

MICROFILM DIVIDER

OMB/RECORDS MANAGEMENT DIVISION

SFN 2053 (2/85) 5M



ROLL NUMBER

DESCRIPTION

2415

2007 SENATE JUDICIARY

SB 2415

2007 SENATE STANDING COMMITTEE MINUTES

Bill/Resolution No. **SB 2415**

Senate Judiciary Committee

☐ Check here for Conference Committee

Hearing Date: January 31, 2007

Recorder Job Number: 2425

Committee Clerk Signature *Maria L Solberg*

Minutes: Relating to implanted microchips in individuals.

Senator David Nething, Chairman called the Judiciary committee to order. All Senators were present. The hearing opened with the following testimony:

Testimony In Support of Bill:

Sen. Randy Christmann, Dist. #33 introduced the bill. (Meter :45) This bill speaks for itself once you get to the point of the reason of the bill. He explained his journey of the bill, implanting livestock to driving a gravel truck for the county (truck having a "key card" monitor.

Sen. Lyson questioned (meter 4:20) how would this effect electronic monitoring on sex offenders? The committee discussed electronic bracelet's verse an implanted devise.

Sen. Nething stated the concerns of the bill are the employee and the employer only.

Discussion of the Federal Law

Sen. Lyson spoke of (meter 8:59) currently they implant chips in newborns. Would this bill prohibit this? No they have the consent of the parents.

Jim O'Shanigh, Dist. #31, (meter 11:18) Gave Testimony – Att. # 1

Steve Bitz, Attorney in Bismarck with Civil Libertarian concerns. (meter 19:13) Addressed the "product side of bill, spoke of U.P.C. codes and a 36 number microchip for individual products.

Discussed the human aspect of assigning I.D. numbers with a 33 bit chip, long term health

aspects and privacy issues. Spoke of reasons one may make a requirement comparing it to credit cards and car rentals. Spoke of current law. (meter 24:36) and how it would not protect you from this.

Sen. Olafson questioned the civil liberties of a person on parole or probation. Criminal have given up there liberties. Mr. Bitz does not believe they should have a chip either. This is a civil liberties interest that all should be free in there person. It would be an invasion of ones body. Discussion of this.

Sen. Marcelles spoke of homeland security and going through security systems for example airports. National I.D. card is what will be used at that time. Sen. Nething spoke of how he goes through security and shows them his card. Discussion of doing something voluntarily verses mandating.

Irma Bitner, Registered Nurse (meter 30:12) gave testimony – Att. #2

Testimony in Opposition of the Bill:

None

Testimony Neutral to the Bill:

None

Senator David Nething, Chairman closed the hearing.

2007 SENATE STANDING COMMITTEE MINUTES

Bill/Resolution No. **SB 2415**

Senate **Judiciary Committee**

☐ Check here for Conference Committee

Hearing Date: February 7, 2007

Recorder Job Number: 3055

Committee Clerk Signature	<i>Maria L Solby</i>
---------------------------	----------------------

Minutes: Relating to implanted microchips in individuals.

Senator David Nething, Chairman called the Judiciary committee to order. All Senators were present. The hearing opened with the following committee work:

Sen. Lyson made the motion to Do Pass SB 2415 and **Sen. Olafson** seconded the motion.

Reviewed the original hearing (meter 1:00) Spoke of no opposition, it would allow a parent to implant a child, and discussion of "ankle bracelet's". This is a bill that will change as technology changes; this is an employee protection bill. Definition of a person was reviewed. (meter 3:14) 12.1-15.

All members were in favor and the motion passes.

Carrier: **Sen. Lyson**

Senator David Nething, Chairman closed the hearing.

Date: 2-7-07

Roll Call Vote # 1

2007 SENATE STANDING COMMITTEE ROLL CALL VOTES

BILL/RESOLUTION NO. 2415

Senate _____ Judiciary _____ Committee _____

☐ Check here for Conference Committee

Legislative Council Amendment Number _____

Action Taken Do Pass

Motion Made By Sen. Lyson Seconded By Sen. Olafson

Senators	Yes	No	Senators	Yes	No
Sen. Nething	✓		Sen. Fiebiger	✓	
Sen. Lyson	✓		Sen. Marcellais	✓	
Sen. Olafson	✓		Sen. Nelson	✓	

Total Yes 6 No 0

Absent 0

Floor Assignment Sen. Lyson

If the vote is on an amendment, briefly indicate intent:

- a. For a tax exemption, within eighteen months after the month in which the first incremental oil was produced.
 - b. For a tax rate reduction, within eighteen months after the end of the period qualifying the project for the rate reduction.
5. To receive, from the first day of eligibility, a tax exemption or the reduction on production for which any other tax exemption or rate reduction may apply, the industrial commission's certification must be submitted to the tax commissioner within eighteen months of the completion, recompletion, or other qualifying date.
 6. To receive, from the first day of eligibility, a tax exemption under subsection 6 of section 57-51.1-03 on production from a two-year inactive well, the industrial commission's certification must be submitted to the tax commissioner within eighteen months after the end of the two-year inactive well's qualification period.

If the industrial commission's certification is not submitted to the tax commissioner within the eighteen-month period provided in this section, then the exemption or rate reduction does not apply for the production periods in which the certification is not on file with the tax commissioner. When the industrial commission's certification is submitted to the tax commissioner after the eighteen-month period, the tax exemption or rate reduction applies to prospective production periods only and the exemption or rate reduction is effective the first day of the month in which the certification is received by the tax commissioner."

Renumber accordingly

REPORT OF STANDING COMMITTEE

SB 2405: Transportation Committee (Sen. G. Lee, Chairman) recommends **DO NOT PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2405 was placed on the Eleventh order on the calendar.

REPORT OF STANDING COMMITTEE

SB 2415: Judiciary Committee (Sen. Nething, Chairman) recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2415 was placed on the Eleventh order on the calendar.

REPORT OF STANDING COMMITTEE

SCR 4016: Natural Resources Committee (Sen. Lyson, Chairman) recommends **DO PASS** (7 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SCR 4016 was placed on the Eleventh order on the calendar.

REPORT OF STANDING COMMITTEE

SCR 4023: Judiciary Committee (Sen. Nething, Chairman) recommends **DO NOT PASS** (4 YEAS, 2 NAYS, 0 ABSENT AND NOT VOTING). SCR 4023 was placed on the Eleventh order on the calendar.

FIRST READING OF HOUSE BILLS

HB 1045: A BILL for an Act to create and enact a new subsection to section 11-18-03 and a new subsection to section 38-18.1-06 of the North Dakota Century Code, relating to filing of a statement of succession in interest to abandoned minerals; and to amend and reenact section 38-18.1-02 of the North Dakota Century Code, relating to filing of a statement of succession in interest to abandoned minerals.

Was read the first time and referred to the **Judiciary Committee**.

HB 1048: A BILL for an Act to create and enact chapter 38-13.1 of the North Dakota Century Code, relating to trusts for unlocatable mineral, leasehold, and royalty interest owners; and to repeal chapter 38-13 of the North Dakota Century Code, relating to execution of oil and gas instruments affecting interests owned by absent persons.

Was read the first time and referred to the **Judiciary Committee**.

The Senate stood adjourned pursuant to Senator Christmann's motion.

William R. Horton, Secretary

2007 HOUSE JUDICIARY

SB 2415

2007 HOUSE STANDING COMMITTEE MINUTES

Bill/Resolution No. SB 2415

House Judiciary Committee

☐ Check here for Conference Committee

Hearing Date: 3/13/07

Recorder Job Number: 4945

Committee Clerk Signature

W Penrose

Minutes:

Vice-Chairman Klemin: We will open the hearing on SB 2415.

Sen. Randy Christmann: Sponsor, support this bill. This proposal was brought to me by some citizens, and I had never heard of this possibility really. Then as I got to thinking about it more, it sort of made some sense to me, that this technology as it progresses, that we want to make sure that things that seem bizarre don't start happening here. We can get leveraged into a lot of things by employer/employee relationships. There was a situation that really happened and got me thinking that it could happen again, when someone has authority over someone else they could require it. In a truck that I drove, there was a round steel wheel lug size object on the back of the cab wall. There was a key opening on there. I asked what those were and I guess years before that, apparently they were common, because you could buy these things on the market, there was a little card that went in there and somehow turned and during the day, as you were driving, that key kept turning and was marked in there, so at the end of the day the boss checked to see on the keyed log if there were any long spots besides your lunch and breaks where you weren't driving, and if you were taking a break. Well, in modern times, a person in authority, who wanted to monitor his employee's work habits, it does seem kind of ought there maybe, but it is possible. Just because someone does have authority over you,

doesn't mean that anyone ought to feel that they are required to subject themselves to implants or anything like that, where your employer could monitor you and find out where you are when you are off duty. It made sense to me, and I see no reason why we would need to not have this and that it could prevent some troubles in the future.

