

Brian Larson Clark

**Abstract:** In this paper, both the emergence and the problems of ubiquitous surveillance structures are explained. Through this explanation, solutions to these problems are proposed on three fronts: educational, legislative, and tactical.

## **Disarming the Panopticon: Understanding and Neutralizing Electronic Surveillance Structures Through Tactical Intervention**

For decades, the notion of a “surveillance society” where every facet of our private life is monitored and recorded has sounded abstract, paranoid or far-fetched to some people. No more!... Yet too many people still do not understand the danger, do not grasp just how radical an increase in surveillance by both the government and the private sector is becoming possible ... from a number of parallel developments in the worlds of technology, law and politics. (Stanley and Steinhardt 2003: iv)

**Surveillance structures are everywhere.** They permeate both our public and private lives. They record our credit card transactions. They are embedded into consumer goods. They follow us through public places. They compile logs of our cell phones calls. The ubiquitous invasion of surveillance structures into our lives is problematic on many different fronts as they infringe on our privacy and surreptitiously dictate our daily actions and relationships. They exist as neo-panopticons for the specific purpose of control.

[T]he major effect of the Panopticon [is] to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers (Foucault 1977: 201).

Surveillance structures actively reappropriate the boundary of what is public and what is private. The invisibility of this reappropriation is problematic. Surveillance increasingly falls in the periphery of our attention. It has to circumvent attention to prevent the surveilled from constant awareness of the challenges that surveillance places onto their lives. Through this awareness, popular rejection of surveillance loses its foundation. Therefore surveillance structure are most effective as furtive systems, blending into the environments that they invade.

Paranoia concerning these systems should be replaced with knowledge and understanding. There is a need to bring surveillance structures into public consciousness. For the public to have the traction to dictate how surveillance should be implemented, how these structures operate should be part of common knowledge in order to challenge and critique them.

In this paper, I will shine light on the emergence of the ubiquitous nature of RFID and EAS surveillance structures and how they are implemented in our lives, the dangers of this technology, and suggest tactical interventions to combat the panoptic structure of these

systems.

### **The Barcode and EAS**

To a certain extent, the barcode system demonstrates many of the fundamental aspects of ubiquitous surveillance systems. Barcodes, present on both consumer objects and identification licenses, possesses symbols which can be read as individuated data connected to an object or individual.

The application of ubiquitous tracking of commerce is not new. Before the implementation of RFID, barcodes remained the predominant method of commodity tracking. Barcodes have the ability to identify a specific objects during the moment of scanning (transaction). Their data produces an inscription which serves as an indicator of dynamic artifactual data, revealing when an item is out of stock, when an item is purchased, and so forth. Fortunately, barcodes as purely graphic symbols lack the ability to be remotely sensed therefore are unable to function as an surveillance devices.

On the other hand, electronic article surveillance (EAS) is used purely as a shop-lifting deterrent (see fig.1). It consists of a magnetic tag module that triggers an alarm as it passes through a tactically placed magnetic transponder. As an EAS tag enters the magnetic field, the magnetic resonance is detected, triggering an alarm. This technology has existed in the consumerist setting since the mid-1970's. The ability of an EAS tag to be remotely detected, make it desirable in a setting where surveillance is a concern. However, the EAS systems have no way to individuate different tags as EAS tags contain no data.

Enter RFID.

During the development and refinement of RFID technology in the mid-1970's, the potential ability for RFID to take on the functions of both a barcode and a EAS system caught the attention of the commercial sector. This ability to concurrently track commerce and to identify an individual tag sparked an interest that has fueled the development of current ubiquitous RFID technologies.

### **What is RFID?**

Standing for Radio Frequency Identification Device, RFID is an automatic identification method in which information is stored in a transponder device (commonly referred to as a 'tag' – see fig.2). A RFID tag contains a silicon chip coupled with an antenna which enables it to respond to a radio frequency produced by an RFID transceiver. An RFID transceiver (or reader) is a device that emits a radio frequency and waits for a radio signal reflection of an individual RFID tag.

