales.
- Lead to faster time to shelves for new products and enable stores to better stock the products consumers want.
- Facilitate self-service checkout, cutting costs and boosting convenience.
- Reduce lost luggage in airports.
- Reduce counterfeit products, including in pharmaceuticals. For example, GlaxoSmithKline has started distributing HIV medicine tagged with RFID as a part of its pilot project to help verify whether the medicine is authentic or fake.
- Improve safety in hospitals with RFID-enabled wristbands and RFID-tagged surgical markers.
- Protect the vulnerable such as infants and persons with Alzheimer disease from leaving protected areas.
- Help the elderly and persons with chronic illness to remain in their own homes through RF-enabled medical sensors.
- Transmit soil moisture data to enable more accurate agricultural irrigation.
- Improve travel and tourism. For example, Great Wolf Resorts has issued RFID wristbands to patrons at its resort in the Poconos to use for keyless room entry, food purchases, game tokens and other items, and for entering the water park.
- Boost public health. For example, China is testing an RFID system to assist in controlling avian flu.
- Help first responders in the case of emergency. For example, Japan intends to sprinkle disaster areas with RFID-tagged sensors that will form a mesh network to detect heat and vibration. The Japanese are also embedding tags in manhole covers so that in disaster situations first responders can easily get information about what's buried underground. If U.S. municipalities were to do this, I can just hear people like John Gilmore (founder of the Electronic Freedom Foundation) howl about how the tags would facilitate people blowing up cars.
- My favorite: the RFID dog door. I was glancing at a book about homemade RFID solutions, and the author described how to build a simple RFID-enabled pet door for your dog. I can see it now: the mark of the beast is actually on the beast.

Box 1: What is RFID?

RFID stands for "radio frequency identification." In the case of supply-chain and consumer products, an RFID tag uses a tiny computer chip to store information about a product or an item in the form of a uniquely numbered code called an Electronic Product Code (EPC). An EPC is quite like a Universal Product Code (UPC) on a standard barcode. But while standard barcodes are read with lasers, RFID readers use radio waves to read RFID tag information. Because the EPC is a unique 96-bit number, it can correspond to more information in a database, which allows each specific item to be identified (such as a particular shaver), not just a type of product. An RFID tag will generally not have a power supply of its own. In that way, it is passive, like a copier machine on sleep mode. When its tiny antenna picks up a radio signal from an electronic reader, the radio wave energy sent by the reader provides the power for the tag to reply.[1] The activated tag emits the information contained in its chip, allowing the reader to identify it. RFID technology is a great improvement over labor-intensive barcodes for several reasons: (1) RFID readers have a larger read range of several feet, (2) RFID readers do not have to be within line of sight of the products, and (3) they can identify multiple items at once.

The advent of standard barcodes brought tremendous efficiency gains in the distribution and retail industries, and RFID devices now hold even greater promise. Wal-Mart and other industry leaders have begun to introduce RFID technology into their supply chains, the Food and Drug Administration has recommended their ubiquitous use on pharmaceuticals, and the Department of Defense plans to boost its use of the tags this year. The potential benefits to the economy and consumers are vast: RFID tags may facilitate dramatically reduced supply-chain costs, better inventory management, automated store checkout, reduced theft, more accurate and efficient product recall, improved counterfeit drug prevention, and a host of other benefits.

Yet despite the tremendous potential benefits of RFID technology, privacy advocates worry it could lead to more detailed tracking of the products we buy, maybe even to the level of taking inventory of what is in our homes and what is on our person at any given time. Arguing that stores, corporations, and even libraries will use the technology to spy on people, RFID critics have threatened boycotts to derail the technology's adoption. In response, a number of companies have postponed item-level RFID programs and lawmakers in several states and the U.S. Congress have introduced legislation that, if passed, would curtail the use of RFID technology.

Why Katherine's Fears Are Unjustified

Not only will there be significant benefits from widespread deployment of RFID, but the fears that Katherine and other RFID-opponents are trying to whip up are simply not justified. There are three main reasons why:

First, many of the arguments made against RFID could just as easily be made about existing technologies and systems in widespread use today, and in that sense are much ado about nothing.

