



Fighting the Chip

Privacy Advocate Attorney Fights Digital Angel

by Sherrie Gosset

Reprinted with permission from WorldNetDaily.com

As “Good Morning America,” “Inside Edition,” and “The CBS Evening News” televise the much-hyped “chipping” of eight individuals on May 10, Lee Tien, the senior staff attorney for the Electronic Frontier Foundation is speaking out passionately about what many experts believe are serious threats posed by implanting chips in humans—threats he says are not being adequately portrayed by the major media.

Tien has been in high demand as a commentator on the issue. And the New York City press office of the American Civil Liberties Union, which once called the chip “an outrage” and “unconstitutional,” is currently refusing to comment on the chips, referring all inquiries to Tien or David Sobel of the Electronic Privacy Information Center.

Despite the numerous requests for comments, Tien says that the media have not effectively communicated his stance on the matter: “I’ve been used as part of their press campaign—as a token privacy person. It’s really insulting.”

When the ‘chips were down’ ...

“Digital Angel,” has been described by company communications as an implantable microchip that, once inserted into a human, can be tracked by GPS and the information then relayed wirelessly to the Internet, where an individual’s location, movements and vital signs can be stored in a database for future reference. The chip, along with another non-trackable version (the VeriChip) was developed by the NASDAQ-traded, Palm Beach, Fla., company, Applied Digital Solutions.

ADS tried unsuccessfully to market the implantable tracking chip in 1999 and 2000. The company hit bumpy ground though, with protests coming from civil liberties advocates, libertarians, electronic freedom activists, radical protest organizations, anarchists and religious groups.

Complicating matters was a failed foray into presidential-year politics. WorldNetDaily has reported on an unconsummated partnership between ADS and the Clinton-Gore administration, pushed by then-Secretary of Commerce Norman Mineta just days before the presidential election. The company soon entered a dramatic financial



AP WireWorld Photo/Maria Lavandier

The Jacobs family could be one of the first to be implanted with the microchip identification device VeriChip.

free-fall, according to the South Florida Business Journal. Whereas in 2000 shares were \$18, by November of the following year they traded at 53 cents. In August of 2001, shares hit an all-time low of 16 cents. The company lost millions and was threatened with de-listing by NASDAQ.

Following Sept. 11, however, the company found its golden opportunity to reintroduce the chip, first in its non-tracking form (the VeriChip). An announcement of “phase two” of the company’s strategy is likely to ride on the heels of the much-publicized May 10 implantation event.

ADS stated in its promotional materials and website that the sophisticated Digital Angel tracking chip was intended to be implanted in human beings, tapping into an estimated \$100 billion worldwide market.

ADS chairman and CEO Richard J. Sullivan answered privacy-advocate critics at a private unveiling of the Digital Angel prototype in October 2000,

“And let me be very clear on one important point,” he said. “The potential marketplace I’m talking about is for an attachable device ... something worn on the outside ... close to the skin. ... We’re not planning on or even considering any other application at this time. Only external uses! All of our energy ... all of our

focus ... all of our effort is in this direction. Period. Any other approach or suggestion is purely hypothetical speculation at this time.”

Sullivan delivered this statement a week after his website had displayed extensive information about development of the chip for human implantation, and after McKinsey & Co. consultants had prepared a marketing projection for a whopping \$70 billion market in the U.S.

Major media ‘ignorant’ and ‘remiss’

Tien is speaking out because he believes the media are doing a poor job of reporting the threats that the chip can propose to individual rights, as well as the technical security weaknesses inherent in the Digital Angel technology delivery system.

“The impression I’m getting is that the implantation thing has a ‘gee-whiz’ factor that the media seems to like,” Tien told WND. “But ever since Sept. 11, reporters have been less aggressive about challenging the privacy implications of the technologies or the practices.”

“The media give an obligatory nod to civil liberties and privacy issues,” Tien explains, “but the reports lack objective, educated analysis, resulting in them being ‘one-sided.’ There are few reporters inter-

Mark of the Beast Watch

ested in drilling into the real problems.”

‘Frog in the pot’ marketing

Tien is especially concerned over involuntary uses of the chip and the company’s intentional strategy to “handle” the public and media, so they are gradually accepting of a more dangerous form of the chip—the GPS-tracked “Digital Angel” chip.

CEO Sullivan has suggested that all foreigners entering the U.S. should be injected with the company’s chips, which he said should replace green cards. While ADS has repeatedly stated that they are only pursuing voluntary applications of the chips, their proposed uses clearly indicate otherwise. The stunning array of potential uses ADS is pushing aggressively include the implantation of prisoners, parolees, people under house arrest, children, the elderly, airport workers, nuclear power plant workers, gun owners and computer users (as a form of log-on ID).

The company also envisions the implanted chips creating a “cashless society,” being used instead of ATM and credit cards. ADS also wants to control all of the databases for all uses of the chips.

“My take on it,” Tien explains, “has always been that the whole idea of forcing people to be tracked against their will is absolutely repugnant.”

“They’re doing the frog in the water trick – getting the memo out that this is voluntary, making it hard for civil liberty advocates to counter it,” Tien explains. “But no matter what great uses are promised by the company, it is just part of an overall, larger trend – a movement toward the much bigger location tracking development of the chip.”

Tien also stresses that once the chip is “colonized” into the prison system, it will be even harder to prevent involuntary uses from spreading to other areas of society.

“We’re very concerned about this habituating of the public. The idea is, ‘Oh well, it’s here, so get over it. It must not be so bad.’ But once they get it in limited form, the jump to tracking form is easier for the company.”

