2020-06-18 15:30:04.048711

UPLOADERS SIGNATURE

Name—Nickname—Pseudonim of the uploader
Mr. Beauregard

Did you digitise the file?
No, it is from JSTOR

How long did it take to scan?
0 minutes

Where was the source found?
This is republished from my own library

Why are you sharing this file?
You can tell an anecdote
You can leave a personal message!

All the JSTOR papers downloaded while writing my thesis are now de-watermarked and republished to Library Genesis. These are the first republished papers from my graduation application, Tactical Watermarks. Tactical Watermarks, is an online republishing platform. I actively make use of digital watermarks as a means to explore topics such as anonymity, paywalls, archives, and provenance. While the primary intention of analogue watermarks was to leave traces of authenticity, marks of quality or even aesthetic enhancements, digital watermarks are being used as a way to create accountability for users. Through this platform, I describe and document ways of living within and resist a culture of surveillance in the realm of publishing.

REPUBLISHED THROUGH

TACTICAL WATERMARKS

Resisting Surveillance: Identity and Implantable Microchips

Nancy Nisbet

ABSTRACT

Surveillance technologies and centralized databases are threatening personal privacy and freedom. Radio Frequency Identification (RFID) microchip technology is one of several potential human tracking and authentication systems. The author's interactive art installation *Pop! Goes the Weasel* aims to explore opportunities for resisting surveillance by altering underlying assumptions concerning identity. Viewers are encouraged to experiment with resistance by avoiding access control, intervening in the database and subverting notions of a stable or single identity. The author is planning a future project to develop an interface between the author's two implanted microchips and her computer in order to track her computer usage as it relates to her technology-induced shifting sense of self.

There is no power relation without the correlative constitution of a field of knowledge, nor any knowledge that does not presuppose and constitute at the same time power relations.

—Michel Foucault [1]

Although surveillance of human behavior is not new, technological developments and heightened concern over public security are increasingly facilitating, and arguably justifying, ubiquitous surveillance. Leading contenders in contemporary social surveillance systems include: the establishment of national ID cards, the use of biometric identifiers and, potentially, the implantation of identifying microchips. Perhaps the most serious risk to personal privacy and freedom that any of these systems pose is through the possible development of an involuntary centralized or interconnected database. The implementation, control of access, and restrictions of use of such information repositories have many privacy advocates concerned [2,3]. The trend toward the convergence of diverse databases of collected information in North America and elsewhere recalls Bentham's Panopticon [4] and the specter of coercion that emerges in Foucault's analysis of power and knowledge in a disciplinary society.

My concern with the limits and risks of the explosion of surveillance technologies prompted me to undertake an artistic exploration of a particularly threatening system, that of implanted radio-frequency identification microchips. *Pop! Goes the Weasel,* an interactive art installation first presented at the Inter-Society for Electronic Art (ISEA) symposium in Nagoya, Japan, in October 2002, is the first of several artworks that I have undertaken to this end.