For example, in *Spychips,* Katherine claims that the deployment of RFID enables the creation of a giant linked

database that tracks everything you purchase. But bar codes and credit cards already enable stores to link personally-identifiable information (PII) to purchases (although PII-lined data is almost never aggregated because retail chains jealously guard this data for competitive advantage and to keep the trust of their shoppers). In spite of Katherine's claims in her book, companies like Information Resources Inc. do not collect PII from point-of-sale terminals and integrate it into the massive database in the sky. Buying a product with an RFID tag on it is no different with respect to this than buying a product with a bar code. In both cases if you pay by cash, the store doesn't know who bought the product. In both cases if you use a credit card, they do. RFID doesn't change the equation one bit.

In *Spychips* Katherine says that RFID is "already being used in passports to track people across borders." When. When Americans or foreign citizens enter this country they must show a paper-based passport or visa. Presenting a 'contactless' RFID-enabled (and encrypted) smart passport doesn't change this equation one bit.

Again, in Spychips Katherine wrote: "…Imagine the power of being able to log onto a Google-like Internet search engine and find out all the items associated with a particular person." But after 10 years of e-commerce and people buying all sorts of things online, we can't we do this now. There is no database showing that in the last few months I went online to buy a tie, two books (including a copy of *Spychips*), and a jacket. An RFID-enabled future doesn't change this equation either.

Second, Katherine tries to whip up fear and loathing by making it sound as if all sorts of truly horrible things will happen just because they potentially could. But the key point is that "could" is not the same as "will" or "would".

According to Katherine, and I quote:

- Cards "*could* squeal on you as you enter malls."
- "Readers hidden in doors, walls, displays, and floors *could* frisk the RFID chips in your clothes and other items on your person to determine your age, sex and preferences."
- Companies *could* use it to "flash you a corresponding customer price."
- RFID "*could* give government officials the ability to set up invisible check points."
- You *could* be "pinpointed on the globe in real time."
- "Your insurance company *could* monitor your food consumption."
- "Readers *could* be hidden in artificial landscape boulders or signs."
- "RFID *could* lead to '1984'."
- "The government *could* track everyone."

- "The tag killing option *could* be easily halted by government directive."

- "Throwing away a spy-chipped product package *could* give people a false sense of security if the company has hidden a second chip in the product itself for surreptitious tracking purposes."

And my favorite "could" of them all:

- "The end point of all this tracking *could* be the implementation of an RFID device in people's flesh to number and identify them for a multitude of reasons, including buying and selling."

There is no doubt that correctly used RFID will be productive and highly beneficial. There is also no doubt that if RFID is misused it could potentially lead to some harmful consequences. But this is not unique to RFID. This dichotomy between benefit and harm exists with all technologies. Put to correct use, cameras, guns, chemicals, cell phones, syringes, X-Ray machines, household cleaners, the Internet, cars, and airplanes, to name just a few, can have productive and beneficial uses. But if misused all can cause harm. But we don't ban these beneficial technologies because harm is possible.

Third, not only is "could" not the same as "would," it won't become "would." It's true that some, but certainly not most, of these worst-case scenario "coulds" are possible. It is possible, as Katherine warns, that the government could forcibly implant RFID chips in our bodies. But will this happen? In assuming that it might, Katherine assumes that: a) consumers are easily manipulated dupes; b) corporations and governments are all powerful Leviathans; and c) there are no laws governing either.

So let's look at what would be required for some of Katherine's scenarios to come true. In *Spychips* Katherine states that: "It's almost inevitable that governments will appropriate the RFID infrastructure and turn it to their own surveillance purposes." But what she fails to point out is that if it wanted to, the government already has the means to monitor every one of my phone calls, open every piece of my mail, use infrared sensors to monitor my houses, and bug my bedroom. "The government" doesn't need RFID to do any of this. While the government could do all these things, they don't. They don't because they are governed by a host of laws and regulations, not to mention the Fourth Amendment. Moreover, when government does cross the line protecting American civil liberties, as they have occasionally done, they are almost always caught and punished.

Katherine recently stated that "If the VeriChip becomes a common payment device similar to the "contactless" payment system in the Exxon Mobil Speedpass, all who wish to buy and sell goods will be compelled "to receive a mark on their right hand or on their forehead," as it says in the Book of Revelations. But let's look at what would have to happen to enable this dystopian future. It would simply

require that we have a revolutionary overthrow of the U.S. government and scrap the Constitution; eliminate the Supreme Court; do away with Congress; shut down the free press; and convince Americans to give up their inborn skepticism of authority and love of liberty. But other than those "simple steps," the mark of the beast requirement is pretty easy to impose. (Hopefully, you know sarcasm when you hear it…).

