C. Austin Fitts: Let's turn to our interview. It's always a special treat because Katherine Albrecht is just amazing – she has an amazing ability to articulate and communicate the challenges of new and very invasive technology.

Katherine is an author and co-author of six books and videos. The two most popular are *Spychips* and *The Spychips Threat*. She was a guest on the *Solari Report* in April of 2010, and we talked about her book *Spy Chips* at that time.

She's the director of the CASPIAN Consumer Privacy Network. She holds a doctorate and masters from Harvard in education, and is extremely well educated, in addition, on all aspects of digital technology. Katherine, are you with us?

K. Albrecht: I sure am. It's a delight to be on with you and your listeners tonight, Catherine.

C. Austin Fitts: Well, I want you to know you're the only person who's ever been the hero twice on the *Solari Report*.

K. Albrecht: Oh, my goodness. Well, thank you so much. That's really an honor.

C. Austin Fitts: You joined us in April 2010 on the *Solari Report*. So let's assume, for a second, that our subscribers have listened to that. Bring us up to date on what's happened since then, and the latest developments in invasive technology, including the RFID chips.

K. Albrecht: Well, there have been some disturbing developments, both on the RFID front and on the digital privacy front. So why don't we dive in first to the RFID, and then I want to get into some of the changes that Google has made since 2010 that many people are not even aware of, and what some of those implications are.

As far as the RFID goes, when I first discovered that there was such a thing as RFID – radio frequency identification microchips, or tiny microchips hooked up to antennas that could transmit information through walls or through purses, and reader devices could be placed in doorways or floors or furniture or really anywhere, I was convinced that, and I believe the industry was convinced that the place that we were going to see the deployment of RFID was in consumer products, so that they would replace the barcode or supplement the barcode.

So that every physical object on Planet Earth would become trackable. I mean that's still part of the longer-range plan. It's been a little bit harder for them to pull off than I think they thought back in 2002 and 2003.

But the plan, just to lay out the big picture, is for every physical object on earth – and I mean every sheet of paper and every Bic pen and every coffee cup and every jumbo jet and every sewing needle would have its own unique ID number, that would be encoded into a microchip. The microchip would be hooked up to a miniature antenna that could transmit that ID number at a distance to a reader device.

And all of these objects – now that we have the storage capacity to actually keep track of an immense amount of data in these blade servers and – we have almost an unlimited ability to keep track of data now – that all of these objects would report their whereabouts, and that a centralized computer system would keep track of everything, all the time.

And they refer to that as the Internet of things. In the same way that now we've got an Internet, where I can just punch in an IP address, and I can bring up a website that accesses files in Germany or India or anywhere on the globe, the creators of the RFID industry envision a world where you can do the same thing, and figure out where the teaspoon is from your grandma's silver set. And you could pinpoint its precise location – in which drawer, in which of your aunt's homes it wound up.

So that kind of a picture, I think, becomes a little bit chilling, once, of course, you start to understand that that's not just about managing inventory and getting things more conveniently into Wal-Mart stores, but that's really ultimately about tracking and controlling people.

Because really what makes people who they are, are the things that they do and interact with on a daily basis – the things they eat, the things they wear, the people that they have contact with, the places that they go. All of that information would be trackable and reported back to the central brain, as it were, through this Internet of things.

So in 2002 to 2005, in that whole range, we really waged what I think was an extremely effective campaign against the use of RFID in consumer products. And, at that time, I truly believed that other civil liberty and privacy organizations, of which there are many in the U.S. – that they would step up and deal with the non-consumer aspects of this – the tracking of people or the tracking of money, the tracking of credit cards and the like.

And so I always made it very clear, from the outset, that my organization, CASPIAN, which is Consumers Against – it's probably now about to be Surveillance, Privacy, Invasion And Numbering – that our group is a consumer group, and we were opposing the use of this on consumer products.

Well, what wound up happening, instead, is they kind of went around us. And, at this point, the number one application for RFID that regular people are likely to see is probably the worst possible application, and that is in identity documents and in credit

cards. So we are now seeing RFID tags – if I give a speech, and there's 1,000 in the room, probably three-quarters of them have an RFID tag in their wallet, right on their credit card.

So that's, again, probably one of the worst possible places you could put it. Because once you tie RFID and microchips into transactions with human beings, in which people have to be identified – because credit cards are sensitive, and they give access to our resources.

And once you begin to tie them into ID cards, like they're doing in border states with the enhanced driver's licenses, then you get dangerously close to tying them in and linking them in with biometrics and, ultimately, with the human body. And that's why we've also waged a pretty aggressive campaign against the microchipping of human beings, which we actually have stopped.

We were able to stop that a couple of years back. People may not remember this but there was a period of time, a couple of years ago, when Blue Cross Blue Shield was running trials of human microchipping, when we had a trial underway down in West Palm Beach, Florida, of 200 Alzheimer's patients who were literally being injected with trackable microchips.

We had Tommy Thompson, the former head of the FDA sitting on the board of directors for the VeriChip Corporation that manufactures these devices. We had Columbian President Uribe actually stating to a member of the U.S. Congress that he would be willing to implant microchips into Columbian guest workers before they traveled to the U.S.

So there really was a period of time in which it felt like it was almost inevitable that these implantable microchips were coming and coming very fast. And what we did was uncover, due to a very persistent pet owner whose dog died after a tumor developed around his implantable microchip – she rolled up her sleeves and dug up all of this research from obscure toxicology and medical journals, and discovered that what happens when you put these microchips into animals in the laboratories is that they get cancer.

And the reason that the laboratories were even publishing this was not because they were researching the physical effects of these microchips, but because they implant the microchips into laboratory animals to keep track of them, so they can distinguish between the ones who have had an experimental treatment and the control group. And what they were finding was that their research was being invalidated when they were doing these toxicology studies.

Because totally independent of whatever substance they were testing, they were discovering that these animals were getting cancer around their microchips. And so once that information came to light, I worked with Todd Lewan from the Associated Press, and

we spent six months really doing a very in-depth research piece of several thousand words, which was published in all the places the Associated Press gets published, literally all over the world.