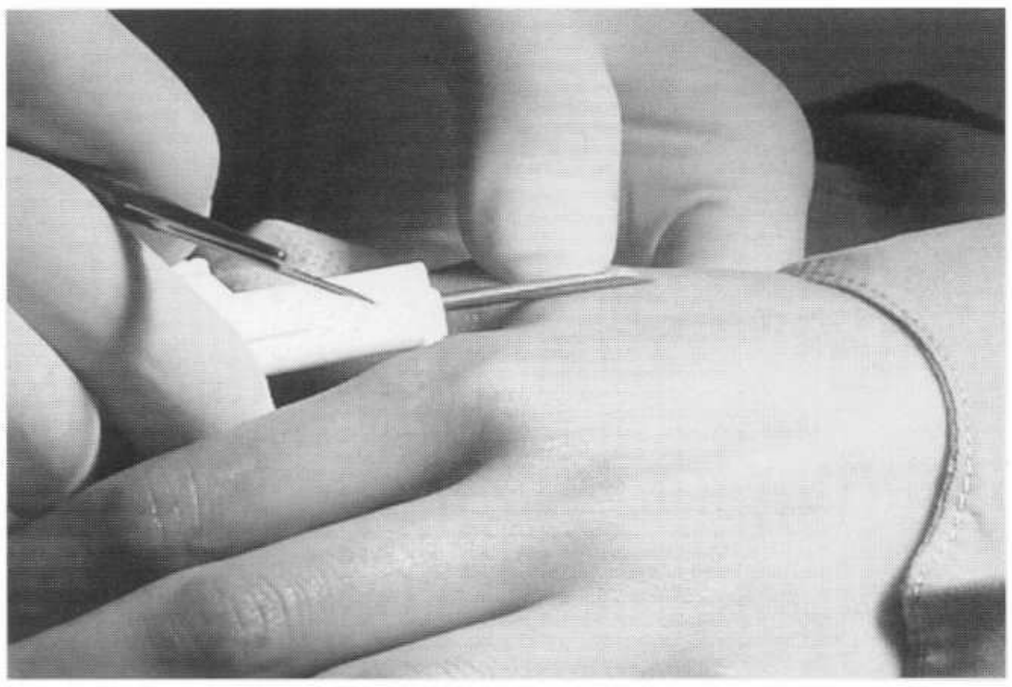
***2001–2002**: I have two microchips implanted in my body—one in the back of each hand. The first was injected in October 2001 (Fig. 1) and the second in February 2002* [5].

Radio Frequency Identification Technology

Since the 1980s, Radio Frequency Identification Technology (RFID) [6] has developed to the point that today it is widely used in tracking and access applications. It is a wireless system commonly used for livestock and pet identification as well as automated vehicle identification systems such as toll roads and parking garages. RFID technology has the potential to drastically alter human surveillance. As microchips get smaller and power supply issues [7] are resolved, forms of human surveillance that invade the body will increase. Some human bioengineering research in the United Kingdom already uses implanted RFID technology [8]. In October 2002, the United States Federal Drug Administration's apparent [9] decision that RFID microchips used for nonmedical applications do not need FDA approval for implantation into humans [10] significantly bolstered corporate interest. Applied Digital Solutions, Inc. (ADS) is marketing external [11] human tracking devices such as the wristwatch-like Digital Angel and the internal VeriChip for "a variety of security, financial, emergency identification and healthcare applications" [12].

***2001**: I approached four surgeons and a veterinarian and asked whether or not they would agree to perform the microchip implantation for artistic research purposes. The vet agreed to supply me with the microchip but refused to inject it into me. One surgeon did not reply to my message. The second declined. The third agreed on condition that the Canadian Medical Association sanctioned the procedure. The fourth simply agreed.*

Fig. 1. A surgeon implants an RFID microchip into the artist's left hand with a specially designed needle, October 2001. (© Nancy Nisbet)



Nancy Nisbet (artist, educator) #403, 6333 Memorial Road, University of British Columbia, Vancouver, BC V6T 1Z2, Canada. E-mail: <nnisbet@interchange.ubc.ca>.

Based on a paper presented at ISEA 2002, 11th International Symposium on Electronic Art, Nagoya, Japan, 27–31 October 2002.

Article frontispiece. Photograph of workman's hand, C-print, 11 inches in diameter, 2001. Detail from *Pop! Goes the Weasel.* (© Nancy Nisbet)

Identity and Microchip Implantation

For any surveillance or tracking data to be meaningful it must be associated with a particular person, location or thing being observed; ultimately, it is a process that relies on some form of identification. The dystopic futures of much science fiction are only too replete with the tracking and controlling of humans through surveillance implants. Such fictions are becoming science, and the future is imminent [13,14].

Deciphering and altering the underlying assumptions of a system can enable disruption of that system. Some of the assumptions of identity upon which surveillance relies are: that a person's identity is singular, that one's identity is constant and unchanging, that identity has a fundamental connection to the body and, finally, that identity is ascertainable.