Every RFID tag contain its own unique identification number. Most RFID tags can only be read while others have the ability to have their identification numbers changed through the communication with the transceiver.

### **The Threat of RFID to Privacy**

"Privacy is a psychological as well as a social and political requirement. For instance, people seek control over the degree of anonymity they possess in their relationships by choosing what personal information to reveal to another person based upon their relationship (Ingram 1978)."

Paired with an ubiquitous computing structure, RFID poses direct challenges to an individual's privacy. "RFID tags represent a move towards smaller and smaller units of tracking. These tags are also programmed with certain information which can be particular to each tag. As Foucault's flock was broken into individual trackable and predictable sheep

and then regrouped at will, the development of these tags opens the possibility of a more detailed and intimate control. This makes Deleuze's point that the current historical framework is not interested in unique individuals confessing their truth but connected units being scanned for their code (Cameron 2005)."

The size and prevalence of this RFID technology opens up new paths of surveillance unaccessible by previous surveillance systems. With RFID being implemented in both consumerist and state institutions, the ability for the use of RFID against the interest of the general public becomes a grave concern. There are multiple qualities of RFID technology that can be deployed for malicious purposes. These purposes explained below in more detail are outlined by [Privacyrights.org](http://Privacyrights.org):

**Hidden Tags.** The size of RFID opens up the possibility of tags to be hidden in an object without the knowledge of the individual who possesses it. With the mode of communication between the tag and the receiver being radio waves, these waves can easily pass through fabrics and plastics and remain invisible to the naked eye.

The use of hidden tags is already being exercised in such stores as Abercrombie and Fitch. In such stores, RFID tags are permanently sewn into a hem of the clothing and can not be removed without physically cutting the fabric. Additionally, RFID has been known to be hidden within electronic devices including the casing of cell phones.

**Hidden Receivers.** The reading range of RFID receivers are determined by the size and power of the antenna. Because of this, receivers can be placed at a distance out of sight to the public. Receivers can be incorporated into any space, including public spaces where people assemble and congregate. Inside malls, EAS systems are already hidden underneath floors and within walls. Fortunately, this strategy has not been implemented with RFID systems.

**Tag Singularity.** Every RFID tag possesses its own unique identification number. Known in the commerce world as the EPC (Electronic Product Code), these identification numbers give the ability to differentiate individual RFID-embedded objects. Paired with an electronic registration system, RFID-embedded objects can be linked directly to the purchaser's personal data.

**Monolithic Data Aggregation.** The use of RFID in ubiquitous structures encourage the creation of monolithic databases that collect individualized data. This data can be linked to other databases, such as personal financial information, without an individual's knowledge or consent.

**Individual Tracking and Profiling.** To expand the idea of data aggregation, data can be used for the purpose of profiling an individual without their knowledge. An item of clothing, or an electric device, such as a cell phone, can be associated with an individual giving a surveiller the ability to track a specific individual.

### **Latour, Data Aggregation, and Inscription**

In the discussion of monolithic data accumulation in ubiquitous surveillance structures, Latour becomes relevant. "In Latour's later work, he tackled the process by which these inscriptions travel throughout the world and are used to create new knowledge. According to Latour, inscriptions (through some mysterious homing instinct) tend to accumulate within particular locations that Latour refers to as "centres of calculation". Centres of calculation are essential for 'acting at a distance':" (Goodall)

"...how to act at a distance on unfamiliar events, places and people? Answer: by somehow bring home these events, places and people. How can this be achieved, since they are distinct? By inventing means that (a) render them mobile so that they can be

brought back; (b) keep them stable so that they can be moved back and forth without additional distortion, corruption or decay, and (c) are combinable so that whatever stuff they are made of, they can be cumulated, aggregated or shuffled like a pack of cards." (Latour, 1987, 223)