And that caused the VeriChip Corporation's stock value to plummet from over $11.00 a share to just 24 cents a share within just a matter of weeks.

C. Austin Fitts: It's amazing what happens when you hit the price of the stock. That's when you can get real change.

K. Albrecht: They got D listed. They're now a penny stock. I've always believed that they're a stock scam. I think they're a pump and dump. I don't think that they've ever been a legitimate company. And I think that Scott Silverman, who runs the – I don't even know what name he's going by now. He's given a bunch of different names and keeps buying and selling out shares of the company.

But I think that that company, just from an investment perspective – what they have relied on is very breathless media reports about – you know they've been claiming that they were going to develop an implantable glucose censor that diabetics could inject into their flesh. And it would wirelessly transmit their blood sugar levels.

There are 1,001 technical reasons why that's just not going to happen. And even if it did, it would not be this company that I would rely on to do it, because they don't even have a research arm.

C. Austin Fitts: Right.

K. Albrecht: So they literally are just a little office park – one office, a three-person operation that has managed to make millions off of the public's gullibility and, I believe, fear of microchipping. So right now, to the best of my knowledge, just to give people an update on the implant situation, as far as humans go, I'm not aware of any human beings that are currently being microchipped in the U.S. or anyone actively promoting implantable microchips for human beings in the U.S.

With that said, there's a growing movement in communities across the country to mandate the microchipping of pets. So Los Angeles County – the unincorporated areas of L.A. County, for example – it is, by law, that you must microchip your dog, or you face an ever escalating series of fines that actually gets very punitive, very quickly.

And there was one dog, Charlie Brown, which we've reported on our ChipMeNot.com website, which features all of the animal studies and the animals that have died from the microchip, who actually bled to death in Los Angeles County after being microchipped. So it's a dangerous technology. It's got a lot of downsides.

We hear regularly from people whose pets have developed cancer around the microchips. And we have put together kind of an informal registry of those stories at ChipMeNot.com. And we're encouraging people to visit the website, and if they know of any stories of animals who've had adverse reactions from these microchips – it certainly seems as though the veterinary associations – they're in the pay and in the pocket of the microchipping companies.

Because there's huge, huge money involved in doing this. The veterinarians make a lot of money from it. All of the animal organizations receive huge donations from the companies that benefit from their endorsement of this. And so there's really a – I hesitate to call it a conspiracy, but certainly there's a lot of financial interest in promoting that, and not a lot of interest in reporting on the adverse reactions. So we've kind of taken that on at ChipMeNot.com.

Now getting back to the human chipping, the places, as I said, you're likely to see an RFID tag – and I'm guessing that most people on this call right now – if you have a credit card, you probably have a remotely readable microchip in your credit card. And you'll know that because your credit card will say PayPass or EasyPass or – there's a whole bunch of different names for it.

The symbol for the credit card is – it looks like the letter "C" nested inside of itself – a big one, a medium one, and a small one. They're like little waves coming out. And if you see that on your credit card, then your credit card contains a microchip and an antenna, and it can be read, in the clear, unencrypted, by any credit card reader that's held within range of it.

So there has been – I don't know if anybody on the call has been a victim of this. But a lot of people are reporting, "Hey. Wait a minute. All these charges suddenly were getting racked up to my credit card. I have no idea where they got the number." Well, it may be that they got it by hacking a database.

But it may also be that they got it simply by walking through a crowd at the mall on Sunday afternoon, as you were doing your shopping. Because it's literally that easy to skim the numbers and the expiration dates and even the names off of people's cards, by simply standing next to people who have these things in their purses and wallets.

C. Austin Fitts: I wanted to let you know. I just got back from Amsterdam. And in almost all the restaurants and shops, I couldn't use my credit cards because they didn't have an RFID chip in them.

K. Albrecht: Yes. That's actually a contact chip. That's not an RFID chip, which is –

C. Austin Fitts: Oh, okay.

K. Albrecht: The European system is called Chip and Pin, and that's actually a contact-based chip that they have in the credit cards. And the idea there is that the microchip encodes the individual's pin number.

C. Austin Fitts: Uh-huh?

K. Albrecht: And so when you insert your credit card into a European credit card reader, it makes contact – people might have seen these at Kinko's and in the military ID cards. They have a little square that's gold on the card. It looks like a little, square, gold circuit, for example.

C. Austin Fitts: It looks like a little chip.

K. Albrecht: Yes. Kind of like a chip. Yes. It's flat. It's about the size – my goodness. I don't even know what size that would be. The size of your little fingernail, maybe. Your pinkie nail.

C. Austin Fitts: Right. It's like a quarter of an inch.

K. Albrecht: Yes. About a quarter of an inch squared. And it's slightly raised. It has a little texture to it. And that is a contact chip, so it's not RFID. Because the RF part of RFID is radio frequency, meaning that it broadcasts through the air, as opposed to a contact chip.

So there are contactless RFID tags that are in the American credit cards for really no good reason. Because very few merchants even have contactless credit card readers that they're using. So it's really kind of a question mark as to why they invested this enormous amount of money in putting those contactless chips invisibly to all of our cards.

But over in Europe, those contact chips are accompanied by a pin number. So the idea is that if I were to steal your wallet and grab your credit card and try to pay for something, if I didn't know the pin number that was encoded in that microchip, I'd be unable to use the credit card.

C. Austin Fitts: Oh, okay.

K. Albrecht: So it's an extra layer of security, and probably a good one, to be honest.

C. Austin Fitts: A good one? Okay. That makes me feel much better.

K. Albrecht: Yes. U.S. banks have really resisted incorporating that here in the U.S. And it's still somewhat of a mystery, to me, why they've resisted the chip and pin system, other than just reluctance to change. But they certainly have embraced the sort of wave and go wireless RFID microchip credit cards. So that's the one place that you're likely to see them.

And then the other place that you'll see an RFID tag – they can be used to track people – and this is really the far worse concern – is in the e-passport cards. Not the booklet passports, but the card passports, which are plastic. They look like driver's licenses, but you can use them to cross over the border into Canada or Mexico or the Caribbean.