I had two chips implanted into my body because of the assumption that each surveyed person has one unique ID number—not two: one chip, one person and one unique code. Surveillance relies on minimizing confusion and keeping one's boundaries clear. I implanted only two chips because it takes only two to create a binary system—like the zeros and ones of computer code. With exactly two chips I am able to "code for" an infinite number of identities just through the sequence in which they are scanned.

2000: Wanting to push beyond the spectacle of the implantation of a microchip, I struggled to come to a point of departure—to make a bold and playful entrance into a resistance to corporate- or government-sanctioned surveillance.

Pop! Goes the Weasel—Installation Details

There are four main components of this installation: access gates, photographs, video projection and the RFID scanning system (Fig. 2). The viewer first encounters one of two RFID-controlled gates that allow passage into and out of the installation space. Those viewers choosing to wear an RFID microchip badge will be able to "unlock" the gates, while those without a badge will be locked out (Fig. 3). Five black circular pedestals, each topped with a transparent, backlit photograph of a hand against a background of surgical green silk, are interspersed in the installation. The five hands (Color Plate A No. 2) resemble those of an elderly woman, a gentleman, a patient, an elegant woman and a workman (article frontispiece). Projected on one wall is a short video loop documenting the surgical implantation of a microchip into my hand inter-cut with images of the five hands described above (Fig. 4). The background audio of the video is an almost unrecognizably warped interpretation of the nursery rhyme "Pop! Goes the Weasel" alternating with a medical-sounding beep. The final and crucial underlying component of this installation is the RFID scanning system. The installation houses eight RFID antennae, one hidden under each photograph, one visible at each gate, and the last one in a smaller sixth pedestal that exposes the wiring and scanner of the RFID system. The scanner at this last location is programmed to display, in real time, the viewer's badge ID number at the bottom of the video projection. As someone with a RFID badge approaches the gates or any of the pedestals, the antenna will detect the badge's unique ID number and store viewer-tracking data (ID number, date, time and location) in a database [15]. The presence of an RFID badge at one of the photograph pedestals will also activate a light in the bottom of the pedestal to illuminate the image.

***1997**: At a dinner party with friends, I was introduced to the use of microchips to track fish. The disturbing thought of using such microchips for human surveillance took root in my mind.*

Pop! Goes the Weasel—Objectives

The installation presents issues of surveillance as they relate to identity and the body. It is a site of experimentation with surveillance resistance strategies involving possible avoidance, intervention and subversion of the system.