Not only are these bad uses of the technology never going to happen; in many cases it would be very difficult, if not impossible for them to happen. For example, Katherine sketches a scenario in *Spychips* where RFID readers are set up on off ramps of highways (it's not clear just who would set these up) to read RFID chips in car tires in order to track a particular person. But this implies: 1) that RFID tags are in tires; 2) that they are connected with PII that is publicly accessible; 3) that readers are deployed surreptitiously (which by the way will be very difficult since they emit very readable radio waves and must be powered); 4) that the DOT would let you do anything to their highways that is not in their rule book, including putting something in their right of way without their permission; 5) that the person being tracked happens to pass by that particular reader; and 6) that the information is able to be read. Needless to say, such a scenario is far fetched to say the least. But because most people are not technical experts and do not understand the technical ins and outs of RFID, it is easy to get the average American, and all too often, the unsuspecting press corps, to fall for such fairy tales.

Even if some of these worst-case scenarios were feasible, market forces make it exceedingly unlikely they would occur. In a hyper-competitive marketplace, companies are extremely sensitive to gaining and maintaining customer good will. The easiest way for a company to lose business is to misuse information or to lie.

If a company publicized or misused PII about their customers or made them feel uncomfortable in any way, it would suffer a serious backlash. If a company were to say that it was killing tags only to reactive them, it would suffer a serious backlash including loss of business and legal action for fraud. If it were to hide tags on ladies' underwear, to use Katherine's favorite scare story, how long do you think it would be before an Internet-organized boycott of the store and manufacturer would be in place and thousands of lawyers would descend upon the company like a barbarian horde.

Not only is it highly unlikely that companies would engage in these kinds of activities, but in the vast majority of cases, tags won't even be on the products. If item-level tagging becomes more widespread, the tag on the vast majority of products will be on the box or removable price tag. In other words, a pair of pants might have an RFID tag on the price tag, but once customers get home and throw away the price tag, they will have thrown away the tag. Moreover, technologies are evolving to give consumers empowerment tools. For example, IBM is testing a new "clipped tag" that would enable consumers to pull a tag that would essentially turn the chip into a proximity

tag that could not be read remotely, even from a few feet.

Moreover, much of what Katherine warns about will be done on an opt-in basis. I am actually looking forward to the day when my refrigerator has an RFID reader on it so it can read when I run out of milk and automatically reorder it from Peapod, the Internet grocery store. But if I own a refrigerator with a reader I link to Peapod, that will be my choice. Maytag won't be forcing me to buy an RFID-enabled, Internet-linked refrigerator so they can read what I eat and then sell the information to my insurance company.

Likewise, there are a host of other applications that people can choose. My 14-year son and I went to Staples last weekend to buy a computer printer cartridge. I got to the store only to realize I couldn't remember the model number of the printer I had. My son said, "Dad, if we had RFID on products, we could have uploaded our stuff to our own web site, and then we could have just checked the web using your Treo." Unfortunately, we didn't so we had to trek all the way home to get the printer cartridge number.

Finally, it is important to realize that privacy is not free. Some privacy advocates want to impose their desired level of privacy on the majority of Americans. However, banning, reducing the functionality, or increasing the cost of consumer-level RFID will force consumers to pay higher prices, as well as reduce convenience and services. Moreover, slowing down or constraining RFID will not only hurt consumers, but it will mean that other nations will lead in the RFID industry, damaging U.S. high-tech competitiveness. While we are putting the brakes on new technologies, other democratic, freedom-loving nations, like Japan and France, are embracing them, in part so their technology companies can dominate the global market.

Have We Lost Our Faith In Technology and Progress?

I'd like to share with you a quote warning of the impacts of technology on privacy:

> *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual the right to be left alone.*[1]

The technology and business methods the author opposed? – photography and mass market newspapers, for this statement was written by Louis Brandeis in 1890. New technology always brings a mixture of excitement and fear. For example, in 1966 *Life Magazine* had a cover story warning Americans of a looming new surveillance society stemming from the development of a new and scary technology: the transistor. The authors warned of a world where electronic eavesdropping bugs could be small enough to be placed inside a martini in an olive. In response, Congress held hearings and people worried about whether their most secret conversations were in fact secret. Forty years later we can look back and smile at how naïve they were to be worried.