Rep. Meyer: I'm very familiar with how this works with cattle. I guess when they have the implants, they go to the scale, you can tell where they were born, and information such as that. Are you saying with these, they have tracking capabilities, because you don't have that with cattle now, because it reads through a scanner.

Sen. Randy Christmann: First of all, with livestock, I think it is limited by cost. You can be tracked by your cell phone. So I don't know what the technology is for animals, but if the chip in your cell phone can track you, certainly a chip that can be implanted into you, I would think that if not now, in the very near future would be able to. I think it could be for cattle too, but the cost would be very high.

Rep. Onstad: A person may not require, does that also cover a state agency or corrections department. Sometimes there is a definition for that.

Sen. Randy Christmann: I would leave that to the wisdom of the Judiciary Committee. I told the Senate Judiciary committee the same thing. I would think that it would probably prohibit corrections from doing that, but I'm not sure of that. If the time came, and we wanted to exempt that because that was a good way to manage criminals, I wouldn't have any problems about trying to exempt them. I do think, though that it is unlikely that federal guidelines would ever probably allow us to do that. We're not able to do chemical castration of rapists, etc. We're not able to do things to people surgically, to criminals. I am kind of doubtful that we could do that anyway.

Rep. Wolf: What about a person covering corporations, what about if the microchip contained a radio frequency identification device, would that cover the GPS tracking or are we limiting this bill to just an identification microchip versus what could come in the near future, or we're not there yet.

Sen. Randy Christmann: I think radio frequency identification device would cover most everything that would allow someone to track you. I can't think of an example of something that wouldn't fall into that category. I think it covers it.

Rep. Klemin: Thank you. Further testimony in support.

Jim Oshanyk: (see attached testimony). On IV, on RFD's I thought it very appropriate that it was the last one on the page. He summarizes the whole thing very well. I would like to have you read that on your own time and so my main purpose of testifying this morning was to try and give you some documentation and tell you what it going on.

Rep. Wolf: I have a question about Alzheimer's, diabetes, etc. that a chip could be put into the arm and a hospital would have a scanner that would enable the doctor to know what is wrong if a person couldn't tell you their name, etc. if they were unconscious. So if there were medical concerns, could this be helpful.

Jim Oshanyk: There's good and bad in everything. You have some of both right here. We just feel that we want that privacy and whatever. I would just like to point out to you, in the highlighted portions, these are taking off more quickly in other countries. The Ministry of Health is testing these in hospitals there. But these are being used here for other things, such as complete financial transactions. I didn't cover this in my notes, but in my reading about chips, I read that down the road, you know Wal-Mart and all the big stores have them, and they are going to have it so that when you walk into a bank and you have a Visa/MasterCard, they'll say Good morning, Mr. so and so and they will be able to tell if you have a lot of money in the

bank, etc. I really don't like that. We just ask your support on this. This is a preventative thing, it's not going to cost anybody anything, but it is one step to put the brakes on.

Rep. Koppelman: As I look at this bill, is a class A misdemeanor enough of a deterrent.

Jim Oshanyk: Maybe what will have to be done is amend it, we designed a certain bill that went into the Senate Judiciary committee, this is what they came up with and maybe you will want to go a step farther and make the penalty heavier.

Rep. Klemin: Let me ask you a question. Let's say we've got an example, and this relates back to what Rep. Wolf was talking about. Let's say you have a parent with Alzheimer's and you are the guardian of that person. This parent is then in an institution where they can keep track of your parent. This bill says a person may not require another individual to have this device implanted. But this wouldn't preclude someone like you, as the guardian, from voluntarily agreeing with the institution that your parent could have this chip in order for them to be able to monitor your parent's activities better. Do you see this applying in that situation.

Jim Oshanyk: Well, it could be. There has to be a little give and take in how serious the proposition is. We're looking at this picture as an overall. It's even been brought up about prisoners and sex offenders. That means that they're not going to get this, we thought that you can put bracelets on their ankle or arm or whatever and do the same thing. We're trying to look at this problem overall, so that we can be free to walk around and do whatever we want. In regard to the question about the cattle, the cattlemen in SD, they're in protest. They really are. As far as that program is, it's any chickens, any cows, any horses, any pigs, whatever, it's got to be reported. Let's say you're a rodeo fan and you take your horse and go to Wyoming or Medora, you've got to call into this database and tell them that you're doing that. We're not doing anything wrong, why should we have to report in like this.

Rep. Klemin: Thank you. Further testimony in support.

Steve Bitz, Attorney: I am a resident of Bismarck and reside in District 47, which is the district of Rep. Klemin. There are three areas that I would like to discuss this morning: 1) health impacts; 2) privacy issues and 3) civil liberty issues. Before I get into my testimony, I thought I would address the question you had asked about the minor child. My perspective on that would be that a parent would be able to give informed consent, and have it done, even if this bill were passed. Before I get into the details of the technology that is driving my concerns this morning, and a lot of the legislation that has been passed or has been considered in other states and that is two-fold. First of all there is a product identification aspect and also a human identification aspect to it. As many of you are probably aware, back in the 1970's the Uniform Product Code that put an identification code on each product, the merchant marked for each individual sale. This particular box of tea that I have here is not going to appear any different on the scanner than the same similar box of tea that has the same number on it. One bottle of Coke is the same as another bottle of Coke. Massachusetts Institute of Technology and 103 of the largest multinational corporations have proposed changing that product identification system from going from Uniform Product Code to a Product ID code. What would happen is that each individual product would be implanted with a separate microchip, then everyone's product could be the same product but have different UPC code, so you could track where it went, who bought it, etc. They are going to do that by implanting a radio frequency identification device with a certain number of bytes within that device. A 23 byte device would allow the corporation or company to identify each and every car that was produced in the world; a 29 byte chip could identify every computer; 33 bit chip could identify every human, 54 byte chip – every grain of rice, which obviously isn't going to happen, and the 96 byte chip would allow us to number every grain of sand on the face of the earth. Obviously, this is not the objective, but just to give you some information on how that would work. Our concern here

is not so much with the product identification part of it, as it is with the human aspect of that.

The auto identification center which is the organization of these corporations at MIT, has also suggested in addition to changing just that, that we have a pervasive global system of identification networks everywhere. Basically meaning that with these tracking devices as you are walking into Wal-Mart or Target they would be able to tell, if these things were implanted in your clothes or shoes, exactly what size clothing and shoes you were wearing. They would be able to identify what you are wearing, and so forth. In addition to that, with SmartCards, they would be able to identify how much money you have in your accounts. We're not getting into that issue, but the technology is certainly available. So we're not dealing with science fiction issues here, it is definitely available. My concern this morning is the human identification

aspect of that. It has been suggested already, that not too long ago, by former Secretary of Health and Human Services, Tommy Thompson, that every American should be implanted with a microchip to link their medical records and that military dog tags should be replaced with a Verichip implant. So conceptually the ideas are out there to do that. Now the question is, whether or not, people should have the opportunity to be implanted with the microchip. This bill is not dealing with taking away the right for someone to give informed consent. My first concern is obviously the health impact on this. We do not know at this point what health consequences are of having the microchip implants. Radio identification devices implanted under the skin have antennae and they actually receive a radio frequency signal, they respond back, and shoot through the skin and back and forth. We do not know what the health impacts of that result in, we don't know if it is safe at this point. The next issue would be privacy issues. If you had a microchip, you don't know at any given point whether or not that microchip is being read or if it's giving off data about you. So that can be done without your knowledge.

The third issue would be civil liberty concerns. Folks should have a right to be secure in their

person and possessions. I guess the question would be, what is the likelihood that the microchip implant would be required to participate in commerce or to enroll in the university or to obtain government benefits or those types of things in the future. One point that I would like to make right now, even with our currency, it says that it will pay for all debts public and private. You can go to certain computer stores now that will not accept cash, and I'm not just talking about over the internet, you actually have to pay with a credit card. As a United States citizen, obviously, we should be able to pay with that currency. So what is the likelihood, at some point in the future, that it could be required that people have a microchip in order to participate in commerce or to have access to services. That would be my concern. The other question that was asked, is this bill comprehensive enough, does it deal with all the issues. I don't think so. I think it is a starting point. I actually had looked at some other language, but I didn't bring it in, simply because I thought well we're better off starting with something than nothing at all. I think there are other issues that need to be addressed. But I think this is a starting point for us.