"In the pantheon of inscriptions that are both created by and stored within centres of calculation, Latour ranks the equation as the pre-eminent example of the genre (particular Reynolds's equation for fluid mechanics). Equations are inherently very mobile and very combinable. Through the use of equations, centres of collection are transformed to centres of calculation." (Goodall)

Ubiquitous surveillance structures epitomize this notion of inscription storage within centers of calculation. As credits cards are swiped and as EZ-Pass systems are triggered, information is created and stored in computational nodes. This aggregation of quantitative information can be interpreted to create new information and conclusions. This has already been exercised in the case of EZ-Pass.

### **EZ-Pass: An Example of State RFID Surveillance**

"To survive, the spectacle must have social control. It can recuperate a potentially threatening situation by shifting ground, creating dazzling alternatives- or by embracing the threat, making it safe and then selling it back to us" - Larry Law, from The Spectacle

EZ-pass is an active RFID system that has recently demonstrated the trend towards individual tracking. When an individual orders a free EZ-Pass, he is required to open up a bank account in which the EZ-Pass identification number is connected. The EZ-Pass number is not only connected to the bank account number, but also to a license plate number and a driver's license number. Additionally, these numbers are connected to other identification numbers such as a social security numbers, and insurance numbers.

The purpose for the EZ-Pass bank account number is to have a financial account from which to automatically deduct toll charges (hence, you don't have to stop to pay), but by going through an EZ-Pass booth, the Thruway Authority has the ability to collect other artifactual information about your passing, such a time.

The EZ-Pass system seems like an ingenious and useful service as it is pitched to the unassuming commuter as a system that reduces traffic waiting time. This is absolutely true, but this is just a superficial benefit as commuters unknowingly embrace a potential threat to their private information.

Not only does EZ-Pass save money for the State by reducing the number of toll booth employees, but this technology can be used to attain traffic data and store it directly into a database. Through EZ-Pass, such questions be answered more efficiently: How many people go through this exit at a given time period? At what times it traffic flow heavy? How frequently does an individual use the Thruway system? What is the average milage an individual drives on the road? These may be innocent questions, but there are more menacing ones to be considered.

Because EZ-pass has the ability to gather data in real-time, it has the potential to collect the time when one enters the road system, and when one exits the road system. Through a simple mathematical formula, the average speed of a car can be acquired. This technology then has the potential to create an instant speeding ticket. Or let say an individual with a Hummer decides to drive over the side fence and skip off the roadway

prematurely. The EZ-Pass system would be able to realize something is incorrect with its data. How about if the EZ-pass database is hooked up to the DMV database and finds out that a car registration is expired, or the car is stolen, or the owner has a bench warrant? Can EZ-pass be used as an extension of law enforcement? The answer simple: it already is.

### **Preemptive Action to Deter RFID Abuse**

To prevent the abuse of RFID surveillance technology, a preemptive and contentious strategy is necessary. A commonly debated strategy is one that requires awareness and action by legislative institutions. Three important rules as suggested by Privacyrights.org suggest that the following criteria should be implemented in the form of legislative action:

**Tag Transparency.** Institutions or individuals using RFID systems must make their policies and practices involving the use of their systems public. Individuals have the right to know if products that they acquire contain a part of a RFID system. They also have the right to know the technical specifications of that device. Additionally, institutions have to disclose the purpose of their RFID systems

**Collection Limitation.** Collection of information derived for RFID devices should be limited to information that is considered necessary.

**Accountability.** Institutions or individuals that misuse RFID technology for the purpose of secretly attaining for private information for malicious purposes should be held accountable for their actions.

### **Public Awareness of Surveillance Structures**

To bring surveillance systems into public awareness, there has to be both an attempt to educate the public and an attempt to map the surveillance systems. This strategy has been explored in both iSee by Tad Hirsh and Zapped! by Preemptive Media. In iSee, Hirsh demonstrates the mapping of surveillance cameras for the purpose of public awareness. While iSee deals with qualitative video surveillance, Zapped! deals directly with the mapping of quantitative RFID systems with the goal to educate the public.