And those ID cards, those e-passport cards, are also available incorporated into the driver's licenses of several of the border states: Michigan, New York, Washington State, I believe Arizona and, I think, some other states were looking into this as well – have given their drivers – their citizens an option, that when they sign up for their driver's license, they can check a box and have the e-passport RFID technology incorporated directly into their driver's license.

That's actually an extremely disturbing program. Because the RFID tag that they've put into the e-passport cards and into the driver's licenses – called enhanced driver's licenses – that is actually run not on a secure standard.

And you would think that the State Department – well, the State Department claims that this is for enhanced security. But the problem with it is that the standard that they've chosen to use in those cards is the same standard that is used in all of the product tagging technologies.

Just to simplify what I'm saying there, if you have, let's say, a Michigan State enhanced driver's license in your wallet, and you walk into a Wal-Mart store – the Wal-Mart store will have readers in it to manage its inventory. Because as of 2005, Wal-Mart has been requiring its suppliers to put RFID tags on the crates and pallets that go into their warehouses.

And now they're putting them onto the packaging of quite a few of the products in their stores. And so there are reader devices to keep track of those things for inventory management.

And what people don't realize is if you have one of these ID cards and you stand anywhere near a shelf that has an RFID reader in it, the Wal-Mart shelf will read your ID card right through your wallet or your pocket or your purse or your backpack. And, in fact, the RFID reader can't prevent itself from reading that information, because it's transmitted in the clear.

So that's an enormous problem. It is a problem that the RFID industry itself was absolutely horrified – when the State Department said that they were going to use this EPC or electronic product code standard in government issued secure identity documents, because it's easily cloned. It's easily hacked.

I have actually demonstrated a device at the Michigan State Legislature – that I can literally hold a device the size of a pager in my hand, and I can walk near anyone who has one of those enhanced driver's licenses in their pocket or their wallet. I can stand next to them on the elevator. I can push a little green button on this pager-sized device, and capture the number off of it, without their knowledge.

And then I can push another little button, right next to that green button, and I can begin transmitting that number myself. And I can use it to pose as them, pop open their office door, or any other thing that's tied up with that number. So it's really shocking.

And I believe it was shocking to the RFID industry as well, which submitted many, many pages of testimony saying, "You're out of your mind, State Department, to use the electronic product code. That's designed for maximum read range, which can be 30 to 60 feet away. It's designed to be read through walls. It's designed to be read in the clear, with no encryption. And it's designed for maximum reading and trackability."

So it is my belief that the government intentionally selected a standard that they knew would be compatible with reader devices that are being put in place in public places to manage inventory, so that they would be able to create an infrastructure for also tracking and monitoring people, as they walk around with these devices embedded in their ID cards. So that's kind of the nutshell update on that.

You know people always ask me, "What's it going to take for the U.S. public to be willing to roll up their sleeves and get microchipped?" And I believe it's probably going to take our generation dying off, to be honest. I don't think our generation is ever going to accept that.

So what they're doing now – they've taken a page directly from Hitler's playbook, and they're going after the kids. And in San Antonio, Texas, we have a campaign underway – ChipFreeSchools.com. San Antonio, Texas – the Northside Independent School District is running a pilot this year, in which 4,200 middle school and high school students at one middle school and one high school have been issued RFID active tracking badges that they are required to wear while they're on campus and on the bus.

And what these are – they're active RFID tags, which means that unlike the ones I've been describing, where you have to activate them with a reader, these actually have two button batteries onboard, or two cell batteries. And they transmit a continual 140-foot swatch of personal information at all times, 24 hours a day.

So these kids have these active EMF-emitting devices. And having just come through a two-year breast cancer saga myself, I can tell you, the idea of having an active EMF transmitter literally hanging between a girl's developing breasts, in junior high school and high school, 24 hours a day – it works out to something like 14,000 hours. I was doing the math, and it's shocking. That's the one place you really don't want to have constantly emitting EMF energy.

But even putting aside the health risks of this, the way the system works, they've taken the entire school environment, and they've placed reader devices into the ceiling. They're very unobtrusive; they're every 100 feet. And with that technology, they are able to maintain a constant monitoring and location pinpointing of every single student in that school – of both schools – the entire time they're on campus.

What's even more disturbing is when the kids go home, they continue to have these things in their backpacks or around their necks, and they're broadcasting. If a child is in their bedroom in the average San Antonio suburb, you could walk down the sidewalk and be able to pinpoint the location of those children, because they're beaming out this 140-foot swatch of their unique ID number.

So we've mounted protests against this. We've gone to speak against the school board on this multiple times. They've silenced us. They've essentially said they're not willing to take any further testimony. They don't want to hear from parents.

There is one brave student – Andrea Hernandez, who's in tenth grade and an honor student. And she, for religious reasons, has stood up and said that she does not want anything to do with this technology.

And they've been terribly punitive with her, and they've even threatened her with expulsion. So she can't eat lunch with the other kids. She wasn't allowed to vote for the homecoming queen. They've been bribing the kids with candy and gifts, and she has not been – she's very – publicly not been given the candy, when the other kids get it.

And so it's really been a shaming exercise there. The good news, I suppose – we've gotten a tremendous amount of media attention on this. She's been on the BBC and *Times* . And I don't know where all else. She's been all over the world talking about this now. So it certainly is something where the adults are scandalized.

But she reports that a lot of her friends at the school just kind of shrug and say, "Well, what do you expect? It's part of the modern world." So that's kind of the latest.

I think that's our big battle right now. If we are not able to stop this pilot program that's taking place in San Antonio, then they are going to roll it out to all of the schools across

the Northside Independent School District, and then probably all across the State of Texas. And then, at that point, it's going to be really, really hard to put out the forest fire that's going to come from that.

And what worries me the most is some of these kids are 16, 17 years old. And within ten years, they're going to begin making policy decisions for the rest of us. And if they're trained and conditioned, at this point, to think that it's appropriate for people to have monitoring devices that let authorities monitor their location all the time, then we will have lost, I think, the one thing standing between us and total RFID insanity, which is the fact that people say "no" to it.