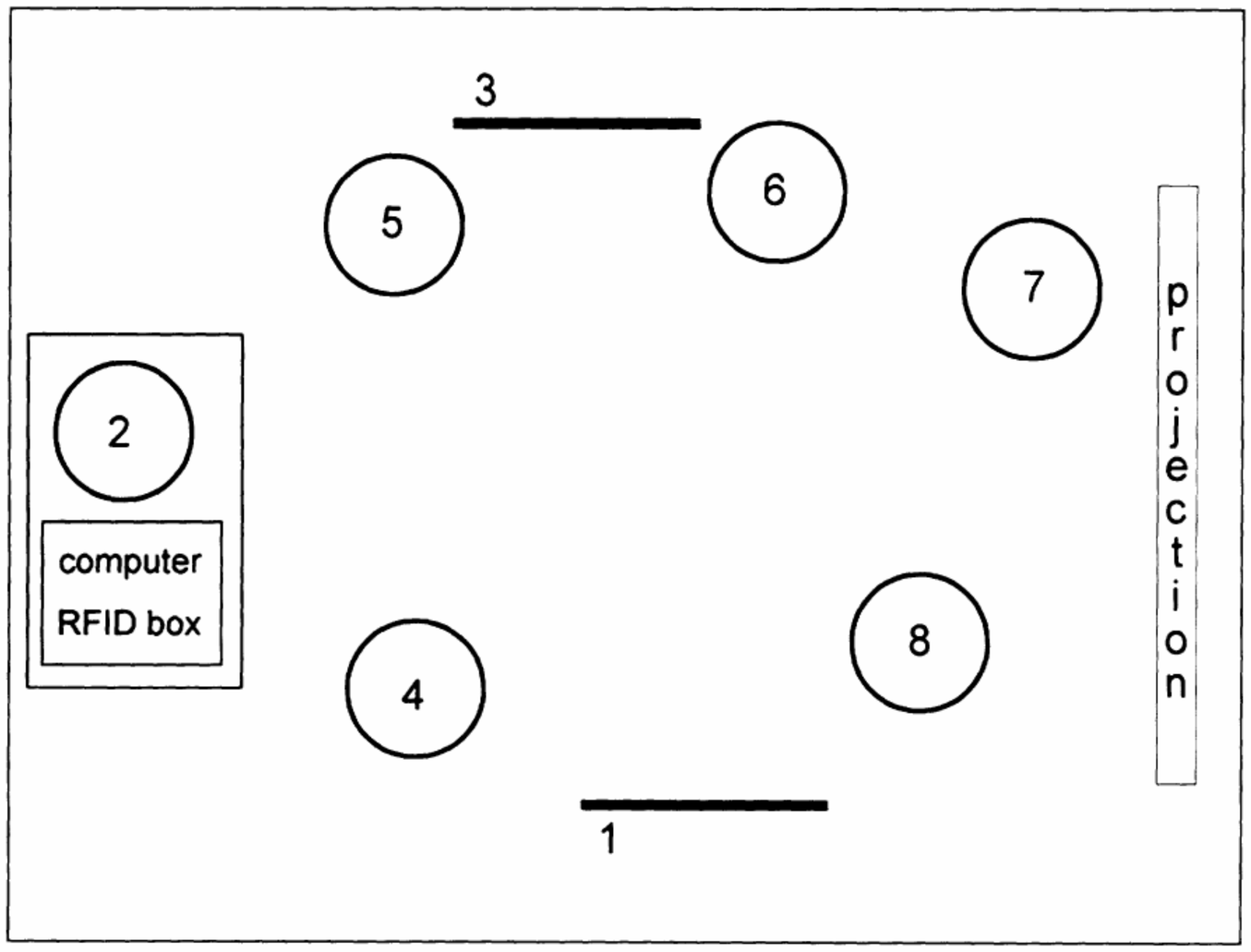
When no one was looking, a gentleman crawled under the gate.

Avoidance: Although the gates suggest restricted access, they are actually "leaky" and allow motivated visitors to discover ways to circumvent the access control.

A workman hurried over to the photograph before the light went out.

Intervention: A forthcoming component of future installations will enable the viewer to effect direct intervention in the surveillance database itself. The small pedestal where the electronics are visible will be the site where the visitor may alter some of the collected information. Each microchip badge is pre-programmed with a unique ID number. This number is associated with a database record that contains other information, such as name, occupation and country of residence. After scanning the badge to open the associated data record, visitors may change the name, occupation and country of residence associated with "their" card. This information remains linked to the card until another visitor adopts the card and changes the associated "identity" yet again.

Fig. 2. A diagram of *Pop! Goes the Weasel* as it was installed at the ISEA symposium in Nagoya, Japan, 2002. The numbers correspond to the locations of the eight antennae, the circles to the six pedestals. Pedestal 2 has a transparent lid; the antenna and associated wiring are visible. The photographs are located on pedestals 4–8. The heavy bars controlled by antennae 1 and 3 designate the electronic gates.