Rep. Dahl: If someone were to have a microchip implanted in you without your consent, wouldn't that already be a battery.

Steve Bitz: That's a good question. Wouldn't common law in statutory doctrines of battery and engaging in privacy apply in this situation. My response to that would be, that the burden is on the person being wronged. For example, if somebody wrongfully implanted a chip in me, the burden would be on me to go and prove my case in court. I would have to prove that this happened. This particular bill provides a penalty and really puts the burden on the wrongdoer. I think it specifies and makes it more clear in statutory form opposed to common law doctrine.

Rep. Klemin: Thank you. Further testimony in support.

Irma Bitner, registered nurse: (see attached testimony). I don't want to have mandatory implantation of the verichip.

Rep. Klemin: Thank you. Further testimony in support.

Alfred Schultz: Support. This is an invasion of privacy and of our rights. I would hope that you would vote against it. You have heard all kinds of arguments about it this morning. I am in favor of the bill.

Rep. Klemin: Thank you. Further testimony in support. Testimony in opposition or neutral. We will close the hearing.

2007 HOUSE STANDING COMMITTEE MINUTES

Bill/Resolution No. SB 2415

House Judiciary Committee

☐ Check here for Conference Committee

Hearing Date: 3/14/07

Recorder Job Number: 5028

Committee Clerk Signature

D Penrose

Minutes:

Chairman DeKrey: We will take a look at SB 2415.

Rep. Klemin: We spent a lot of time on this three line bill.

Rep. Koppelman: I move an amendment, I would like to change it from a class A misdemeanor to a Class C felony. I just think a class A misdemeanor, if you are going to do this, we make it a stronger penalty.

Rep. Klemin: That's actually a year in jail, is not a minor thing.

Chairman DeKrey: Shouldn't we say that they may not do it unless ordered by a court. We may have sexual predators, we have felons out there, and this could be a law enforcement tool. I just don't think that we should absolutely nix it completely.

Rep. Dahl: I don't think you can do this right now.

Chairman DeKrey: I don't think so either.

Rep. Klemin: I would say that technology, for the court to order that, is way off yet. We're just getting to GPS bracelets.

Rep. Meyer: One of the things that this can be used for are for parents and grandparents with Alzheimer's. In just visiting with a few people the other day, if you have a parent that has Alzheimer's and the language in here says you can't, as the child get this for your parent.

Rep. Klemin: We had several people that testified that this does not preclude informed consent, does not preclude voluntary implantation. This does not preclude a guardian from authorizing this for their ward.

Rep. Meyer: But does this language say that, the language doesn't say that.

Rep. Klemin: It says "you may not require somebody to do that", and requirement vs. voluntary.

Rep. Meyer: If I'm a child that wants to have that into a grandparent or parent that has Alzheimer's, that person may not give you that consent. That was my point.

Rep. Kretschmar: You would have to be a guardian.

Rep. Klemin: You would have to have a guardian appointed to give that consent. If they are incompetent, they have to have a guardian anyway.

Rep. Wolf: When it says that a person may not require, does a person cover corporation, etc. is that written in the code. When I look at the bill for Washington and Oklahoma, some are defining what person means.

Rep. Klemin: We have a definition, that's why every time you see one of these bills where the legislative council gets to go in and change words around, where it may have said person before, but you meant an individual, they always changed that to the word individual. That's why on line 7, you'll see the word "individual" there. So person means a natural person, or any kind of legal entity.

Rep. Wolf: It talks about the violation as a class A misdemeanor, which is a year in jail. But in the other states, it talks also about a year in jail or a fine of up to \$10,000. Do we want to put anything in about a fine.

Rep. Klemin: A class A misdemeanor, it is already in the alternative under our penalties.

Rep. Wolf: Is it \$10,000 fine.

Rep. Klemin: It is 1 year in jail or \$2,000 or both.

Rep. Wolf: We don't want to increase the fine on that, can we increase the fine.

Rep. Klemin: Well, we could by

Rep. Wolf: Could we leave the year in jail but increase the fine.

Rep. Klemin: I don't believe you can.

Rep. Kingsbury: I don't want to go this direction, I am going to vote against this.

Chairman DeKrey: Is there a second to the Koppelman motion.

Rep. Koppelman: In that case, I move a Do Pass.

Rep. Griffin: Second.

7 YES 6 NO 1 ABSENT

DO PASS

CARRIER: Rep. Koppelman

Date: 3/14/07
Roll Call Vote #: 1

2007 HOUSE STANDING COMMITTEE ROLL CALL VOTES
BILL/RESOLUTION NO. 2415

House JUDICIARY Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number _____

Action Taken Do Pass

Motion Made By Rep. Koppelman Seconded By Rep. Griffin

Representatives	Yes	No	Representatives	Yes	No
Chairman DeKrey	✓		Rep. Delmore		✓
Rep. Klemin	✓		Rep. Griffin	✓	
Rep. Boehning	✓		Rep. Meyer		✓
Rep. Charging			Rep. Onstad		✓
Rep. Dahl		✓	Rep. Wolf		✓
Rep. Heller	✓				
Rep. Kingsbury	✓				
Rep. Koppelman	✓				
Rep. Kretschmar		✓			

Total (Yes) 7 No 6

Absent 1

Floor Assignment Rep. Koppelman

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE (410)
March 14, 2007 10:48 a.m.

Module No: HR-48-5271
Carrier: Koppelman
Insert LC: . Title: .

REPORT OF STANDING COMMITTEE

SB 2415: Judiciary Committee (Rep. DeKrey, Chairman) recommends **DO PASS** (7 YEAS, 6 NAYS, 1 ABSENT AND NOT VOTING). SB 2415 was placed on the Fourteenth order on the calendar.

2007 TESTIMONY

SB 2415

*Sen
to
House*

*HH #1
1-31-07*

Senate Bill 2415

I. I would like to thank the chairman and his committee for allowing me to speak in favor of this bill.

II. As of now there are 7 states that have introduced or considered legislation in 2006 related to RFIDs.

A. Rhode Island which considered a bill to restrict the use of RFIDS for the purpose of tracking the movement or or identity of an employee, student or obtaining a benefit or services. (1)

B. New Hampshire legislature passed a law on May 24, 2006 creating the Commission on the use of Radio Frequency Technology to study the benefits and potential privacy implications. (1)

C. In Georgia, a resolution was adopted on March 28-06 to create the House Study Committee on Biological Privacy. (1)

D. Legislation was introduced in New Jersey on May 15, 2006, to prohibit requiring an individual to have a microchip implanted, to require an informed written consent before implantation, and to entitle those implanted to have the microchip removed at any time. (1)

E. The state of Washington is presently working on legislation. (2)

F. Wisconsin has passed Wisconsin Act 482. (3)

G. I am proud to say North Dakota's Legislature is currently considering the Implanted Chip.

H. Colorado has a bill which will become effective on 9-1-2007. (4)

I. Oklahoma is presently working on a bill. (8)

J. In all there have been at least 17 states working on RFIDs. But not all of the states have worked on implants. (1)

III. CHIPS CURRENTLY IN HUMANS:

A. Two U.S. Employees were injected with RFID Microchips at company request. This was done at Cincinnati, Ohio. (5A)

B. An officer in Mexico had himself and 200 people injected with the chip. (5B)

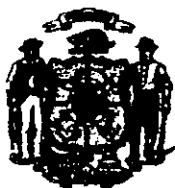
C. Chips could be used in hospitals, schools, and prisons. November 12, 2005 In Chattanooga, Tenn. People with mental retardation are being offered a device that could save lives in case of medical emergency. It's a microchip that would be implanted under the skin. But there are questions about this cutting-edge technology

**to people who can't make decisions for
themselves . (6)**

IV. Privacy concerns and Summary

(7)

I thought Monbiot on RFIDS was very appropriate .



Legislative Briefs

from the Legislative Reference Bureau



Legislative Brief 06-13

June 2006

HUMAN MICROCHIP IMPLANTATION

2005 Wisconsin Act 482, passed by the legislature and signed by Governor Jim Doyle on May 30, 2006, prohibits the required implanting of microchips in humans. It is the first law of its kind in the nation reflecting a proactive attempt to prevent potential abuses of this emergent technology.

BACKGROUND

Microchip implantation technology has been widely used for pets and livestock for a number of years, but has only recently been developed for human use. In October 2004, the U.S. Food and Drug Administration (FDA) cleared a radio frequency identification (RFID) microchip for medical use in humans. It is made by VeriChip Corporation, to whose board of directors former Governor Tommy Thompson was appointed in July 2005. Currently, human RFID implantation is used for medical records, a form of identification, and as a timesaving device.