C. Austin Fitts: Right.

K. Albrecht: So that's the big battle, I think, on the human and the animal tracking front. And that's kind of the update on the RFID. So I didn't know if you had any questions on the whole RFID.

C. Austin Fitts: One of the things I found, when I worked in government, was it was very hard to conceptualize about how this data could be aggregated with other data and used, and used with ill intent behind it, and the power of data in a whole variety of different ways.

And I've posted the new DVD that you're featured in – *Shadow Government*.

K. Albrecht: Oh, good. Yes.

C. Austin Fitts: Yes. We do a "Let's Go to the Movies" section. And so that's our movie of the week – our documentary.

K. Albrecht: I was actually the executive producer of that film.

C. Austin Fitts: Well, it doesn't surprise me because that film does a marvelous job of helping you envision how this works. It makes the invisible visible. And you start to really see the invasiveness of it and the dangers of it.

So maybe you could talk a little bit about the documentary – how it came to be and what it does, because I want to encourage everybody to get it. If you have never envisioned how this stuff could be really organized and used, I think it does a marvelous job of doing that.

K. Albrecht: Oh. Well, thank you, Catherine. I appreciate your endorsement of the film. The way the film came about – it's actually based on Grant Jeffrey's book *Shadow*

Government. I never had an opportunity to meet him. He passed away earlier this year, unfortunately, from an embolism.

But Grant Jeffrey had done quite a bit of work on the whole privacy issue from a Biblical perspective. And the good folks at Cloud 10 Pictures, up in Canada, contacted me, as just one of the people they wanted to interview for the film.

As we got to talking, and I took a look at the script, they said, "Oh, wait. You're leaving out all this important other stuff." And so long story short, we wound up rewriting the script and identifying a whole new set of experts for them to interview, really to look at the state of the art and some of the cutting edge research that's being done. And talked to many of my activist friends. It was a lot of fun, being able to fly around the country and interview some of the top minds on this stuff.

The movie *Shadow Government* essentially opens with a man who wakes up in the morning, and he's just going about his business. But it shows you, at each stage, as he's turning up the thermostat and picking up the newspaper out of the driveway, etcetera, etcetera – it's showing you, at each stage, what either is possible today or is being envisioned as a tracking method.

And you kind of see this happening, and you sort of think, "That's creepy. They don't really need to be watching that," or "Boy, he's throwing away his orange juice." And they know what he's putting in the garbage because of the RFID tag. That's pretty creepy.

But then it comes really to a head when he gets a visit from government agents who want to know why it was that he was photocopying certain posters. And they had to do with – he was opposing abortion. And they wanted to know why he was making those photocopies.

He said, "How did you even know the photocopies were mine?" And then we bring in someone from the EFF, who talks about the fact that all photocopiers for the last – I don't know – ten-plus years have hidden a tiny pattern of yellow dots.

And this is true for probably the photocopier in your own office. There's a little pattern of dots and if you make a photocopy, and you stick it up in what you think is an anonymous location, they can pull it down and find that little, tiny pattern of dots, and trace the photocopier right back to you.

So that's just one of many, many experiences that he has, where he says, "What in the heck is going on here? How do they know everything about me?"

C. Austin Fitts: Right.

K. Albrecht: I think it's a good wake-up call for people to really realize that these technologies that are so convenient, and that we take for granted, really have a sinister dark side, and that there are people that are availing themselves of that. You know?

It's not just a theoretical thing. This stuff really does happen, and pretty regularly.

C. Austin Fitts: We have one question I wanted to ask you.

K. Albrecht: Yes?

C. Austin Fitts: Because you're the person who got me to swear off Google forever.

K. Albrecht: Oh, good.

C. Austin Fitts: Somebody's always trying to talk me into some Google platform, and I'm always saying, "Never." I want to ask you more about search engines when we get to solutions. But, first, this question – let me read it to you. "I'd be interested in hearing Albrecht's comments about Petraeus's use of Gmail for his personal email, along with Broadwell's use of Gmail for her anonymous emails to and about Jill Kelly.

"The FBI was able to trace them and hence gain access to their other Gmail accounts and other people's Gmail accounts, leading all the way to General Allen in Afghanistan. Whoa. And these are national security professionals? Why are national security professionals using Gmail?"

K. Albrecht: Isn't that crazy? It is. And what I think is funny, Catherine, is your listeners probably know more about why to avoid Gmail than even General David Petraeus. It's a crazy thought. In April of 2010, Google really took off the velvet glove and revealed the fist inside of it. You know Google has been coming out with an incredible array of really useful products. And they're all free.

And the thing that people forget to ask themselves is: "Wait a minute. When was the last time a multibillion-dollar corporation gave me all of its products for free? There's got to be a catch."

And the reality is there is a catch. Those are not products. You're the product. And that's just the bait to get you to log on and reveal enormous amounts of information about yourself, so that they can put it all together.

C. Austin Fitts: Right.

K. Albrecht: And so in April, what Google did was – they announced what I'm referring to as kind of the "oneness policy," kind of like the Lord of the Rings – "one ring to rule them all." It's one privacy policy to keep track of everything.

So they explained this and said, "In the past, we've had all these different privacy policies for all of our different services. And we're just going to make it easier on you by consolidating them all into one privacy policy."

Well, what they really did, though, was said – all of the privacy policies that required them to keep your data confidential – that all bets are off now, and that they're going to consolidate everything they can find out about you, to get a centralized view of you from every source they can.

And one of the key places that – well, there are actually two key places where they get that centralized view of you. Number one is every time you type into the Google search engine. You're essentially logging on and typing into the global brain and saying, "Here's what's on my mind."

You know I think if back in the 1950's, Stalin had had the ability to require every person in the far-flung Soviet Union to log on 10, 15, 20, 30 times a day and download the contents of their brain into the Soviet Politburo, there would have been certainly an outcry in the West.

But we do the same thing today 15, 20, 30 times a day, every time we do a Google search. Because Google does not exist to give you the answer to all your questions. Google exists as an open question mark to say, "What are you thinking about now?"

And we log onto there, and we tell them, "Well, I'm thinking about having this for dinner. I'm thinking about checking out this particular dentist. Hey, I'm thinking about that rash. I can't figure out what it is.