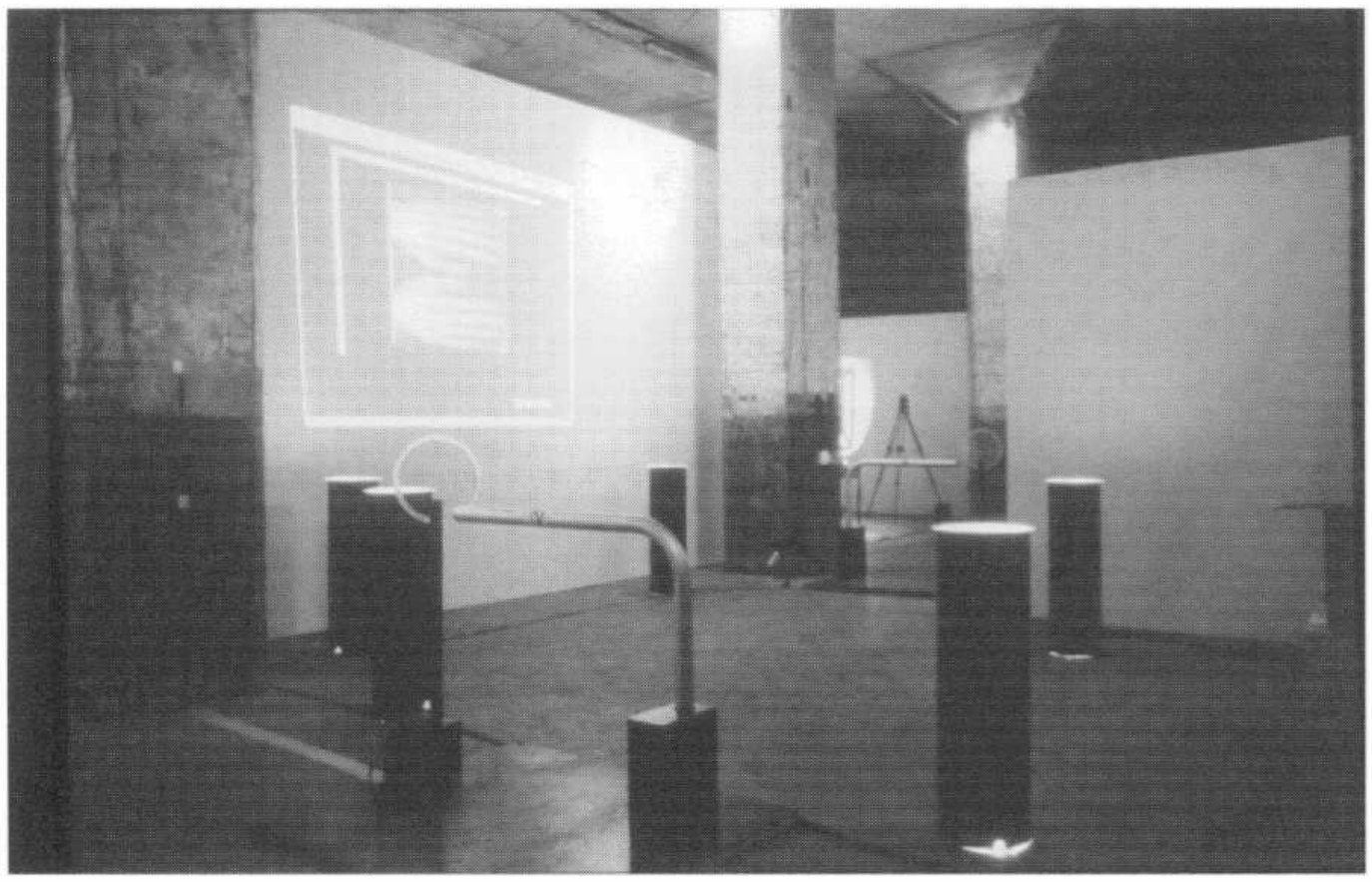


Fig. 3. *Pop! Goes the Weasel*, installation view. (Photo © Nancy Nisbet) One of the access gates is visible in the foreground. On the wall to the left is the projection of the video. The five photograph pedestals are visible in the mid-ground.

After the others left the installation, an elderly woman quietly altered the database.

Subversion: In the constant change in "whom" the data belongs to, identity is blurred (the data is associated with multiple people but with one ID badge), and the collected information becomes meaningless.

A lady covertly passed off her badge to another.

This installation aims to remind participants of the ubiquity of surveillance structures, encourage visceral responses to potential future modes of surveillance and allow visitors to practice intervening in and avoiding surveillance as possible forms of resistance. Already significantly conditioned to surveillance and authentication interfaces, visitors routinely placed their own hands upon the photographs. This connection is a form of self-implication. The hand that reaches out is also the hand surveyed. Whose hand is it? Is this person someone you know? Is it someone like you? Could it be you?