Medical Records. The technology used by VeriChip allows a hospital with a special scanner to read a unique medical identification code in the microchip. Medical personnel can then input that code into a computer database and quickly locate medical records for a patient. This could save precious time during an emergency or reduce risks when treating a patient with dementia.

Security. This technology is also being used for improved safety and security. Some organizations have already begun to use implanted microchips as an electronic key to provide access to highly sensitive areas.

Convenience. As with most technology, it can be seen as a timesaving convenience. Some night clubs in Europe already allow patrons with microchip implants to pay with the electronic codes they carry under their skin, and some in the U.S. have experimented with programming computers to read RFID implanted microchips to accomplish such tasks as unlocking a car with a wave of the hand.

HEALTH AND PRIVACY CONCERNS

2005 Wisconsin Act 482 is not intended to prohibit human microchip implantations, but is generally seen as a first step in regulating a procedure that has raised health and privacy concerns.

Health Risks. As with any surgery, health risks are involved. The FDA has reported on the specific risks of the VeriChip microchip, some of which are: adverse tissue reaction, migration of implanted transponder, electromagnetic interference, electrical hazards, and magnetic resonance imaging incompatibility.

Identity Theft. Privacy advocates warn that carrying personal identification on an RFID microchip may lead to more identity theft. Although the current technology requires a sensor to be very close to the microchip, and the microchips only contain an identification code, some have compared this technology to wearing your Social Security number on your sleeve.

Mass Implantation. Civil libertarians warn that human implantation has not received enough debate and may put us on a slippery slope toward a system of human

Prepared by Anthony Gad, Legislative Analyst

Reference Desk: (608) 266-0341
Web Site: www.legis.state.wi.us/lrb

(/)

numbering. They contend that human microchip implantation will first be sold to the populace as being beneficial, fun, and ultra-convenient, convincing many that microchip implantations are benign.

Some worry that mass implantation will lead to large scale abuse. For example, U.S. Senator Arlen Specter reported that Columbian President Alvaro Uribe suggested that Columbian seasonal workers could have microchips implanted into their bodies before being permitted to enter the U.S. The senator's reported objection to this idea centered on its lack of effectiveness, as immigrant workers might be able to remove the microchips.

LEGISLATIVE HISTORY

2005 Wisconsin Act 482 has only two provisions. It prohibits requiring anyone to undergo a microchip implantation and provides that violators forfeit up to \$10,000 per day. Although the act has a limited scope, the legislative debate reflected a wide-ranging discussion of potential applications.

2005 Assembly Bill 290. On April 4, 2005, Assembly Bill 290 was introduced by Representative Marlin Schneider to prohibit requiring an individual to undergo microchip implantation and subject a violator to the equivalent of a Class A forfeiture from the Criminal Code. The drafting record describes a proposal to prohibit requiring, coercing, or attempting to coerce any individual into having a microchip implanted. As introduced, the legislation did not mention "coercing or attempting to coerce," and instead focused on "required" implanting.

Amendments. Two amendments were adopted during the legislative process. In the assembly, a simple amendment was passed to reduce the scope of the prohibition on required human microchip implantation, but a senate substitute amendment subsequently reversed

those changes. Assembly Amendment 1 to 2005 Assembly Bill 290 would have allowed requiring microchip implantation of certain sex offenders and minors at the direction of their parents. It was introduced by Representative Scott Suder, the author of 2005 Wisconsin Act 431, which requires that certain sex offenders receive lifetime tracking with a global positioning system. Senate Substitute Amendment 1 to 2005 Assembly Bill 290 removed the exceptions introduced by Assembly Amendment 1 and returned the language to its original form.

OTHER STATES

At least 17 states have introduced or considered legislation in 2006 related to RFIDs, including Rhode Island which considered a bill to restrict the use of RFIDs for the purpose of tracking the movement or identity of an employee, student, or client as a condition of obtaining a benefit or services. Some states, such as New Hampshire and Georgia, are studying the issue. The New Hampshire Legislature passed a law on May 24, 2006, creating the Commission on the Use of Radio Frequency Technology to study the benefits and potential privacy implications. In Georgia, a resolution adopted on March 28, 2006, created the House Study Committee on Biological Privacy. Few states have taken the step toward regulating human implantation of RFID microchips. Legislation was introduced in New Jersey on May 15, 2006, to prohibit requiring an individual to have a microchip implanted, to require an informed written consent before implantation, and to entitle those implanted to have the microchip removed at any time.

FOR FURTHER INFORMATION

View a copy of 2005 Wisconsin Act 482 at www.legis.state.wi.us

1 AN ACT prohibiting the required implanting of a microchip in an individual, adding new
2 sections to chapter _____ RCW, and providing a penalty.

3 **BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:**

4 NEW SECTION. Section 1. The following definitions apply throughout sections 2
5 and 3 of this act.

6 (1) "Person" means an individual, corporation, business trust, estate, trust,
7 partnership, limited liability company, association, joint venture, government, government
8 subdivision, agency or instrumentality, public corporation, or any other legal or commercial
9 entity.

10 (2) "Microchip" means a radio frequency identification transponder.

11 NEW SECTION. Section 2.

12 (1) No person shall require an individual to undergo the implanting of a microchip.

13 (2) No person shall implant or attempt to implant a microchip into an individual
14 without the informed, written consent of the individual, or the individual's legal guardian.

15 (3) No person shall use the presence or absence of an implanted microchip within
16 an individual as a basis for discriminating against that individual.

17 NEW SECTION. Section 3.

18 (1) A person who violates section 2(1) of this act is guilty of a class C felony and shall
19 be subject to at least one year of imprisonment or a fine of \$10,000.

20 (2) A person who violates section 2(2) or section 2(3) of this act is guilty of a gross
21 misdemeanor and shall be subject to at least three months of imprisonment or a fine of
22 \$5,000.

(2)

2005 Assembly Bill 290

Date of enactment: May 30, 2006
Date of publication*: June 13, 2006

2005 WISCONSIN ACT 482

AN ACT to create 146.25 of the statutes; relating to: prohibiting the required implanting of a microchip in an individual and providing a penalty.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 146.25 of the statutes is created to read:

146.25 Required implanting of microchip prohibited. (1) No person may require an individual to undergo

the implanting of a microchip.

(2) Any person who violates sub. (1) may be required to forfeit not more than \$10,000. Each day of continued violation constitutes a separate offense.

(3)

* Section 991.11, WISCONSIN STATUTES 2003-04 : Effective date of acts. "Every act and every portion of an act enacted by the legislature over the governor's partial veto which does not expressly prescribe the time when it takes effect shall take effect on the day after its date of publication as designated" by the secretary of state [the date of publication may not be more than 10 working days after the date of enactment].

First Regular Session
Sixty-sixth General Assembly
STATE OF COLORADO

INTRODUCED

LLS NO. 07-0206.01 Stephen Miller

HOUSE BILL 07-1082

HOUSE SPONSORSHIP

Hodge,

SENATE SPONSORSHIP

(None),

House Committees
Judiciary

Senate Committees

A BILL FOR AN ACT

101 CONCERNING A PROHIBITION ON REQUIRING AN INDIVIDUAL TO BE
102 IMPLANTED WITH A MICROCHIP.

Bill Summary

(Note: This summary applies to this bill as introduced and does not necessarily reflect any amendments that may be subsequently adopted.)

Makes it a class 3 misdemeanor for a person to require an individual to be implanted with a microchip. Specifies that each day of a continued violation shall constitute a separate offense.

1 *Be it enacted by the General Assembly of the State of Colorado:*

Shading denotes HOUSE amendment. Double underlining denotes SENATE amendment.
Capital letters indicate new material to be added to existing statute.
Dashes through the words indicate deletions from existing statute.

4

1 **SECTION 1.** Article 13 of title 18, Colorado Revised Statutes, is
2 amended BY THE ADDITION OF A NEW SECTION to read:

3 **18-13-130. Required implantation of microchip in individual**
4 **prohibited.** (1) A PERSON MAY NOT REQUIRE AN INDIVIDUAL TO BE
5 IMPLANTED WITH A MICROCHIP.

6 (2) A VIOLATION OF THIS SECTION IS A CLASS 3 MISDEMEANOR
7 PUNISHABLE AS PROVIDED IN SECTION 18-1.3-501. EACH DAY IN WHICH A
8 PERSON VIOLATES THIS SECTION SHALL CONSTITUTE A SEPARATE OFFENSE.

9 **SECTION 2. Effective date - applicability.** (1) This act shall
10 take effect September 1, 2007.