"Zapped! takes a close look at—and a new approach to—the mass deployment of Radio Frequency Identification (RFID). RFID is not yet a household name or a pervasive technology, but Preemptive Media predicts that everyday encounters with this technology (whether known or not) will soon be commonplace. Zapped! is an effort to learn about and respond to the tags that industry is embracing for product tracking, the government for border control, schools for attendance-taking and public libraries for automatic checkout (Preemptive Media)."

Preemptive Media has covered a lot of conceptual ground through their desire to educate the public about RFID. They hold Zapped! workshops which teach how to build RFID devices. Additionally, they have published an educational workbook, a school pack, and video documentation which is publicly available online. Like Hirsh's iSee, Zapped! has also made an attempt to compile a map; specifically a map of the presence of RFID devices in Tokyo.

Zapped! demonstrates progress in the attempt to understand RFID surveillance, but more ground needs to be covered as a proactive and comprehensive strategy to disable these structures does not exist.

### **Disarming the Panopticon**

Without a legislative framework in place, the consideration to disable surveillance structures through tactical intervention becomes an issue. To explore tactics to defuse the panoptic structures of surveillance technology, one must give a serious look at shoplifters as a conceptual seed for research and development. Through the tactics that they employ

for illegally obtaining goods, they are essentially operating outside the vision of surveillance. In the act of undermining surveillance, four shoplifting methods become relevant:

**Radio Jamming.** Radio Jamming is the act of transmitting radio signals for the purpose of disrupting communication between receivers and transceivers. Limor Fried's creation of a low-power RF jamming device entitled "Wave Bubble" (see fig. 3) demonstrates the possibility of jamming in a public environment.

Even though the Fried interest is to reappropriate personal space through the disruption of cellular phone signals in an immediate vicinity of the device, 'it can be easily tuned to disrupt RFID, GPS, WiFi or any other RF communications system (Fried, 26).'

Interestingly, the market for jamming devices is also thriving as 'companies have been formed solely for the purpose of developing high-power 'cell phone jammers' (Fried, 27).'

Even though the use of 'active' jammers of this nature is explicitly illegal according to FCC regulations<sup>1</sup>, the use of jammers in the confines of government and corporate institutions is not being enforced. Jammers are becoming more common in courtrooms, business meeting rooms, and other spaces where the use of cell phones would be disruptive.

Jamming technology in the hands of the average citizen could be a powerful defense against the invasion of ubiquitous surveillance if the popular attitude toward surveillance soured. In the scenario where a significant percentage of the population is carrying around jamming devices around in their pockets, the nature of surveillance industry would be temporarily disabled and would be forced to react and evolve.<sup>2</sup>

**Radio Shielding.** While jamming employs an active signal to disrupt the communication between a transceiver and a receiver, shielding passively blocks the communication link by preventing a signal from reaching the receiver.

Shoplifters go about this through the utilization of a metal pouch acting as a Faraday cage. In a scenario where this tactic is used, a shoplifter would place an object of interest in the metal pouch and walk out of a store. The metal in between the transmitter and the receiver acts as a barrier, disrupting communication between the two modules.

**Tag Saturation.** Anti-shoplifting devices still have technical flaws. They give 'false positives.' A false positive is the event of an anti-shoplifting device errantly triggering an alarm when there is not a tag present.

In the security tag industry, the term 'tag pollution' is commonly used to describe the event of a rogue tag activating alarms in multiple businesses as it is transported through a marketplace environment. When a consumer exits a store with an active security tag and enters other stores setting of multiple alarms, tag pollution creates not only audible annoyances, but also bureaucratic annoyances. According to some store policies, every alarm event must be logged in a database and pursued according to company standards.