Further Work

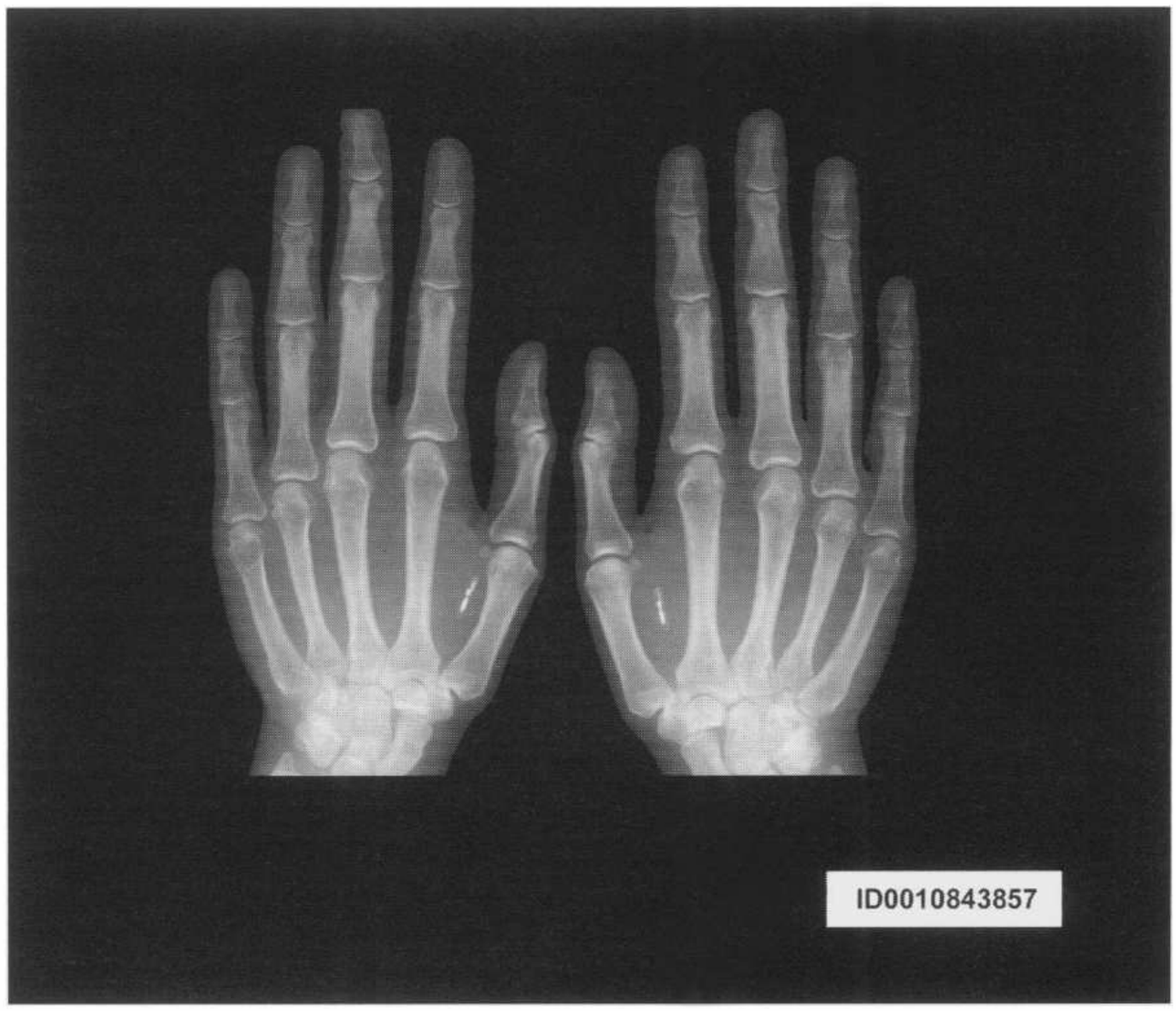
I am interested in the interface between the body and interactive informational technologies. Subjection of my body to the cultural coding and technical invasion of implanted microchips is fundamentally different from wearing them as an accessory like a watch or tattooing numbers on my body. I am interested in embodiment versus adornment. These chips are permanent, nontransferable and hidden, and they "talk" to certain machines.