"Hey, I'm thinking about the fact that my kid has a cold. I'm thinking about the fact that I may be losing my home, and I need to look at some mortgage options. I'm thinking about the fact that I may be addicted to prescription pain pills or some illegal drug. I'm thinking about the fact that my husband's having an affair."

I mean we type all these things, and we type them 5, 10, 15, 20, 30, 50 times a day. For a lot of people, Google is their home page. And for Google to be able to know what every person on the globe is thinking about that many times a day is an immense amount of power.

And believe me, it is not power that's lost on the world's governments. That's why the Chinese government hacked into Google – so that they could find the dissidents.

Because they know: if you want to find dissidents, who has the most information about everybody? And the answer is Google.

C. Austin Fitts: Right.

K. Albrecht: So that's the one place. And that's why we developed Startpage and ixquick, which are the two private search engines. We like to call them the world's most private search engines. I started off just interviewing the folks from ixquick, which is a meta search engine that takes your query and submits it to multiple other search engines, and then gives you the results.

And I fell in love with the company and wound up being their spokesperson. And now I'm a VP with the company. And then I helped them develop Startpage, which is a portal to Google results. So the IxQuick.com – that will give you results from everybody but Google.

And then Startpage gives you anonymized Google results, so that Google never sees you. They only see us. And we go and get Google results for you, without the tracking cookies. We don't record your IP address.

In fact, we make no record whatsoever that you've even been there. So even if there were a subpoena or, God forbid, a hacker or something like that, there would literally be nothing on our server to obtain. So that's the search engine.

And I recommend that everybody that's listening please tell everybody else. If you think about it, every time we say Google this or Google that, we are giving thousands of dollars of free advertising to this company, by using its name as a verb.

C. Austin Fitts: Right.

K. Albrecht: So we say Startpage around here. It was a hard habit to break. But we don't say Google it anymore. We say Startpage it.

And then the other piece is the Gmail program, which is the other place that Google gets an immense amount of information about us. And that goes even beyond what you type in the search engine.

Because what you write to people in email is really – oftentimes you'll put an attachment there. It might be your medical records. It might be your new business plan. If you send anything to or from a Gmail account, in the fine print, you are agreeing to allow Google to capture, read, correlate, collate, do whatever they want with the information in there.

And it belongs to them. And even if you delete it, they don't delete it. They own it forever. So I don't write to people with Gmail accounts anymore.

C. Austin Fitts: Oh, well that's a good idea. Yes. That's a good idea.

K. Albrecht: Well, I've got to stop – if someone writes to me from a Gmail account, I have to stop and look and say, "Anything that I reply, I have to be comfortable with sending it directly to Google and having it go in my dossier, in my entry."

And so I will never put anything about where I'm going to be, or my schedule, or my phone number, or any kind of addresses or anything. And oftentimes, I'll literally call the person up and say, "I'm so sorry. But unless you get another email account, I can't correspond with you about this sensitive topic. Because it's Gmail."

You know even my doctor – she said, "Yes. Send me your test results." And I said, "Sure." And she said, "Here's my email address." It was Gmail, so we had a little talk.

I don't want Google knowing that. So people who love Startpage and ixquick have really been clamoring for us to develop an equivalently private email.

And I think the whole Petraeus thing is really bringing this to the surface – that we need the ability to write private email. I'm not excusing what David Petraeus did. But certainly if I'm going to be writing to my doctor, I want the ability to send my medical records privately and know that nobody's going to see them.

C. Austin Fitts: Right.

K. Albrecht: So our Startmail product will be coming out in 2013. And if people would like to be on the beta test list, they can send an email to beta@startpage.com, and just say that you heard me on the *Solari Report*.

And you will get an automated confirmation that will put you on a list, and you'll get free access. As soon as it's available, we'll get you free access for a couple of months, to kick the tires and let us know what you think. And that'll be coming out pretty soon.

C. Austin Fitts: Okay. Well, I will definitely send one in personally myself. That's terrific. Okay. So now let's turn to RFID chips. How do we protect ourselves from this technology – maybe starting with the credit cards?

So I'm one of those people who walk around putting things in sleeves, including my passport.

K. Albrecht: Yes

C. Austin Fitts: Is that going to work? Is that going to help?

K. Albrecht: Yes. That is a good idea. They make RFID blocking wallets. And I would strongly recommend that everyone get one. You don't even have to go to that extent. There are places online – you can Startpage it, or you can make an RFID blocking wallet out of duct tape.

Aluminum foil - the tin foil hat crowd was right. You can block the transmission of radio frequency waves with aluminum foil. But it's not like kryptonite; just having a little bit there doesn't do it. You have to actually completely envelope the thing that is trackable with the aluminum foil.

So even if there's a little crack or a little opening, you can still have a transmission. So you want to be pretty thorough about blocking it.

The other thing you can do is – there's really no reason for you to need the RFID tag in your credit card. So you can deactivate it. You can call the company. They won't be able to deactivate the tracking capability of the tag. Because it's a live tag in your credit card.

But they can deactivate the contactless portion of it to be usable. And that doesn't really help you much, frankly. Because if somebody gets the number, they're not going to try to make a new contactless card and use it as a contactless card. They're just going to use the number as a regular credit card.

So I think that's kind of a cop out on the part of the credit card companies. The other thing you can do is – if you hold your credit card up to a bright light or hold a flashlight up to it, if you can locate the chip – it'll be like a square.

And then it'll have an antenna running around the edge. If you can locate where the chip is, you can either pop it out with a little powerful hole punch of a little awl. Those old-fashioned words.

C. Austin Fitts: Yes.

K. Albrecht: Or you can take a ball-peen hammer and just hit it several times really hard. The other thing you can do is put it in the microwave for about five seconds. And it will arc and spark and pop. Don't do that to your passport though. Because that's U.S. property, and damaging it can actually be a federal offense, believe it or not.

Your passport – this is the booklet passport – actually has a very short read range. That's only a read range of literally millimeters – maybe a couple of inches at most. And that is encrypted.

So the booklet passports, believe it or not, are among the more secure forms of RFID. It's those e-pass card and the credit cards that are such a problem.