To employ this tactic in an interventionist situation, the action would play upon the vulnerabilities of the EAS system, giving the tag-holder a tactical stronghold to disarm a surveillance structure by injecting an atmosphere of chaos. If tag pollution is regularly employed on a mass scale, current commercial panoplic and procedural structures would be disabled.

How does this apply to shoplifters? The tactic that they employ is to surreptitiously place tagged clothing into another consumers possession. As that consumer leaves the store, the alarm is triggered, creating a distraction, and giving the shoplifter a window to make an escape.

Compatible EAS tags can be acquired inexpensively on online auction websites including Ebay. The acquisition of massive amount of these tags is therefore legal and

simple to do. Because of the compatibility standards of EAS, any version of these tags operate in an array of stores. In many larger chain stores such as Wal-Mart and Target, EAS systems are sensitive to all standards of EAS.

The accessibility and standardization of EAS tags bring forth the possibility of these tags to be massively distributed in a consumerist area such as a mall for the purpose of saturating EAS systems. Through a mass distribution of these tags to the crowd, the crowd itself could act as the distributive vehicle for saturating these systems. Not only would an action like this, trigger alarms, but it would bring instant public awareness to surveillance through the process of alienation.

**Evasion.** Evading surveillance is the most obvious way of avoiding detection. An effective way to deal with ubiquitous surveillance is to know where that surveillance is located and avoid it whenever possible. Tad Hirsch and the Institute of Applied Autonomy advocates this method through the creation of iSee.

"iSee is an application for web-browsers and PDAs that charts the locations of closed-circuit television (CCTV) surveillance cameras in urban environments. With iSee, users can find routes that avoid these cameras ("paths of least surveillance") allowing them to walk around their cities without fear of being "caught on tape" by unregulated security monitors."

This tactic is effective dealing with structures such as EZ Pass. If EZ-Pass was required on all vehicles, the vascular spans of the highway system poses many alternative paths conducive for avoiding the EZ-Pass surveillance.

### **Identifying, Cleaning Up, and Distorting Informational Artifacts**

With RFID and similar ubiquitous control systems playing a more predominant role in society in recent years, tactics to identify, critique, and undermine this technology becomes increasingly necessary. With RFID chips embedded in everything from credit cards to clothing, the surveilled is becoming increasingly vulnerable to the exposure of private data.

As we move through both physical and virtual spaces throughout our daily routines, we are leaving behind our data artifacts. These artifacts implicitly expose our actions, not only to the eyes of authoritarian structures, but to the masses itself. Anyone with enough ambition to track down data on an individual can usually find an access point with a simple Google search.

If it is of social importance to keep data private, not only does it become important to educate the population about the existence of personal data artifacts, but it also becomes important to encourage the practice of 'personal informational hygiene.' Initially, this may seem a little absurd, but for an individual to inject the practice of cleaning up their informational entrails in their daily life, that individual's ability to protect his privacy is enhanced.

In situations where data artifacts can not be kept private, a more proactive approach may be required. Previously, I alluded to Limor Fried's cell phone jamming device. In the case of embedded RFID tags where removal is difficult, jamming devices of this type would prove quite effective.

The concept of jamming could be brought a step further. Jamming a transponder becomes problematic because of the visibility of the action. If the realization that transponders are not reading data due to jamming, a red flag is sent up that there is a problem, and the development of more robust transponders will be undertaken.

A more implicit action could be derived from the concept of jamming: distorting. Instead of blatantly disabling a device from collecting information, why couldn't a technique be implemented where an data artifact is swapped with a different 'false' artifact.

By bringing this up, the idea of encryption comes into mind. What I am referring to is NOT at all encryption. There is a big difference between distortion and encryption. In

encryption, data is put through an algorithm for the purpose of being deciphered. Distortion on the other hand is the act of changing data so there is no decipherable artifact. Distortion could be referred to as a technological 'red herring' by substituting a real artifact with a false one with the intent to lead a surveillance system down a different path.