11 (2) However, if a referendum petition is filed against this act or
12 an item, section, or part of this act during the 90-day period after final
13 adjournment of the general assembly that is allowed for submitting a
14 referendum petition pursuant to article V, section 1 (3) of the state
15 constitution, then the act, item, section, or part, shall not take effect unless
16 approved by the people at a biennial regular general election and shall
17 take effect on the date specified in subsection (1) or on the date of the
18 official declaration of the vote thereon by proclamation of the governor,
19 whichever is later.

20 (3) The provisions of this act shall apply to offenses committed on
21 or after the applicable effective date of this act.

TWO U.S. EMPLOYEES INJECTED WITH RFID MICROCHIPS AT COMPANY REQUEST Government Contractor Adopts Controversial VeriChip Implant in Workplace

Cincinnati video surveillance company CityWatcher.com now requires employees to use VeriChip human implantable microchips to enter a secure data center, Network Administrator Khary Williams told Liz McIntyre by phone yesterday. McIntyre, co-author of "Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID." contacted CityWatcher after it announced it had integrated the VeriChip VeriGuard product into its access control system.

The VeriChip is a glass encapsulated RFID tag that is injected into the flesh of the triceps area of the arm to uniquely number and identify individuals. The tag can be read through a person's clothing, silently and invisibly, by radio waves from a few inches away. The highly controversial device is being marketed as a way to access secure areas, link to medical records, and serve as a payment instrument when associated with a credit card.

According to Williams, a local doctor has already implanted two of CityWatcher's employees with the VeriChip devices. "I will eventually" receive an implant, too, he added. In the meantime, Williams accesses the data center with a VeriChip implant housed in a heart-shaped plastic casing that hangs from his keychain. He told McIntyre he had no qualms about undergoing the implantation procedure himself, and said he would receive an implant as soon as time permits.

"It worries us that a government contractor that specializes in surveillance projects would be the first to publicly incorporate this technology in the workplace," said McIntyre. CityWatcher provides video surveillance, monitoring and video storage for government and businesses, with cameras set up on streets throughout Cincinnati.

The company hopes the VeriChip will beef up its proximity or "prox" card security system that controls access to the room where the video footage is stored, said Gary Retherford of Six Sigma Security, Inc., the company that provided the VeriChip technology. "The prox card is a system that can be compromised," said Retherford, referring to the card's well-known vulnerability to hackers. He explained that chipping employees "was a move to increase the layer of security....It was attractive because it could be integrated with the existing system."

Ironically, implantable tags may not provide CityWatcher with that additional safety, after all. Last month security researcher Jonathan Westhues demonstrated how the VeriChip can be skimmed and cloned by a hacker, who could theoretically duplicate an individual's VeriChip implant to access a secure area. Westhues, author of a chapter titled "Hacking the Prox Card" for Simson Garfinkel's recent "RFID: Applications, Security, and Privacy," said the VeriChip "is not good for anything" and has absolutely no security.

"No one I spoke with at Six Sigma Security or at CityWatcher knew that the VeriChip had been hacked," McIntyre observed. "They were also surprised to hear of VeriChip's downsides as a medical device. It was clear they weren't aware of some of the controversy surrounding the implant."

Although CityWatcher reportedly does not require its employees to take an implant to keep their jobs, Katherine Albrecht, "Spychips" co-author and outspoken critic of the VeriChip, says the chipping sets an unsettling precedent. "It's wrong to link a person's paycheck with getting an implant," she said. "Once people begin 'voluntarily' getting chipped to perform their job duties, it won't be long before pressure is applied to those who refuse."

Albrecht predicts that news of the security flaws will combine with public squeamishness to make the VeriChip a hard product to sell, however. "Obviously, nobody wants their employer coming at them with a giant hypodermic needle. But when people realize it takes a scalpel and surgery to remove the device if it gets hacked, they'll really think twice," she said. "An implant is disgusting enough going in, but getting it out again is a bloody mess."



Eric Schmidt? Jimmy Wal
Steve Jobs?

To print: Click here or Select File and then Print from your browser's menu

This story was printed from silicon.com, located at <http://www.silicon.com/>

Story URL:

<http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39124983,00.htm>

RFID chips in humans get green light
FDA gives approval for use in patients

By Alorie Gilbert

Published: Thursday 14 October 2004

The US Food and Drug Administration has approved the practice of injecting humans with tracking devices for medical purposes, according to a Florida company that makes the devices.

Applied Digital, maker of the implantable VeriChip for humans, announced on Wednesday the FDA's approval of its technology for use in hospitals following a year-long review by the agency.

The computer chips, which are about the size of a grain of rice, are designed to be injected into the fatty tissue of the arm. Using a special scanner, doctors and other hospital staff can fetch information from the chips, such as the patient's identity, their blood type and the details of their condition, in order to speed treatment.

The company is targeting the devices at patients suffering from Alzheimer's disease, diabetes, cardiovascular disease and other conditions requiring complex treatment.

Medical data is not stored on the devices, also known as radio frequency identification chips. Rather, it's stored in a database that links the chips' unique serial numbers with patient data. In its review, the FDA carefully studied the privacy issues around the technology, specifically the risk that medical records could be improperly disclosed, according to Applied Digital.

So far, no hospitals in the United States have placed orders for the chips, an Applied Digital representative said. So the company is planning to give away scanners, which cost \$650 a piece, to 200 trauma centres around the country to jump-start the market.

The patient ID chips are taking off more quickly in other countries. In Mexico, more than 1,000 patients have been implanted with VeriChips. The Italian Ministry of Health is testing the technology in some hospitals there.

Applied Digital, based in Palm Beach, Florida, also markets the VeriChip as an authentication tool for use in building security and to complete financial transactions. The attorney general of Mexico and 200 people on his staff have already been implanted with the company's chips as part of an effort to control access to areas where confidential documents are kept.

The tags, which are inserted with a syringe, have been used to track pets and livestock for years, the company said.

Applied Digital has sold about 7,000 VeriChip devices, and approximately 1,000 have been inserted in humans, the company said in July. The company would not provide more current figures or disclose the price of the chips.

Copyright © 2007 CNET Networks, Inc. All rights reserved.
[About CNET Networks](#) | [About CNET Networks UK](#)

Health & Science**Ethical Questions Raised over Implantable Chips**

by Joseph Shapiro

All Things Considered, November 12, 2005 · In Chattanooga, Tenn., people with mental retardation are being offered a device that could save lives in the case of a medical emergency. It's a microchip that would be implanted under the skin. But there are questions about giving this cutting-edge technology to people who can't make decisions for themselves.

VERICHIP MAY IMPLANT THE MENTALLY IMPAIRED IN CHATTANOOGA

Several hundred mentally impaired residents and employees of The Orange Grove Center in Chattanooga, Tennessee, may be injected with VeriChip RFID implants, according to a November 12 National Public Radio story. The Center is considering implanting the glass encapsulated RFID tags, which have a read range of approximately six to eighteen inches, as a way to identify "wanderers" and those who need medical assistance. Though the chipping is said to be "voluntary," the patients would not be able to consent themselves; their parents and legal guardians would have to make the decision for them.

VeriChip Corporation has been trying to find new ways to "sell" its unpopular product. The device, about the length of the diameter of a dime, is typically implanted under the flesh of the upper arm, in the triceps area. Despite years of effort, the company has only been able to convince about 50 living people in the United States to undergo the procedure.



To aid to enhance its image, the company has hired former Secretary of Health and Human Services Tommy Thompson to join its board and tout the implant as a way to link patients to a national medical database. Other marketing initiatives have included chipping bar patrons as a way to pay for drinks, implanting employees in the Mexican attorney general's office, and chipping the remains of the victims of hurricane Katrina. However, this latest initiative to chip the residents of the Orange Grove Center is the first time living persons would be chipped without their express consent.

Reportedly, VeriChip will waive the usual \$200 implantation fee to "show the benefits for people with cognitive disabilities."

Coincidentally--or maybe not-- this reported initiative was followed by VeriChip's announcement that it will make an initial public offering of its stock in the second quarter of 2006.

Those wishing to express concerns about the chipping can contact the Orange Grove Center's Fundraising/Public and Media Relations Office: (423) 308-1160.

Indigo Jo Blogs

In which an unemployed graduate has an excuse to use his politics degree. Reli
and media issues (and anything)

« Inside scoop on Lebanon protests | Main | Reflections on "Undercover Mosque" »

Monbiot on RFIDs

George Monbiot has an article in today's Guardian about the emerging "radio frequency identification tags", used in one company in Ohio to identify two workers who are entitled to enter the strongroom. The chips are implanted under the skin to identify people, are getting cheaper, and have obvious ramifications for personal liberty:

At first the tags will be more widely used for workers with special security clearance. No one will be forced to wear one; no one will object. Then hospitals - and a few in the US are already doing this - will start scanning their unconscious or incoherent patients to see whether they have a tag. Insurance companies might start to demand that vulnerable people are chipped.