C. Austin Fitts: Now if you do that – if you put your credit card in the microwave and sort of nuke the chip, will the credit card still work?

K. Albrecht: It will. Yes. The purpose of that chip is not so that your credit card can be scanned. The purpose of the chip is so that you can wave the credit card at one of these contactless credit card readers. And, again, that's just not what people are doing. So it hasn't caught on yet, despite the fact that they've been doing this like five years – putting these into credit cards.

I believe the industry did this on the basis of some research, which – I think the research is accurate. They found that people spend more, the less they have to actually see the credit card. And so the idea of the industry here was that: rather than you having to actually open your wallet and take out your credit card and take a look – and when you see that little credit card symbol, you remember your bill, and you go, "Oh, yes. Wait a minute. Maybe I shouldn't buy this."

They found that when people don't have to physically handle the card, they spend a lot more money – like 30, 40 percent more, in some cases.

C. Austin Fitts: Wow.

K. Albrecht: And they even tested this at a fast-food drive-in. They had a wave and go fast-food payment system that they tested. And they found that people were eating like 30 percent more calories, when they didn't have to actually take out money and pay for the food, when they were able to just kind of wave it, and not have to think about it. So all of that, I found just fascinating.

And I think the industry said, "Well, we make our money – we get a percentage every time a dollar is spent on the credit card. So if we can get people to spend more money, then we can make more money." So I think that's the reason.

It just really has not caught on – this idea that I could just take my purse and wave it in front of a reader. And right through my purse, you'd be able to get the ID number, and I'd never have to take my wallet out at all.

But I think if people began to really push for that, then you'd begin to realize how easy it would be for a hacker to read your number through your purse too. And I think that's the dirty little secret of these cards – is just how hackable and readable they are.

There's no security, no encryption. Your number is transmitted literally in the clear to anyone with a reader device who can get close enough to you to snag it.

C. Austin Fitts: One of our subscribers from Texas is very excited about this new email, and wants to know when the email service will be available from Startpage.

K. Albrecht: It's probably going to be spring of 2013. And you know we call Startpage the world's most private search engine. And Startmail really will be the world's most private email. And when I say private, I'm talking encrypted to the point where even we will not have access to your email.

C. Austin Fitts: Oh, that's wonderful.

K. Albrecht: And that's pretty exciting. We have come up with a way.

C. Austin Fitts: So you can turn around to the Department of Justice and say, "Well, we can't give it to you. Because we don't have access."

K. Albrecht: That's right.

C. Austin Fitts: Right.

K. Albrecht: The only way that they'd be able to access your email would be if they had physical access to your computer, or if they hacked your computer with a Trojan, so that they could watch what you were typing from your keyboard. But they're not going to be seeing it from us.

So to put that together – and we are using state of the art technology. This is 2013 level technology. And we've got a brilliant team of engineers over in Europe working on this.

I'm so excited, because they have left no stone unturned. They have tested every aspect of this. And it will be third-party certified, just like Startpage is, by both Certified Secure and EuroPriSe.

So we're going to go the extra mile, and not just tell you that it's secure, but have third-party independent audits verifying every single aspect of it as being secure.

C. Austin Fitts: Oh, that's wonderful.

K. Albrecht: So that's going to be coming out – as I said, it'll probably be sometime in the spring of 2013. It keeps getting delayed a little bit because we keep realizing that – "Ooh. We got to add this. And, oh, if we want it to be perfect, we've got to add that." So it's really just a process of fine-tuning a Ferrari here, I think.

C. Austin Fitts: Okay. One more question.

K. Albrecht: Oh. And let me just repeat. If people missed it, it's beta@startpage.com. And just say that you heard Katherine Albrecht on the *Solari Report*, and we'll go ahead and get you on the list.

I'm not sure how quickly that list is going to fill up, so I would encourage people to please go ahead and sign up. And we'll look forward to getting your feedback when it's ready.

C. Austin Fitts: One more question before we finish – a question from Kansas City. "What about Apple's iCloud system, relative to privacy?"

K. Albrecht: Ooh. Yes. Let's talk Apple for just a minute. When I think about what's being built right now – you know not to get too esoteric, but essentially we are building eyes and ears into the physical fabric of our world.

And as we build those eyes and ears – the eyes, of course, being the surveillance cameras, and the ears – a lot of these surveillance cameras – people didn't realize it, but they came originally equipped with microphones that just never got turned on. And now they're starting to turn the microphones on.

So you have bus departments, for example, that have put cameras onboard the buses. And now they're turning the microphones on too, so now they can listen to your conversation on the bus. So we're building eyes and ears into the world.

We're also building trackability into the physical objects in the world that can communicate with those eyes and ears. And the big question that all of the watchers have been asking – and we really featured this in our book *Spychips*, which – by the way, if you haven't read it, everybody please get a copy, even if it's just from the library.

Because everything we wrote about in 2005 and 2006 – it's all occurring exactly the way we wrote it. In fact, the book is more relevant and timely today than when we wrote it. Because we were so far ahead of our time. Not because we have any kind of magical skills, but just because we were reporting on what they said they were going to do.

And they're doing exactly what they said they were going to do, just like they said they were going to do it. So this idea that everything becomes traceable – they really cut to the chase, I believe, with all these Apple products.

Now instead of having to figure out – "Well, how do we get the RFID tags on the consumers, so that we can track them?" – you're already logging into the global brain multiple times a day through your smartphones – your Android smartphone and your Apple iPhone.

C. Austin Fitts: Now I just have to correct you – our cellmates, not our cell phones.

K. Albrecht: Yes.
C. Austin Fitts: You have to explain the new change in name.

K. Albrecht: Yes. I did a contest on the show. I said, "You know these aren't phones. We grew up with phones – the kind where you go – ring, ring, ring – 'Hello. Yes. This is Katherine. Oh, I'm fine. Thanks. Okay. Bye.' Click. Right? That's a phone."

But these addictive devices that you see people staring into all day long and getting injured thumbs using so addictively have really become the portal to the global brain. I did a contest on my show, and I said, "Let's come up with a new name. Because cell phone is not the right name for them anymore."