To better articulate this idea, I will present a real-world example:

Let's say that an individual, I will name him Mike, received his credit card statement in the mail. He opens the envelope, reads it, and then discards it. The question of how he discards his credit card statement becomes the crux of my point:

Mike could be careless, or perhaps ignorant of identity theft, so he throws the mail directly in the trash. Through this action he makes himself vulnerable to be surveilled as a stranger pokes through his trash as it sits on the curb.

In another scenario, Mike uses a paper shredder to destroy his information, therefore covering up the artifact of his personal data. In this case, the paper shredder acts as the jammer, blocking strangers from reading his data. But in our data-dependent consumerist world the stranger may have the ambition to realize and respond to the destruction of the artifact and deduce a technique to reassemble it.

In a third scenario, Mike throws his credit card statement away, but not before changing the data on it, in a way that it is incorrect, but maintaining the general semantics. When the stranger goes through the trash this time, he acquires the false credit card statement, not knowing that it is false, therefore unable to question, respond, and adapt.

A device that would obscure data artifacts such as presenting an irrelevant RFID number to a RFID receiver could be an effective way to combat RFID surveillance structures in the future. Even though this tactic could be uncovered by the surveillers, the aspect of uncertainty is inserted into the mix as the fidelity of data is compromised.

### **Sousveillance (Panoptic Reflectionism)**

"All such activity has been surveillance: organizations observing people. One way to challenge and problematize both surveillance and acquiescence to it is to resituate these technologies of control on individuals, offering panoptic technologies to help them observe those in authority. We call this inverse panopticon "sousveillance" from the French words for "sous" (below) and "veiller" to watch." (Mann, Nolan, Wellman)

Sousveillance, a neologism coined by Steve Mann, could serve as an additional proactive tactic to engage surveillance structures. Sousveillance, being the opposite of surveillance, is described as a "watchful vigilance from underneath." A more basic definition is 'the act of surveilling the surveillers.' As this concept applies to video surveillance, sousveillance has resulted in the public turning the camera back onto law enforcement, governmental officials, and other authority units.

*EyeTap*, invented by Steve Mann, is an example of wearable computing sousveillance device. A camera is worn over the eye for the purpose of watching what the human eye is watching. Additionally, cameras such as ACM's *CFP2005*, is a camera affixed to a wearable vest that can be worn in public places.

In the case of RFID structures, sousveillance can be extended to the tagging of items important to the taggers. In the marketplace, the people trade capital for RFID tagged commodities. Sousveillance in this scenario may involve additionally tagging capital in return for tagged commodities. It is very possible to utilize this tactic since RFID tags come in forms that are flat, small, and sticky. The ubiquitous framework in this case would have to be constructed, but the action of tagging money without a ubiquitous framework could serve as protest, spreading RFID awareness to anybody in possession of tagged money. As for as

the concern of the legality of such an action, this is not a case of defacing money, since tags can be removed.

### **Conclusion**

The public's complacency and unawareness to RFID technology incapacitates them from presenting a formidable challenge to the potential problems that may arise out of this technology. To approach this problem, challenges to this emerging technology should be approached on three fronts: public awareness, legislative action, and a plan for tactical intervention. It is through these fronts that vulnerabilities created by surveillance can be effectively challenged, helping to preserve individual privacy through the emergence of ubiquitous technologies.

## **References**

Cameron, H (2005) CCTV and (In)dividuation. *Surveillance & Society* vol. 3 issue 2  
Ingham, R. (1978) *Privacy and Psychology*. New York: John Wiley & Sons

Fried, L (2005) *Social Defense Mechanisms: Tools for Reclaiming our Personal Space*. MIT Thesis

Foucault, M. (1977). *Discipline and Punish*, A. Sheridan (Trans.). New York: Vintage.  
Goodall, G. (2004). *Inscriptions*. <http://www.deregulo.com/facetation/2004/09/inscription-ive-been-avoiding-this-bit.html>

Hirsh, T (2002). *iSee*. Institute for Applied Autonomy. <http://www.appliedautonomy.com/isee.html>

Latour, B., & Woolgar, S. (1979). *Laboratory Life : The Construction of Scientific Facts*. Thousand Oaks: CA: SAGE.

