GlobalResearch
Center for Research on Globalization

“Smart Cards” in a Surveillance Society: The Implanted Radio-Frequency Identification Chip

RFID tags implanted in physical objects or human beings

By Tom Burghardt
Global Research, February 02, 2013
Antifascist Calling and Global Research 6 September 2008

Region: USA
Theme: Police State & Civil Rights

If incorporating personal details into an RFID (radio-frequency identification) chip implanted into a passport or driver’s license may sound like a “smart” alternative to endless lines at the airport and intrusive questioning by securocrats, think again.

Since the late 1990s, corporate grifters have touted the “benefits” of the devilish transmitters as a “convenient” and “cheap” way to tag individual commodities, one that would “revolutionize” inventory management and theft prevention. Indeed, everything from paper towels to shoes, pets to underwear have been “tagged” with the chips. “Savings” would be “passed on” to the consumer. Call it the Wal-Martization of everyday life.

RFID tags are small computer chips connected to miniature antennae that can be fixed to or implanted within physical objects, including human beings. The RFID chip itself contains an Electronic Product Code that can be “read” when a RFID reader emits a radio signal. The chips are divided into two categories, passive or active. A “passive” tag doesn’t contain a battery and its “read” range is variable, from less than an inch to twenty or thirty feet. An “active” tag on the other hand, is self-powered and has a much longer range. The data from an “active” tag can be sent directly to a computer system involved in inventory control–or surveillance.

But as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) state in a joint **position paper**, “RFID has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties.” As these organizations noted:

While there are beneficial uses of RFID, some attributes of the technology could be deployed in ways that threaten privacy and civil liberties:

> * **Hidden placement of tags**. RFID tags can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items. As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases, and more.
>
> * **Unique identifiers for all objects worldwide**. The Electronic Product Code potentially enables every object on earth to have its own unique ID. The use of unique ID numbers could lead to the creation of a global item registration

system in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer.

* **Massive data aggregation**. RFID deployment requires the creation of massive databases containing unique tag data. These records could be linked with personal identifying data, especially as computer memory and processing capacities expand.

* **Hidden readers**. Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being "scanned."

* **Individual tracking and profiling**. If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe could serve as a de facto identifier for the person wearing it. Even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies. ("Position Statement on the Use of RFID on Consumer Products," Privacy Rights Clearinghouse, November 14, 2003)

RFID under the skin

As the corporatist police state unfurls its murderous tentacles here in the United States, it should come as no surprise that securocrats breathlessly tout the "benefits" of RFID in the area of "homeland security." When linked to massive commercial databases as well as those compiled by the 16 separate agencies of the "intelligence community," such as the Terrorist Identities Datamart Environment (TIDE) that feeds the federal government's surveillance Leviathan with the names of suspected "terrorists," it doesn't take a genius to conclude that the architecture for a vast totalitarian enterprise is off the drawing board and onto the streets.

As last week's mass repression of peaceful protest at the Republican National Convention in St. Paul amply demonstrated, the Bush regime's "preemptive war" strategy has been rolled out in the *heimat*. As the *World Socialist Web Site* **reports**,

> On Wednesday eight members of the anarchist protest group the Republican National Convention Welcoming Committee (RNCWC) were charged under provisions of the Minnesota state version of the Patriot Act with "Conspiracy to Riot in Furtherance of Terrorism."

> The eight charged are all young, and could face up to seven-and-a-half years in prison under a provision that allows the enhancement of charges related to terrorism by 50 percent. …
>
> Among other things, the youth, who were arrested last weekend even prior to the start of the convention, are charged with plotting to kidnap delegates to the RNC, assault police officers and attack airports. Almost all of the charges listed are based upon the testimony of police infiltrators, one an officer, the other a paid informant. (Tom Eley, "RNC in Twin Cities: Eight protesters charged with terrorism under Patriot Act," World Socialist Web Site, 6 September 2008)

As the ACLU pointed out, "These charges are an effort to equate publicly stated plans to blockade traffic and disrupt the RNC as being the same as acts of terrorism. This both trivializes real violence and attempts to place the stated political views of the defendants on trial," said Bruce Nestor, president of the Minnesota Chapter of the National Lawyers Guild. "The charges represent an abuse of the criminal justice system and seek to intimidate any person organizing large scale public demonstrations potentially involving civil disobedience," he said.

An affidavit filed by the cops in order to allow the preemptive police raid and subsequent arrests declared that the RNCWC is a "criminal enterprise" strongly implying that the group of anarchist youth were members of a "terrorist organization."

Which, as we have learned over these last seven and a half years of darkness, is precisely the point: keep 'em scared and passive. And when they're neither scared nor passive, resort to police state tactics of mass repression. While the cops beat and arrested demonstrators and journalists outside the Xcel Energy Center, neanderthal-like Republican mobs chanted "USA! USA!" while the execrable theocratic fascist, Sarah Palin, basked in the limelight. But I digress…

Likened to barcodes that scan items at the grocery store check-out line, what industry flacks such as the Association for Automatic Identification and Mobility (**AIM**) fail to mention in their propaganda about RFID is that the information stored on a passport or driver's license is readily stolen by anyone with a reader device–marketers, security agents, criminals or stalkers–without the card holder even being remotely aware that they are being tracked and their allegedly "secure" information plundered. According to a blurb on the AIM **website**,

Automatic Identification and Mobility (AIM) technologies are a diverse family of technologies that share the common purpose of identifying, tracking, recording, storing and communicating essential business, personal, or product data. In most cases, AIM technologies serve as the front end of enterprise software systems, providing fast and accurate collection and entry of data. ("Technologies," Association for Automatic Identification and Mobility, no date)

Among the "diverse family of technologies" touted by AIM, many are rife with "dual-use" potential, that is, the same technology that can keep track of a pallet of soft drinks can also keep track of human beings.