In future work I will use my implanted microchips to interface with my computer and to track my identities as I travel in both physical and cyber spaces. I will use an RFID reader attached to my computer to scan the chips in my hands, depending on my perception of the nature of how I am using my computer at that moment. The scanning will initiate the collection of data for my own private database [16]. I have arbitrarily associated the chip in my left hand with my identity at play, while the chip in my right hand is associated with my identity at work [17]. I am interested in juxtaposing *where* "I" go inside my computer and cyberspace with *which* "I" is going there and *what* "I" am doing there. While collecting this "virtual" data, I will also record "real-world" observations. Using a GPS (global positioning system) unit, I will record my geographical coordinates; with a web cam I will document my physical surroundings. Where am I (is my body) when I go "*there*" in cyberspace? I want to explore the connections of my physical body and associated identity(ies) to my computer and my virtual identities. I will investigate the nature of these identities and how my perceptions of identity/self may be shifting.

Exploration and experimentation with the RFID human computer interface will have significant impact on the project. What is the experience of tracking my every computer encounter? How do I negotiate the conscious decisions to identify with one or another identity (as represented by chip ID number)? How does the performative aspect of using my system in public spaces such as cyber cafés, libraries, etc., influence the project—my notion of self, my awareness of self?

As a more public aspect of this work I plan to develop a scanner "detector." As RFID technologies become more widely

Fig. 4. A detail (video still of an x-ray of the artist's hands) of the projection in the installation. (© Nancy Nisbet) The top portion plays a video loop while the small box in the lower right corner displays the current badge ID number.



used, I may not be able to determine when my implanted chips are responding to hidden scanners. The scanner detector will ensure that I remain aware of my microchips' "conversations" with public surveillance devices: The detector will allow me to resist accordingly and play with the performative potential of such knowledge.

Conclusion

Tracking and identification systems are rapidly being developed: RFID technology is one of the forerunners of ubiquitous surveillance. I am interested in provoking questions about these authentication systems: How is identity ascertained/maintained? What are the hidden risks? Will chipping become mandatory? How will these systems be implemented? Who will have or control access to the information? What are the weaknesses that resistance can explore? *Pop! Goes the Weasel* aims to encourage resistance to surveillance structures by blurring viewer identities, by avoiding access control mechanisms, and by intervening directly in the database. My ongoing work will closely examine my personal microchip interface with the computer and playfully consider the resulting data with respect to my body and my perception of self.

Current concern for national security around the world reflects international political tensions and is one factor that has done much to bolster support for increased human surveillance and has brought such identification technologies to the forefront of discussion. It may be too late to prevent such pervasive and invasive technical developments, but it is not too late to demand protection for individual privacy and freedom. For all the benefits that may emerge from the digital "angels" being developed, there is the very real risk of their becoming the 21st century's all-too-watchful Big Brothers.

Acknowledgments

Special thanks is given to Grant Gregson, programming; David Floren, electronics; Jackie Seo, makeup effects; Rob Bos and Marina Roy, video and photography assistance; and to my friends and colleagues who offered their support. Project development continues in co-production with the Banff New Media Institute.

References and Notes

1. M. Foucault, *Discipline and Punish: The Birth of the Prison,* Alan Sheridan, trans. (New York: Pantheon, 1977) p. 27 (orig.: *Surveiller et Punir: Naissance de la prison* [Paris: Gallimard, 1975]).

2. Elaine M. Ramesh, "Time Enough? Consequences of Human Microchip Implantation," <http://www.fplc.edu/risk/vol8/fall/ramesh.htm>.

3. C.W. Crews, "Human Bar Code Monitoring Biometric Technologies in a Free Society," *Cato Institute Policy Analysis* No. 452, 1–20 (17 September 2002).