Latour, B. (1987). *Science in action : how to follow scientists and engineers through society*. Philadelphia, PA: Open University Press.

Mann, S., J. Nolan and B. Wellman (2003) *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*. *Surveillance & Society* vol. 1 issue 3

Preemptive Media (2005). *Zapped!*. <http://www.zapped-it.net>

"RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (2003)." Privacy Rights Clearinghouse. <http://www.privacyrights.org/ar/RFIDposition.htm>

"SmartEAS Solutions (2006)." <http://www.sensormatic.com>

Stanley, J. and B. Steinhardt (2003) *Bigger monster, weaker chains: the growth of an American surveillance society*. Washington: Technology and Liberty Program, American Civil Liberties Union.

## Notes

1. The operation of transmitters designed to jam or block wireless communications is a violation of the Communications Act of 1934, as amended ("Act"). See 47 U.S.C. Sections 301, 302a, 333. The Act prohibits any person from willfully or maliciously interfering with the radio communications of any station licensed or authorized under the Act or operated by the U.S. government. 47 U.S.C. Section 333. The manufacture, importation, sale or offer for sale, including advertising, of devices designed to block or jam wireless transmissions is prohibited. 47 U.S.C. Section 302a(b). Parties in violation of these provisions may be subject to the penalties set out in 47 U.S.C. Sections 501-510. Fines for a first offense can range as high as \$11,000 for each violation or imprisonment for up to one year, and the device used may also be seized and forfeited to the U.S. government

2. In analyzing tactical strategies, the framework of electronic article surveillance (EAS) systems come back into play because of their predominance in the marketplace. The current usage of these structures serve as a logical precursor to how RFID will eventually be implemented.



Fig. 1 - A collection of EAS tags

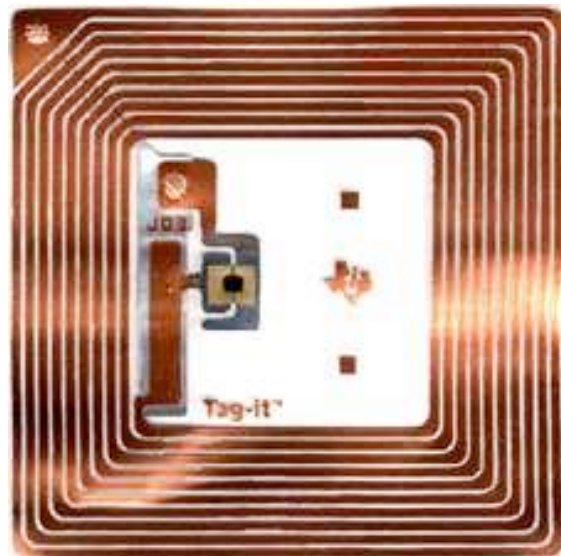
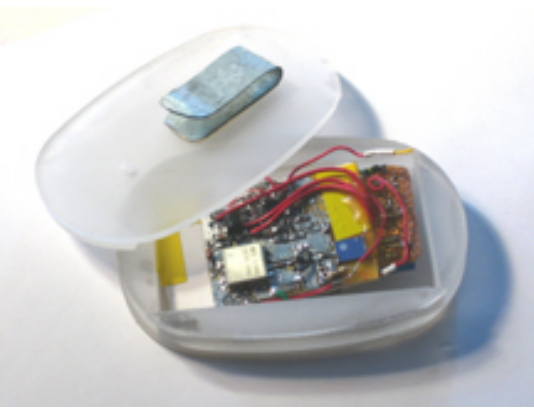


Fig. 2 - An RFID Tag



**Fig. 3 - Fried's "Wave Bubble"**