And we got some really great entries. I love the one "cellmate." It's your cellmate.

C. Austin Fitts: I thought that was great.

K. Albrecht: And the question I always ask is: how many bars do you have on your cell? We always say, "How many bars of antenna power there?" But yes, you have bars on your cell, and you're carrying your cell around with you, basically.

C. Austin Fitts: Right. Right.

K. Albrecht: You're a prisoner of our own cell there. So, yes, the cellmates that we're carrying around, and that we're using to essentially log into the global brain and report our position. And you'll see young people nowadays – in Minneapolis, they just were boasting on the RFID Journal that they had the biggest gathering of people tagged with RFID ever.

It was on a public street. It was 50,000 zombies, 50,000 people dressed up as zombies – and put an RFID wristband on their right wrist and walked around the streets of Minneapolis during the Pub Crawl. So they went from bar to bar drinking. And every doorway that they walked through tracked and monitored their location.

Now you would think that if you told these 20-something and 30-something young people, "Hey, you're being tracked through that RFID tag," they would say, "Ooh. Get this thing off of me." Right? Because isn't being young all about being free from surveillance and not monitored and watched in that way?

Well, they've found the way around that, which is by making it cool and hip and tying it in with Facebook. And so the latest thing now, with these big concerts – the Coachella concert in California being one of the first ones to do this – they actually have you – they put the RFID tag on your right wrist.

They fully tell you it's RFID. They completely tell you it's a trackable microchip. They even have you enter the event by pressing your right hand to a right-hand reader, which actually is a circle with a right hand in it. And you press your right hand up to the right hand reader, and you hear a beep, so you know you're getting read.

Well, now what they have people doing is logging in through Facebook portals. So all of the RFID event management companies, which have only been around for like a year and a half – this is really new, but it's really taken off – is they put up these huge Facebook portal, billboard, kiosk kind of things.

And so the Coachella Festival, for example – it's a big music festival out in the middle of nowhere in the desert of California. As people drove up to the Coachella Festival, they had the Indio police create a barricade a mile around the event, and stop all vehicular traffic that was going towards the festival, and made everybody in the car roll down the window and stick their right hand out of the car, so that the police could scan all of their RFID tags before they were allowed to proceed.

So this is young people getting conditioned to police checkpoints checking their RFID tags on public streets. And these were police. This was not private security. They somehow enlisted the local police to do this.

C. Austin Fitts: Right.

K. Albrecht: When you get to the event – so you fully know that police are scanning you. When you get there, they have a whole bunch of different stages. It's kind of like Woodstock. And so as you go to each different stage, everybody was walking up and cueing, standing in line to press their RFID reader up to this Facebook kiosk to give an update of their location on social media, so that their friends could see where they were.

So far from what you and I, Catherine, might think – that young people would be appalled at the idea of being tracked and monitored in this way, they've made it cool, so

that they stand in line to report their location, so they can be tracked and monitored. It's really crazy.

C. Austin Fitts: One of the things, and it's a much longer conversation, but one of the dangers of this kind of technology is the ability for the system to use it to harvest you financially.

So when you adopt and agree to be tracked like this and to live in a no privacy world, what it means is you're competing in the marketplace with people who have complete privacy, but also have complete access to your data, which means that intelligence can be used to out game you constantly. And so, to me, it's very much a financial issue, and tremendously diminished your ability to basically build financial security.

It's a much longer, deeper conversation. But when it comes to both your purchases, but also your investments, it really gives the top of the financial system a way to game you in dramatic ways that, really, it's very hard for you to understand or fathom.

K. Albrecht: Well, I'll give you just a really practical example of that. Marty Abrams, who is a consultant for the retail industry, he actually talked about in retail stores – these are the very face-to-face kind of financial transactions - but actually identifying shoppers, so that you could offer higher prices to the undesirable ones.

C. Austin Fitts: Right.

K. Albrecht: So they're not just wasting your time and pushing a cart and breathing your air. So that they actually become valuable, you charge them higher prices or offer them poor service.

Bank of America actually designed a system where the bank card that they issue you would have an RFID tag in it. There would be a reader device in the door as you walk in, and it would send a message to the teller as to who you are and what your bank account was, so that they could decide whether to just close the window and make you go to the ATM machine, or have the bank president come out with a glass of wine in his hand and invite you back into his office.

No longer do we just walk around making our own decisions about who knows our financial circumstances. But we would be beaming them out, so that people could use them to take advantage of us.

C. Austin Fitts: Right. One more question, just because one came in that's very good. "Your cell phone SIM chip has the same issues. It seems more intrusive."

K. Albrecht: Yes. There are interesting laws that cover cell phones, in ways that – RFID is the Wild West, and RFID is not covered. But the lines are beginning to blur a little bit. I am truly concerned about what's happening with the cell phones.

The cell phone is no longer a phone. It's now become an Internet portal. It's now become a GPS Wi-Fi, blah, blah, blah, Blue Tooth – I mean we are emitting so many things as we walk around with these little cellmates, these little link lords or whatever you want to call them – these cell phones.

C. Austin Fitts: Right.

K. Albrecht: But I think no longer is the issue really even going to be the SIM card in your cell phone or your phone emissions. I think that these phones are actually going to become your keys, your wallet, your payment system, your loyalty cards, your membership cards, your everything else.

And, again, it's just like these kids going up and pressing their right hands to the Facebook portal. Your phone is going to be something that you are actively using to identify yourself and show the world that you're there.

C. Austin Fitts: And, of course, the danger is what the banking system wants, more than anything, is a global digital currency.

K. Albrecht: Oh, yes. And they're going to do it through the phone.

C. Austin Fitts: Yes. They're going to do it through the phones. And that's why the Google and Apple wallet scare me to death.

K. Albrecht: Yes. And the watch word you want to look for here is NFC or "near field communication." That's the phrase you want to be looking for. Because that's the – NFC payments is really going to be the payment system of the future, and it's all going to be based on the cell phone.

Because now we're up to like 80 percent cell phone penetration in the population. And any time you hit 80 percent – this is kind of my little rule of thumb – any time you hit 80 percent voluntary cooperation with really anything, then you can push the other 20 percent onboard by mandating it, by giving them no other choice.