4. Jeremy Bentham, "Panopticon Papers," in Mary Peter Mack, ed., *A Bentham Reader* (New York: Pegasus, 1969) pp. 194–208. Bentham's Panopticon is a circular architectural model designed in 1791. The essence of its power is that it allows seeing without being seen.

5. J. Scheeres, "New Body Art: Chip Implants," <http://www.wired.com/news/culture/0,1284,50769,00.html>, 11 March 2002.

6. An RFID system is composed of three parts: an antenna, a reader (transceiver) and a unique radio frequency microchip (transponder or RF tag). The reader sends a pulse to the antenna that emits radio signals of a specific frequency (134 kHz, in this case) to activate a microchip. Power generated from the transceiver allows the passive microchip to relay its ID information back to the reader and positively identify the object or individual. See <http://www.aimglobal.org/technologies/rfid/what_is_rfid.htm>.

7. Currently, RFID microchips used in animals, and in a few people, are passive (have no power supply), and reading of the ID number can only occur at a maximum distance of about 5 feet. If these microchips could be powered and still remain small enough for implantation, it would enable tracking over larger distances.

8. Kevin Warwick of the Cybernetic Intelligence Research Group at the University of Reading in the U.K. has used microchip implants in his bioengineering research on interfacing with the nervous system via RFID; <http://www.rdg.ac.uk/KevinWarwick/html/project_cyborg_1_0.html>.

9. It is noteworthy that subsequent to the ADS press release, the FDA issued a warning letter to ADS Inc. on 8 November 2002, indicating that in marketing the chip for medical benefit, "the VeriChip is adulterated . . . or misbranded" under the Federal Food, Drug, and Cosmetic Act"; <http://www.fda.gov/foi/warning_letters/g3668d.htm>. This points to conflicting statements issued by ADS to the media and to the FDA—one wonders why ADS feels this "misbranding" is necessary. One must also question the FDA's evident lack of concern over the implantation of such a device into humans for any reason.

10. ADSX Press Release, 22 October 2002, announcing the FDA's permission to use implanted microchips for "security, financial and personal identification or safety applications": <http://www.adsx.com/news/2002/102202.html>.

11. "The Digital Angel Safety and Location Systems surpass ordinary location-enabled devices. Only Digital Angel alerts you to the exact location of people, pets and objects in real time"; <http://www.digitalangel.net>.

12. ADSX Press Release, 31 October 2002, announcing the use of VeriChip for the above-mentioned (see Ref. [10]) purposes, including "healthcare applications"; <http://www.adsx.com/news/2002/103102.html>.

13. J. Wilson, "Girl to Get Tracker Implant to Ease Parents' Fears," 3 September 2002; <http://www.guardian.co.uk/uk_news/story/0,3604,785071,00.html>.

14. "Fla. Family Takes Computer Chip Trip," 10 May 2002; <http://www.cbsnews.com/stories/2002/05/10/tech/main508641.shtml>.

15. The functioning of the installation occurs primarily behind the scenes. The surveillance system designed for this installation consists of eight antennae, two RFID readers and many RFID microchip badges. Five of the antennae are contained within the photograph pedestals; two are visible at the gates, and the eighth antenna is visible through the transparent top of a sixth, shorter, pedestal located beside the computer and RFID system box (Fig. 2).

16. In this project I am not becoming a passive subject of others, but remain empowered and pro-active in the representation and interpretation of my identity(ies).

17. Rather than affirming a dualistic approach to understanding identity, the choice of assigning the microchips with "work" and "play" was made in recognition of widespread familiarity with shifts in one's identity(ies) between that expressed in workplace environments and that predominating when engaging in play. The tracking project is not limited to these two versions of my identities but will expand over time to track several identities.

Nancy Nisbet is a Canadian artist who works with new media, installation, performance and photography. Her current artistic and academic practice broadly concerns human relationships with technology and human relationships mediated by technology. She is an assistant professor in the Department of Art History, Visual Art and Theory at the University of British Columbia in Vancouver, Canada.