Indeed, the Association touts **biometric identification** as "an automated method of

recognizing a person based on a physiological or behavioral characteristic." This is especially important since "the need" for biometrics "can be found in federal, state and local governments, in the military, and in commercial applications." When used as a stand-alone or in conjunction with RFID-chipped "smart cards" biometrics, according to the industry "are set to pervade nearly all aspects of the economy and our daily lives."

Some "revolution."

The industry received a powerful incentive from the state when the Government Services Administration (GSA), a Bushist satrapy, issued a 2004 memo that urged the heads of all federal agencies "to consider action that can be taken to advance the [RFID] industry."

An example of capitalist "ingenuity" or another insidious invasion of our right to privacy? In 2006, IBM obtained a patent that will be used for tracking and profiling consumers as they move around a store, even if access to commercial databases are strictly limited.

And when it comes tracking and profiling human beings, say for mass extermination at the behest of crazed Nazi ideologues, IBM stands alone. In his groundbreaking 2001 exploration of the enabling technologies for the mass murder of Jews, communists, Roma and gays and lesbians, investigative journalist Edwin Black described in *IBM and the Holocaust* how, beginning in 1933, IBM and their subsidiaries created technological "solutions" that streamlined the identification of "undesirables" for quick and efficient asset confiscation, deportation, slave labor and eventual annihilation.

In an eerie echo of polices being enacted today against Muslims and left-wing "extremists" by the corrupt Bush regime in their quixotic quest to "keep America safe" in furtherance of capitalist and imperialist goals of global domination, Black **writes**:

> In the upside-down world of the Holocaust, dignified professionals were Hitler's advance troops. Police officials disregarded their duty in favor of protecting villains and persecuting victims. Lawyers perverted concepts of justice to create anti-Jewish laws. Doctors defiled the art of medicine to perpetrate ghastly experiments and even choose who was healthy enough to be worked to death–and who could be cost-effectively sent to the gas chamber. Scientists and engineers debased their higher calling to devise the instruments and rationales of destruction. And statisticians used their little known but powerful discipline to identify the victims, project and rationalize the benefits of their destruction, organize their persecution, and even audit the efficiency of genocide. Enter IBM and its overseas subsidiaries. (IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation, New York: Crown Publishers, 2001, pp. 7-8)

As security and privacy analyst Katherine Albrecht **writes** describing IBM's patented "Identification and Tracking of Persons Using RFID-Tagged Items in Store Environments,"

...chillingly details RFID's potential for surveillance in a world where networked RFID readers called "person tracking units" would be incorporated virtually everywhere people go–in "shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, [and] museums"–to closely monitor people's movements. ("How RFID Tags Could Be Used to Track Unsuspecting People," *Scientific American*, August 21, 2008)

According to the patent cited by Albrecht, as an individual moves around a store, or a city center, an "RFID tag scanner located [in the desired tracking location]… scans the RFID tags on [a] person…. As that person moves around the store, different RFID tag scanners located throughout the store can pick up radio signals from the RFID tags carried on that person and the movement of that person is tracked based on these detections…. The person tracking unit may keep records of different locations where the person has visited, as well as the visitation times."

Even if no personal data are stored in the RFID tag, this doesn't present a problem IBM explains, because "the personal information will be obtained when the person uses his or her credit card, bank card, shopper card or the like." As Albrecht avers, the link between the unique RFID number and a person's identity "needs to be made only once for the card to serve as a proxy for the person thereafter." With the wholesale introduction of RFID chipped passports and driver's licenses, the capitalist panoptic state is quickly–and quietly–falling into place.

If America's main trading partner and sometime geopolitical rival in the looting of world resources, China, is any indication of the direction near future surveillance technologies are being driven by the "miracle of the market," the curtain on privacy and individual rights is rapidly drawing to a close. Albrecht writes,

China's national ID cards, for instance, are encoded with what most people would consider a shocking amount of personal information, including health and reproductive history, employment status, religion, ethnicity and even the name and phone number of each cardholder's landlord. More ominous still, the cards are part of a larger project to blanket Chinese cities with state-of-the-art surveillance technologies. Michael Lin, a vice president for China Public Security Technology, a private company providing the RFID cards for the program, unflinchingly described them to the New York Times as "a way for the government to control the population in the future." And even if other governments do not take advantage of the surveillance potential inherent in the new ID cards, ample evidence suggests that data-hungry corporations will.

I would disagree with Albrecht on one salient point: governments, particularly the crazed, corporate-controlled grifters holding down the fort in Washington, most certainly will take advantage of RFID's surveillance potential.

In 2005 for example, the Senate Republican High Tech Task force praised RFID applications as "exciting new technologies" with "tremendous promise for our economy." In this spirit, they vowed to "protect" RFID from regulation and legislation. Needless to say, the track record of timid Democrats is hardly any better when it comes to defending privacy rights or something as "quaint" as the Constitution.

Under conditions of a looming economic meltdown, rising unemployment, staggering debt, the collapse of financial markets and continuing wars and occupations in Iraq and Afghanistan, U.S. imperialism, in order to shore up its crumbling empire, will continue to import totalitarian methods of rule employed in its "global war on terror" onto the home front.

The introduction of RFID-chipped passports and driver's licenses for the mass surveillance and political repression of the American people arises within this context.

Tom Burghardt *is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly, Love & Rage and Antifa Forum, he is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by* ***AK Press****.*

Articles by: **Tom Burghardt**
http://antifascist-calling.blogspot.com/