But the key point is that over our 200-plus year history America has had enough confidence to choose opportunity and the excitement and not give into the fear. We didn't ban cameras in the 1890s or organize boycotts of newspapers that had the audacity to include pictures of people in them. We didn't ban telephones even though for many years, people talked on party lines. We didn't boycott stores that first accepted Diners' Club cards in the 1950s. We didn't ban transistors in the 1960s for fear of hidden transmitters in martini olives. We didn't ban or slow down the Internet in the 1990s. And we shouldn't ban or slow down RFID in the 2000s.

The U.S. is the worldwide leader in information technology in part because Americans have accepted the benefits of innovation without trying to control the risks ahead of time. RFID is no different. If it's like past rollouts of IT, things will work out fine with little harm to privacy. Moreover, industry appears to be well on the way to addressing legitimate privacy issues through their efforts with EPC Global and other venues. For example, working with the Center for Democracy and Technology and other consumer organizations, a number of companies involved with either developing or deploying RFID developed a set of "Privacy Best Practices for the Deployment of RFID."[2]

I don't fear new technology. To the contrary I welcome it. But I do fear that because determined technology-skeptics and foes are working hard (with the complicity of the media – see Box 2) to legitimize irrational fear, Americans' view of the future and technological innovation may be changing from one where most of us had faith in the future to one where resistance to innovation is legitimized as worthy civic involvement, even when it stems from that irrational fear.

Franklin Roosevelt famously stated that "the only thing we have to fear is fear itself." De we really want to live in a society defined by people who portray new technologies as the next step to a totalitarian state, or do we want to move forward as we always have, supporting innovation and trusting informed consumers, active citizens, businesses in competitive marketplaces and democratic government to address issues if and when they arise. Is America really going to be the only developing country to forfeit the vast benefits of RFID because a small but vocal and determined minority can scare the rest of us into opposing this technology? For the sake of my 14 year old son, and all our health, time, safety, freedom, and convenience, I fervently hope not.

Box 2: Confusion Reigns Supreme: Even "Objective" Organizations Like *Consumer Reports* Succumb To the Fairy Tales and Hype Spun by RFID Opponents.[3]

While it may not be surprising that some privacy extremists are trying to scare consumers and policymakers into opposing RFID, it's more surprising that at least one mainstream organization that looks out for consumer interests has fallen prey to the misleading propaganda coming from the RFID opponents. In this case, *Consumer Reports* magazine recently issued a special report entitled "The End of Privacy."

Succumbing to the same mistake that "could" is the same as will, *CR* warns that "tiny devices attached to everything you buy could put you under extensive surveillance." But it gets worse. The article opens with the sobering warning: "Oh, for the good old days when Big Brother merely watched you [and what days were these?]. Soon he'll be coming home with you in what you buy, wear, drive, and read." With so-called objective reporting like this, it makes one long for the good old days of objective yellow journalism.

Where did *CR* get its information? From the fact that they repeated a large amount of the disinformation contained in *Spychips*, it's clear that the *CR* authors decided the best way to write an objective article was just to transcribe claims from Katherine Albrecht's book. Clearly showing that they have read *Spychips* cover to cover, the article asks, "could a high-tech thief 'break into' the tags and cull your banking and medical information?" Drawing from *Spychips* (a book warning that government could implant RFID chips in our bodies) the CR authors repeat the notion that RFID "could" one day be sewn into clothes and that "tags could broadcast to a database that can be linked to your credit card," and this raises the "potential for corporate and government snooping" to a new level.

But like all anti-RFID propaganda, the article doesn't exactly spell out how these abuses will or could happen. For a simple reason, because they won't and/or can't. Bottom line: fear sells more magazines than objectivity and journalistic integrity and fact checking. Sound and balanced reporting, and common sense are lost as the news business merges with the entertainment industry.

ENDNOTES

1. See Robert Ellis Smith, Ben Franklin's Web Site, (Providence, RI: Privacy Journal, 2000), p. 122.

2. Center for Democracy and Technology, "CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology" (www.cdt.org/privacy/20060501rfid-best-practices.php).

3. *Consumer Reports*, "The End of Privacy?" June 2006, pp. 33-39.

About the author: Dr. Robert D. Atkinson is President of the Information Technology and Innovation Foundation.

About the Information Technology and Innovation Foundation

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policies proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

For more information contact ITIF at 202-626-5732 or at mail@innovationpolicy.org, or go online to www.innovationpolicy.org

ITIF • 1250 Eye St. N.W. • Suite 200 • Washington, DC 20005