The armed forces will discover that they are more useful than dog tags for identifying injured soldiers or for tracking troops who are lost or have been captured by the enemy. Prisons will soon come to the same conclusion. Then sweatshops in developing countries will begin to catch on. Already the overseers seek to control their workers to the second; determining when they clock on, when they visit the toilet, even the number of hand movements they perform. A chip makes all this easier. The workers will not be forced to have them, any more than they are forced to have sex with their bosses; but if they don't accept the conditions, they don't get the job. After that, it surely won't be long before asylum seekers are confronted with a similar choice: you don't have to accept an implant, but if you refuse, you can't stay in the country.

The article concludes on our country's muted response to the progressive erosion of our privacy and freedom and how our population is gradually submitting "to the demands of the machine".

Colleen Hammond (Catholic talk show host, writer and blogger) brought this up on her blog Dressing With Dignity in October 2004 (see here). I made the point in the comments to that entry that the same technology which is supposedly able to prevent children falling into the hands of undesirables could just as easily be used to trap children in abusive situations at the hands of their carers (the same could be true of elderly people) by making it easier for people to catch up with them when they run away. Of course, when the chips are implanted for "safety" reasons in childhood, they would end up remaining in the body for decades and so could be used to track them much later, for good or evil purposes.

Islam Ringtone:
Send 10 Compli
Ringtones to you
MobileContentPlus.cc

Former Muslim
Out
Man raised as M
now sees Jesus
different light.
www.EveryStudent.cc

Free Quran
English, Spanish
French Free Qur
& Free Shipping
www.freequran.org

Islam Muslim
Meet Hundreds o
Thousands of M
Singles for Love,
Friendship
www.MuslimFriends.cc

Adema Rington
Refusing Consci
ringtones by Ade
instantly!
GetPhoneTones.com

Advertise on this site

(8)
STATE OF OKLAHOMA

1st Session of the 51st Legislature (2007)

SENATE BILL 47

By: Crain

AS INTRODUCED

An Act relating to public health and safety;
prohibiting the forced implantation of a microchip;
authorizing the State Department of Health to impose
a fine in certain circumstance; providing for
codification; and providing an effective date.

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

SECTION 1. NEW LAW A new section of law to be codified
in the Oklahoma Statutes as Section 1-1430 of Title 63, unless there
is created a duplication in numbering, reads as follows:

A. No person may require an individual to undergo the
implanting of a microchip.

B. The State Department of Health may impose a fine not to
exceed Ten Thousand Dollars (\$10,000.00) on any person who violates
this act. Each day of continued violation shall constitute a
separate offense.

SECTION 2. This act shall become effective November 1, 2007.

51-1-543

JC

1/30/2007 10:12:05 AM

STATE OF OKLAHOMA

1st Session of the 51st Legislature (2007)

HOUSE BILL 2092

By: Tibbs

AS INTRODUCED

An Act relating to crimes and punishments;
prohibiting the required implanting of a microchip in
an individual; providing penalty; providing for
codification; and providing an effective date.

BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

SECTION 1. NEW LAW A new section of law to be codified
in the Oklahoma Statutes as Section 1220.2 of Title 21, unless there
is created a duplication in numbering, reads as follows:

A. No person shall require an individual to undergo the
implanting of a microchip.

B. Any person convicted of violating the provisions of this
section shall be subject to a fine of not more than Ten Thousand
Dollars (\$10,000.00). Each day of continued violation shall
constitute a separate offense.

SECTION 2. This act shall become effective November 1, 2007.

51-1-5411 LRB 12/28/06

Same
to House

AH #2
1-31-07

Good morning---I am Irma Bitner, a registered nurse. I work with a home health agency here in Bismarck. I would like to share a few of my concerns with the mandatory implantation of the veri chip. The FDA has approved it, but that does not make it completely safe.

In a letter the FDA wrote to the Digital Angel Corporation, they have listed some of the risks involved with the implantation of the veri chip. Adverse reactions could be serious burns and the possibility of migration which could cause tissue damage. Failure of the implanted transponder, insertor, or scanner could also create problems.

I feel the incompatibility with the MRI is the most serious risk because of the combination of a powerful magnetic field, coupled with pulsed radio frequency fields. It could potentially cause severe burns.

In addition, there is a privacy concern brought about by the FDA letter. It is a possibility that a criminal or anybody with a reader could read the information and clone another with the same functionality. *How can this be called security when a chip can be read by anyone and cloned?*

I prefer my medical records in the record room.

With criminal intent, someone could just gouge it out of a person, causing severe damage to the tissues. The chips could also be a real problem for ambulance patients, due to all the electrical interference. It could cause transponder failure.

The UK Daily Mail reported that teens are preferring suicide over chip implants. I don't want to see this come for our children. Let them have freedom like we had.

The privacy issue (compromised data security)---*Who will control the data banks? And under what checks and balances? How will the data be secured from theft, negligence, abuse? And how will accuracy be ensured?*

This is very likely to become a new multi-million dollar market for the veri chip corporations--pushing all sorts of these products.

We do not want to be a part of the dangerous money making market.

Thank you for your time.

Special Report, October 19, 2004

FDA Letter Raises Questions about VeriChip Safety, Data Security

"The potential risks to health associated with the device are: adverse tissue reaction; migration of implanted transponder; compromised information security; failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick."

- FDA's VeriChip Letter, 10/12/04

FDA letter to the Digital Angel Corporation spells out potential health risks associated with the VeriChip ID implant device. Click here to download a PDF of the full letter. (For the passage above, see page 3, paragraph 2.)

Think it's completely safe to inject an RFID transponder into your flesh? Think again.

Although the FDA approved the VeriChip implant last week, their approval does not mean the device is completely safe, according to an FDA letter CASPIAN has obtained. The letter, dated October 12, 2004, was sent to Digital Angel Corporation and outlines a number of potential health risks associated with the device.

Among the potential problems the FDA identifies are: "adverse tissue reaction," "migration of the implanted transponder," "failure of implanted transponder," "electrical hazards" and "magnetic resonance imaging [MRI] incompatibility." Not to mention the nasty needle stick from the "inserter" used to inject it. (The FDA lists "failure of inserter" -- a bloody possibility we'd rather not contemplate -- among the risks.)

To read the FDA's letter for yourself, download the PDF and refer to Page 3, Paragraph 2.

Of the numerous risks listed, MRI incompatibility is perhaps the most serious. An MRI machine uses powerful magnetic fields coupled with pulsed radio frequency (RF) fields. According to the FDA's Primer on Medical Device Interactions with Magnetic Resonance Imaging Systems, "electrical currents may be induced in conductive metal implants" that can cause "potentially severe patient burns."

Presumably, VeriChip-MRI incompatibility means that doctors will be unable to order this potentially life-saving diagnostic procedure for patients with VeriChip implants, unless the patient undergoes a surgical procedure to remove the VeriChip first.

In addition to health risks, the FDA's letter identifies "compromised data security" as one of the concerns associated with the VeriChip. It appears that not only could someone use a reader device to capture the information from an implanted VeriChip, but they could use that information to create a cloned chip with the same functionality. (Of course, criminals lacking RF engineering skills might be tempted to take a more direct route and simply gouge the device out of their victims' arms instead.)

VERICHIP™

VeriChip Portal Reader

The VeriChip freestanding "Portal" scanners have been designed for use at the point of contact with the subscriber such as a security checkpoint, building access, etc.



If that's not enough to convince you to "say
to the VeriChip, how about knowing your VeriChip implant can be read whenever you pass through a
tollway equipped with a special VeriChip "portal scanner"?

The image at right comes from a company called "Find Me, LLC," a value-added reseller of VeriChip technology based in Louisiana. The company also sells a handheld reader, which presumably anyone can use to read VeriChip data.

That's quite a lot of potential harm for something supposedly designed to *help* patients.



If you're looking for a secure, non-invasive way to alert medical professionals to your health history, we recommend the MedicAlert bracelet as a safe alternative to the VeriChip. Given the MedicAlert's 48-year track record, all emergency health providers know to look for it. It costs far less and has none of the serious health risks associated with an implanted computer chip.

October 12, 2006

Do young people want microchip payment implants? Not really.



The sky is falling! Or is it? .