And we've hit that penetration level with the cell phones now. So I think it's coming, and probably quicker than we think, that we are going to see financial transactions moving over on to the cell phone. And it is a form of RFID.

C. Austin Fitts: Right.

K. Albrecht: It all kind of blurs a little bit because you are using radio waves to transmit an ID number. And, again, it's going to be less about the inadvertent trackability of your cell phone, and more about the intentional – "Hey, here I am. And let me send out my signal."

C. Austin Fitts: Well, Dr. Katherine Albrecht, as usual, you've given us much to think about and many good actions we can take. Just take a second and go through your websites and your radio show, and how we can stay in touch and just be kept apprised of your work, and how we can support you.

K. Albrecht: Absolutely. Thank you so much for that. Well, let's see. The ones that I've mentioned so far are Startpage.com and ixquick.com, the world's most private search engines. I encourage people to – if you have Google as your home page, please take the needle out of your arm.

Get un-addicted. Make the transition over, and make either Startpage or ixquick your home page instead. There also is a way to install them into your browser. So in that upper right-hand corner – you know you have that little Google search window. You can install Startpage or ixquick there instead, so that you can conveniently do the searches right from your browser.

So I would encourage people to definitely do that, and also to send an email to beta@startpage.com to get our private email, when it comes out. The anti-animal chipping website is ChipMeNot.com. There's a lot of very sad stories and pictures of all the animals that have been unfortunately microchipped, and had problems because of that, and died of cancer and other things.

We also have a tremendous amount of evidence there about implantable microchips causing cancer. That's ChipMeNot.com. Our battles against human microchipping, including a 40-page FAQ on implantable microchips, for free, is available at AntiChips.com. And there, you can see our protest against the chipping of the Alzheimer's patients, which got that stopped.

My home website is kmashow.com. It's actually katherinealbrecht.com. But there are so many ways to spell that, so I just said, "kma." Those are my initials. kmashow.com is my radio show website and also my personal website. You can sign up for the radio show website there.

You can also find five and a half years of radio archives. I do a daily radio show. You can search it. There's a little Startpage search window right at kmashow.com.

Oh. And by the way, any webmasters out there, people who run their own websites – if you have Google search on your website, you are transmitting to Google information about every single person who lands on your website and clicks that search box. So please get rid of your Google search box on your website and replace it with a Startpage search box because you can easily make that transition and protect people's privacy.

kmashow.com archived five and a half years of archived radio shows. And, also, a live stream every day. My show airs Monday through Friday, 4:00 to 6:00 p.m. Eastern Time, and also on Saturdays, right through the lunch hour, from 11:00 a.m. to 1:00 p.m. Eastern.

And, again, that's at kmashow.com. And then our anti – well, I guess our Spychips book website, which I share with Liz McIntyre, is at Spychips.com.

And then, finally, the school chipping campaign that we are running right now – we are looking for donations. So if people would like to help out, we would like to do an automated phone dialing system all across San Antonio, to get parents apprised of what's happening there. And we need funding for that. That is at ChipFreeSchools.com. Boy, that's a lot of websites.

C. Austin Fitts: It is a lot of websites. If you could just mention to buy the documentary. I want to make sure that everybody knows this is done – *Shadow Government* is done from a Christian perspective.

K. Albrecht: Indeed it is.

C. Austin Fitts: Yes. And if you could just tell them how they can get a copy of *Shadow Government*.

K. Albrecht: Well, let's see. I have signed copies available on my website. And you can also find them wherever fine products are sold. I think it's available through Amazon. You can also look up shadowgovernmentmovie.com – I believe is the website. shadowgovernmentmovie. You can previews of it, if you want to.

Somebody posted it up on YouTube too. So I don't usually encourage people to do that. But I think it's so important that you get the information. That really trumps even that you purchased the film. But we would encourage you to do that.

So yes. shadowgovernmentmovie.com. YouTube. Amazon. It's all over the place. And, also, my website –kmashow.com. The nice thing about that movie is that it's not really a Christian film until probably the last five minutes of the film.

And I am a Christian. I believe that all of these technologies are part of the fulfillment of Biblical prophecy.

C. Austin Fitts: Right.

K. Albrecht: So that's something I've been pretty outspoken about for many years now. And I like the fact that in that film, we were able to put together a secular case.

And by the time you get to the end of it, you're really biting your nails down to the quick, going, "Oh, my gosh. What do we do?"

C. Austin Fitts: Right.

K. Albrecht: It feels pretty hopeless. And, fortunately, there is that message of hope at the end, of – "Hang on a second. This was all predicted 2,000 years ago. And not only are the scary parts of the Bible true, but the promises of the Bible are true as well." So there's hope.

C. Austin Fitts: Well, I'm a Christian as well. The reason I mentioned that is I always have a group of subscribers who've had very traumatic experiences at the hands of the Christian Church.

K. Albrecht: Indeed.

C. Austin Fitts: And so whenever I recommend something that's Christian, and I don't warn them ahead of time, they just go ballistic.

K. Albrecht: Hmm. Yes. And the thing about the movie – if you turn it off before the last five minutes, you won't even notice that it's a Christian film. It's literally – as you see Grant Jeffrey begin to walk under the trees in those last five minutes of what's an hour and a half movie, that's when you're going to get that message.

He holds up a Bible, and it's pretty obvious what's coming. But I do find that message hopeful.

C. Austin Fitts: Yes, it is hopeful. So open your mind.

K. Albrecht: Yes.

C. Austin Fitts: Listen to the whole thing. Okay. Well, Dr. Katherine Albrecht, as always, it's been a pleasure. Thank you so much for joining us on the Solari Report. Thank you for everything you're doing.

And just keep us posted on how we can support you, and we'll continue to promote all of your good works and your websites. But keep us in mind because we want to see you enjoy every success.

K. Albrecht: Thank you so much. And I think the world of you. And I'm so delighted that you had me back, and it truly is an honor to speak with you. Thank you so much, Catherine. God bless you.

C. Austin Fitts: God bless you.