Security or hype?

Regarding the development of the chips, especially the Digital Angel tracking chip, Tien remarks: “These people [Applied Digital Solutions] have no idea



AP WideWorld Photo/HC

This is an artist’s rendering of an Air Force Navstar Global Positioning System (GPS) Block IIF satellite. Digital Angel will work with this satellite to locate and track any person with “the chip.”

whatsoever about what real security means. I spoke to their Chief Technology Officer, Dr. Keith Bolton. His response was ‘We have this proprietary technology’—a meaningless comment.”

Applied Digital Solutions contends it spent \$40 million dollars on proprietary mixed-media encryption technology, and that the system security, which relies on Secure Socket Layers (SSL), won’t be “spoofed.” Digital Angel location information is accessed by “authorized individuals” by entering a password into an Internet site. But, according to Tien, the chip delivery system is vulnerable to “spoofing” and fraught with security risks.

“The low-end VeriChip is probably quite significantly insecure, but because of its limited capacity, the actual risk is not great.”

However, Tien warns, it would be very different with Digital Angel: “People have the impression that only ‘authorized’ people will see their personal information. But all sorts of people will eventually see it.”

Compounding the problem, Tien says, are existing vulnerabilities in Microsoft software. In March of this year, Digital

Angel Corporation signed an agreement with Microsoft MapPoint in order to strengthen its worldwide GPS mapping capabilities.

“The threat is not just to the people implanted with it, but also for those people who hang out with them. They will all be part of a large surveillance system,” Tien maintained.

Chilling misuses outlined

Raising further technical concerns, Tien asked, “How do you know what information they’ve put on the chip? They don’t suggest that it’s externally programmable, but what if it is now or in the future?”

Tien illustrated his point: “Here I am with this chip. I’ve got a connection. Is it read-only or writable? And if something is wirelessly written to it, what are they saying?” Referring to the fact that wireless networks and radio frequency data transmission packets are notoriously easy to “hijack,” Tien asks, “Who are they saying I am? How hard is it for someone to send a transmission with information identical to my chip?”

Tien argues that such hacking and “spoofing” of the system could be used,

for example, to frame someone by falsely placing their identification chip information into a computer and linking the ID number with a crime scene location. "It's equivalent to saying, 'Here's your DNA at this crime scene. Now prove you weren't there,'" said Tien.

Nabbing cyberpunks?

Nathan Cochrane of The Age newspaper in Australia has also researched and explored various potential misuses of the chip. In an e-mail sent to Declan McCullagh, Washington bureau chief for Wired magazine, Cochrane summed up a potential result of using the implanted tracking chip as a logon identification system, as advocated by ADS: "Can you imagine a tracking system that could tell when you had swapped songs over Napster, then turning you in to the local police, complete with your location accurate to within a few meters?"

The observation parallels similar developments of other electronic identification systems, like electronic tollbooth passes, first marketed as a "convenience" item, but later used to issue speeding tickets to drivers who used the technology.

Cyberspace vulnerabilities critical

During congressional testimony earlier in the year, United States cybersecurity czar Richard Clarke pointed out that when corporate computer systems are hacked into, it is seldom reported to the government. This is because, after such information is reported, it could then be retrieved by researchers and reporters by using the Freedom of Information Act. So corporations typically avoid reporting serious security breaches for fear of the financial consequences that diminished consumer trust could bring.

Clarke testified before Congress that there never has been a "secure" Internet product, and that terrorists could have hacked into government systems leaving "back doors" through which they could enter later. Prior embarrassing security breaches of prominent government websites such as NASA, the Pentagon and the CIA seem to say to privacy advocates, "If the government is struggling to secure its IT systems, just how secure are commercial networks?"

Tien believes that the cyber czar's comments serve to highlight potential areas



Bernie Paulson of McPherson Crop Management of Mankato, Minn., uses a Global Positioning System to map a farmer's field tile system, Saturday.

of concern for those considering allowing companies like ADS to collect and control extremely sensitive information.

Location, location, location

Legal questions arise concerning the vacuum of legal protection of location-based electronic information. As politicians, corporate interests and privacy advocates are still wrestling over issues of who gets to see cell phone location information, the same issues apply to tracking chips. The question is, who will win access to your movement and location information? Your wife's divorce attorney? Your political rival? News reporters? Corporate lawyers? Advertising firms? Government? And who would desire to steal your location information records?

Would the monetary and power value of such personal information give rise to a "digital mafia," buying and selling your location and movement information for profit? In a world where there is mass implantation of tracking chips as a form of ID, one can only imagine the value of obtaining where a political rival was on a given night, with whom, at what hotel, and for how long? And in the cashless society advocated by ADS, what did they buy? The bio-sensor information trans-

mitted and stored by the chips would even tell you how hard their hearts were beating and to what degree their skin temperature rose.

Alternatives to implantation

For medical monitoring, implanting devices in the body is just not necessary, Tien contends. Other companies like "Lifeshirt" of Miami have developed products that monitor vital signs just like ADS chips do, but non-invasively. And as far as tamper-proof identification goes, Tien argues that the body by itself contains unique identifying characteristics that can be effectively confirmed by biometric technologies. These characteristics include fingerprints, irises, DNA and facial angles. As for tracking, Tien points out that using a bracelet in situations where such tracking is unavoidable, is sufficient, and that implantation just isn't a logical necessity in most civilian situations.

"We don't like it. We're very concerned. And we hope this thing falls apart," Tien concluded.

ADS has now changed the name of their GPS trackable device from Digital Angel to PLD—Personal Location Device. □