A breathless report in yesterday's UK Daily Mail proclaimed that "young shoppers want to pay with chip in skin." While this headline is certainly explosive (it got the attention of the Drudge report), it is also utterly preposterous. If you read the article, you will quickly discover that young people do NOT want to "pay with a chip in the skin." Indeed, 92% of them said they did not.

Picking up a survey in which virtually all respondents say they would NOT do something and reporting it as a ringing endorsement is misleading journalism, plain and simple. The Daily Mail should be ashamed.

But assuming there was some real news here, how significant is it that 8% of teens said they'd get a payment chip? Just for kicks, I looked around the net at other studies of UK teens. Let's compare a few statistics. While 8% of teens say they would consider a payment chip implant, another survey shows that 20% of teens are experiencing psychological problems at any given time, and nearly a third of college students have contemplated suicide at some point in their lives. Contemplating suicide would seem far more dramatic than considering a chip implant, yet we don't read stories proclaiming that UK youth are lining up in droves to kill themselves.

What's more, a third of UK teens reported vandalizing property within the last year, a quarter reported shoplifting, forty percent had binged on alcohol, and half reported committing at least one criminal act. [Source] In other words, teens (as we know) are still trying to figure out

the basic rules of social behavior and self-control, and are likely to harm themselves in the process.

Given these other eye-opening statistics, the amazing part of the chipping study is that more teens *didn't* agree, even on paper (where there's no reality check in the form of a massive hypodermic needle), to get a chip implant.

What all this boils down to is that, statistically speaking, teens prefer suicide over chip implants. The headline should instead read, "I'd sooner kill myself than get chipped."

-Katherine Albrecht

Posted by Katherine Albrecht at 10:38 AM | Comments (3)

SUBSCRIBE TO



AND GET A FREE
MESSENGER BAG!
ORDER NOW

YOUR
FREE
GIFT!

SUBS
ENTE
WIRE
TOP I

WIRED

Search Now All of Wired

Go

TOP TECHNOLOGY CULTURE POLITICS COLUMNS BLOGS WIRED MAG THE OUTSIDE WORLD SUBSCRIBE

The RFID Hacking Underground

They can steal your smartcard, lift your passport, jack your car, even clone the chip in your arm. And you won't feel a thing. 5 tales from the RFID-hacking underground.

By Annalee Newitz

Feature:

While You Were Reading This, Someone Ripped You Off

Plus:

Risky Chips: 4 RFID Hacks

James Van Bokkelen is about to be robbed. A wealthy software entrepreneur, Van Bokkelen will be the latest victim of some punk with a laptop. But this won't be an email scam or bank account hack. A skinny 23-year-old named Jonathan Westhues plans to use a cheap, homemade USB device to swipe the office key out of Van Bokkelen's back pocket.

"I just need to bump into James and get my hand within a few inches of him," Westhues says. We're shivering in the early spring air outside the offices of Sandstorm, the Internet security company Van Bokkelen runs north of Boston. As Van Bokkelen approaches from the parking lot, Westhues brushes past him. A coil of copper wire flashes briefly in Westhues' palm, then disappears.

Van Bokkelen enters the building, and Westhues returns to me. "Let's see if I've got his keys," he says, meaning the signal from Van Bokkelen's smartcard badge. The card contains an RFID sensor chip, which emits a short burst of radio waves when activated by the reader next to Sandstorm's door. If the signal translates into an authorized ID number, the door unlocks.

The coil in Westhues' hand is the antenna for the wallet-sized device he calls a cloner, which is currently shoved up his sleeve. The cloner can elicit, record, and mimic signals from smartcard RFID chips. Westhues takes out the device and, using a USB cable, connects it to his laptop and downloads the data from Van Bokkelen's card for processing. Then, satisfied that he has retrieved the code, Westhues switches the cloner from Record mode to Emit. We head to the locked door.

"Want me to let you in?" Westhues asks. I nod.

http://www.wired.com/wired/archive/14.05/rfid_pr.html

2/12/2007

He waves the cloner's antenna in front of a black box attached to the wall. The single red LED blinks green. The lock clicks. We walk in and find Van Bokkelen waiting.

"See? Just broke into your office!" Westhues says gleefully. "It's so simple." Van Bokkelen, who arranged the robbery "just to see how it works," stares at the antenna in Westhues' hand. He knows that Westhues could have performed his wireless pickpocket maneuver and then returned with the cloner after hours. Westhues could have walked off with tens of thousands of dollars' worth of computer equipment - and possibly source code worth even more. Van Bokkelen mutters, "I always thought this might be a lousy security system."

RFID chips are everywhere - companies and labs use them as access keys, Prius owners use them to start their cars, and retail giants like Wal-Mart have deployed them as inventory tracking devices. Drug manufacturers like Pfizer rely on chips to track pharmaceuticals. The tags are also about to get a lot more personal: Next-gen US passports and credit cards will contain RFIDs, and the medical industry is exploring the use of implantable chips to manage patients. According to the RFID market analysis firm IDTechEx, the push for digital inventory tracking and personal ID systems will expand the current annual market for RFIDs from \$2.7 billion to as much as \$26 billion by 2016.

RFID technology dates back to World War II, when the British put radio transponders in Allied aircraft to help early radar system crews detect good guys from bad guys. The first chips were developed in research labs in the 1960s, and by the next decade the US government was using tags to electronically authorize trucks coming into Los Alamos National Laboratory and other secure facilities. Commercialized chips became widely available in the '80s, and RFID tags were being used to track difficult-to-manage property like farm animals and railroad cars. But over the last few years, the market for RFIDs has exploded, driven by advances in computer databases and declining chip prices. Now dozens of companies, from Motorola to Philips to Texas Instruments, manufacture the chips.

The tags work by broadcasting a few bits of information to specialized electronic readers. Most commercial RFID chips are passive emitters, which means they have no onboard battery: They send a signal only when a reader powers them with a squirt of electrons. Once juiced, these chips broadcast their signal indiscriminately within a certain range, usually a few inches to a few feet. Active emitter chips with internal power can send signals hundreds of feet; these are used in the automatic toll-paying devices (with names like FasTrak and

E-ZPass) that sit on car dashboards, pinging tollgates as autos whiz through.

For protection, RFID signals can be encrypted. The chips that will go into US passports, for example, will likely be coded to make it difficult for unauthorized readers to retrieve their onboard information (which will include a person's name, age, nationality, and photo). But most commercial RFID tags don't include security, which is expensive: A typical passive RFID chip costs about a quarter, whereas one with encryption capabilities runs about \$5. It's just not cost-effective for your average office building to invest in secure chips.

This leaves most RFIDs vulnerable to cloning or - if the chip has a writable memory area, as many do - data tampering. Chips that track product shipments or expensive equipment, for example, often contain pricing and item information. These writable areas can be locked, but often they aren't, because the companies using RFIDs don't know how the chips work or because the data fields need to be updated frequently. Either way, these chips are open to hacking.

"The world of RFID is like the Internet in its early stages," says Ari Juels, research manager at the high tech security firm RSA Labs. "Nobody thought about building security features into the Internet in advance, and now we're paying for it in viruses and other attacks. We're likely to see the same thing with RFIDs."

David Molnar is a soft-spoken computer science graduate student who studies commercial uses for RFIDs at UC Berkeley. I meet him in a quiet branch of the Oakland Public Library, which, like many modern libraries, tracks most of its inventory with RFID tags glued inside the covers of its books. These tags, made by Libramation, contain several

writable memory "pages" that store the books' barcodes and loan status.

Brushing a thatch of dark hair out of his eyes, Molnar explains that about a year ago he discovered he could destroy the data on books' passive-emitting RFID tags by wandering the aisles with an off-the-shelf RFID reader-writer and his laptop. "I would never actually do something like that, of course," Molnar reassures me in a furtive whisper, as a nonbookish security guard watches us.

Feature:

While You Were Reading This, Someone Ripped You Off

Plus:

Risky Chips: 4 RFID Hacks

Our RFID-enabled checkout is indeed quite convenient. As we leave the library, we stop at a desk equipped with a monitor and arrange our selections, one at a time, face up on a metal plate. The titles instantly appear onscreen. We borrow four books in less than a minute without bothering the librarian, who is busy helping some kids with their homework.

Molnar takes the books to his office, where he uses a commercially available reader about the size and heft of a box of Altoids to scan the data from their RFID tags. The reader feeds the data to his computer, which is running software that Molnar ordered from RFID-maker Tagsys. As he waves the reader over a book's spine, ID numbers pop up on his monitor.

"I can definitely overwrite these tags," Molnar says. He finds an empty page in the RFID's memory and types "AB." When he scans the book again, we see the barcode with the letters "AB" next to it. (Molnar hastily erases the "AB," saying that he despises library vandalism.) He fumes at the Oakland library's failure to lock the writable area. "I could erase the barcodes and then lock the tags. The library would have to replace them all."

Frank Mussche, Libramation's president, acknowledges that the library's tags were left unlocked. "That's the recommended implementation of our tags," he says. "It makes it easier for libraries to change the data."

For the Oakland Public Library, vulnerability is just one more problem in a buggy system. "This was mostly a pilot project, and it was implemented poorly," says administrative librarian Jerry Garzon. "We've decided to move ahead without Libramation and RFIDs."

But hundreds of libraries have deployed the tags. According to Mussche, Libramation has sold 5 million RFID tags in a "convenient" unlocked state.

While it may be hard to imagine why someone other than a determined vandal would take the trouble to change library tags, there are other instances where the small hassle could be worth big bucks. Take the Future Store. Located in Rheinberg, Germany, the Future Store is the world's preeminent test bed of RFID-based retail shopping. All the items in this high tech supermarket have RFID price tags, which allow the store and individual product manufacturers - Gillette, Kraft, Procter & Gamble - to gather instant feedback on what's being bought. Meanwhile, shoppers can check out with a single flash of a reader. In July 2004, Wired hailed the store as the "supermarket of the future." A few months later, German security expert Lukas Grunwald hacked the chips.

Grunwald cowrote a program called RFDump, which let him access and alter price chips using a PDA (with an RFID reader) and a PC card antenna. With the store's permission, he and his colleagues strolled the aisles, downloading information from hundreds of sensors. They then showed how easily they could upload one chip's data onto another. "I could download the price of a cheap wine into RFDump," Grunwald says, "then cut and paste it onto the tag of an expensive bottle." The price-switching stunt drew media attention, but the Future Store still didn't lock its price tags. "What we do in the Future Store is purely a test," says the Future Store spokesperson Albrecht von Truchsess. "We don't expect that retailers will use RFID like this at the product level for at least 10 or 15 years." By then, Truchsess thinks,

security will be worked out.

Today, Grunwald continues to pull even more-elaborate pranks with chips from the Future Store. "I was at a hotel that used smartcards, so I copied one and put the data into my computer," Grunwald says. "Then I used RFDump to upload the card data to the price chip on a box of cream cheese from the Future Store. And I opened my hotel room with the cheese!"

Aside from pranks, vandalism, and thievery, Grunwald has recently discovered another use for RFID chips: espionage. He programmed RFDump with the ability to place cookies on RFID tags the same way Web sites put cookies on browsers to track returning customers. With this, a stalker could, say, place a cookie on his target's E-ZPass, then return to it a few days later to see which toll plazas the car had crossed (and when). Private citizens and the government could likewise place cookies on library books to monitor who's checking them out.

In 1997, ExxonMobil equipped thousands of service stations with SpeedPass, which lets customers wave a small RFID device attached to a key chain in front of a pump to pay for gas. Seven years later, three graduate students - Steve Bono, Matthew Green, and Adam Stubblefield - ripped off a station in Baltimore. Using a laptop and a simple RFID broadcasting device, they tricked the system into letting them fill up for free.

The theft was concocted by Avi Rubin's computer science lab at Johns Hopkins University. Rubin's lab is best known for having found massive, hackable flaws in the code running on Diebold's widely adopted electronic voting machines in 2004. Working with RSA Labs manager Juels, the group figured out how to crack the RFID chip in ExxonMobil's SpeedPass.

Hacking the tag, which is made by Texas Instruments, is not as simple as breaking into Van Bokkelen's Sandstorm offices with a cloner. The radio signals in these chips, dubbed DST tags, are protected by an encryption cipher that only the chip and the reader can decode. Unfortunately, says Juels, "Texas Instruments used an untested cipher." The Johns Hopkins lab found that the code could be broken with what security geeks call a "brute-force attack," in which a special computer known as a cracker is used to try thousands of password combinations per second until it hits on the right one. Using a homebrewed cracker that cost a few hundred dollars, Juels and the Johns Hopkins team successfully performed a brute-force attack on TI's cipher in only 30 minutes. Compare that to the hundreds of years experts estimate it would take for today's computers to break the publicly available encryption tool SHA-1, which is used to secure credit card transactions on the Internet.

ExxonMobil isn't the only company that uses the Texas Instruments tags. The chips are also commonly used in vehicle security systems. If the reader in the car doesn't detect the chip embedded in the rubbery end of the key handle, the engine won't turn over. But disable the chip and the car can be hot-wired like any other.

Feature:

While You Were Reading This, Someone Ripped You Off

Plus:

Risky Chips: 4 RFID Hacks

Bill Allen, director of strategic alliances at Texas Instruments RFID Systems, says he met with the Johns Hopkins team and he isn't worried. "This research was purely academic," Allen says. Nevertheless, he adds, the chips the Johns Hopkins lab tested have already been phased out and replaced with ones that use 128-bit keys, along with stronger public encryption tools, such as SHA-1 and Triple DES.

Juels is now looking into the security of the new US passports, the first of which were issued to diplomats this March. Frank Moss, deputy assistant secretary of state for passport services, claims they are virtually hack-proof. "We've added to the cover an anti-skimming device that prevents anyone from reading the chip unless the passport is open," he says. Data on the chip is encrypted and can't be unlocked without a key printed in machine-readable text on the passport itself.

But Juels still sees problems. While he hasn't been able to work with an actual passport yet, he has studied the government's proposals carefully. "We believe the new US passport is probably vulnerable to a brute-force attack," he says. "The encryption keys in them will depend on passport numbers and birth dates. Because these have a certain degree of structure and guessability, we estimate that the effective key length is at most 52 bits. A special key-cracking machine could probably break a passport key of this length in 10 minutes."

I'm lying facedown on an examination table at UCLA Medical Center, my right arm extended at 90 degrees. Allan Pantuck, a young surgeon wearing running shoes with his lab coat, is inspecting an anesthetized area on the back of my upper arm. He holds up something that looks like a toy gun with a fat silver needle instead of a barrel.

I've decided to personally test-drive what is undoubtedly the most controversial use of RFIDs today - an implantable tag. VeriChip, the only company making FDA-approved tags, boasts on its Web site that "this 'always there' identification can't be lost, stolen, or duplicated." It sells the chips to hospitals as implantable medical ID tags and is starting to promote them as secure-access keys.

Pantuck pierces my skin with the gun, delivering a microchip and antenna combo the size of a grain of long rice. For the rest of my life, a small region on my right arm will emit binary signals that can be converted into a 16-digit number. When Pantuck scans my arm with the VeriChip reader - it looks sort of like the wand clerks use to read barcodes in checkout lines - I hear a quiet beep, and its tiny red LED display shows my ID number.

Three weeks later, I meet the smartcard-intercepting Westhues at a greasy spoon a few blocks from the MIT campus. He's sitting in the corner with a half-finished plate of onion rings, his long blond hair hanging in his face as he hunches over the cloner attached to his computer.

Because the VeriChip uses a frequency close to that of many smartcards, Westhues is pretty sure the cloner will work on me. Westhues waves his antenna over my arm and gets some weird readings. Then he presses it lightly against my skin the way a digital-age pickpocket could in an elevator full of people. He stares at the green waveforms that appear on his computer screen. "Yes, that looks like we got a good reading," he says.

After a few seconds of fiddling, Westhues switches the cloner to Emit and aims its antenna at the reader. *Beep!* My ID number pops up on its screen. So much for implantable IDs being immune to theft. The whole process took 10 minutes. "If you extended the range of this cloner by boosting its power, you could strap it to your leg, and somebody passing the VeriChip reader over your arm would pick up the ID," Westhues says. "They'd never know they hadn't read it from your arm." Using a clone of my tag, as it were, Westhues could access anything the chip was linked to, such as my office door or my medical records.

John Proctor, VeriChip's director of communications, dismisses this problem. "VeriChip is an excellent security system, but it shouldn't be used as a stand-alone," he says. His recommendation: Have someone also check paper IDs.

But isn't the point of an implantable chip that authentication is automatic? "People should know what level of security they're getting when they inject something into their arm," he says with a half smile.

They should - but they don't. A few weeks after Westhues clones my chip, Cincinnati-based surveillance company CityWatcher announces a plan to implant employees with VeriChips. Sean Darks, the company's CEO, touts the chips as "just like a key card." Indeed.

Contributing editor Annalee Newitz (annalee@techsploitation.com) wrote about Spyware in issue 13.12.

Wired: Staff | Contact Us | Advertising | Subscribe | Customer Service | Member Services