

433MHz

Military Systems compatible with Tracking Student Locator RFID

July 2013

(updated January 2014)

By Pippa King

Active RFID tracking systems devised by military-industrial corporations, such as Lockheed-Martin and Honeywell, are being installed in schools and colleges. These systems go beyond the capacity to monitor student attendance; some schools have already used this data to study social [peer relationships](#) – who spend time with whom. These RFID systems use the same frequency as a global US/NATO- military system for tracking assets, tracking tags of this frequency to within [positional accuracy](#) of [1 meter](#). The military system does not stop working at the school gate and the tags do not cease transmitting outside the school. Data of this accuracy is sensitive. Schools make assurances that this data will be kept private but ‘tuned in’ sensors anywhere can pick up a tags frequency, sensors that the military system have with the same frequency compatibility. Consequently, assurances of privacy to keeping personal data and tag location within schools appear worthless.

The RFID used is 433.92Mhz. [Savi](#), a company owned until September 2012 by [Lockheed Martin](#), developed the 433MHz RFID technology [ISO18000-7](#), ratified in 2004 based on Savi’s patented technology, and have [supplied homeland-security and port-related](#) RFID to the US military during the past decade. According to the [RFID Journal](#), “*Savi RFID tags track assets in shipments throughout the world. Its customers include the U.S. government, as well as [NATO](#) and*

other civil and defense agencies”. Savi “*has been the [primary provider of active RFID solutions for the Department Of Defense, particularly in the agency’s \[In-Transit Visibility Network\]\(#\), which monitors the movements of containers and products through the supply chain by means of 433 MHz active RFID tags, readers and software.](#)*”

In 2006 [Savi announced](#) an intellectual property (IP) licensing programme for RFID ISO18000-7 (433MHz) products, called Quick Start. This was for companies to supply and manufacture the RFID standard. In 2007 seven companies, mostly commercial rather than defence, [signed up](#). Following that in January 2009 the US Department of Defence announced a [\\$429 million RFID contract](#), RFID III, for ISO18000-7 devices, which was awarded to Savi and several other companies. “*It was agreed that current self-certification of interoperability was insufficient [between the companies awarded the contract] and that a more formalized process for determining conformance with the ISO 18000-7 standard and [interoperability](#) across vendors was needed*” – From [DASH7 Alliance wiki](#). Upon RFID III being awarded, Savi initialized the first meeting of DASH7 members in February 2009.

With NATO having 28 member countries and US Military deployed in over 150 countries, 433MHz sensors/active RFID devices are positioned globally for their In-Transit

Visibility Network and with this; 433MHz frequency finds itself firmly embedded globally in society – with the ability to track the active 433 RFID tags carried by students.

In 2012 a 15 year old student, Andrea Hernandez, from San Antonio Texas, [chose not to be tracked](#) by 433 MHz RFID device enforced on the students in [John Jay High School](#) by [Northside Independent Schools District](#). The active RFID tags were worn round the student's neck in a lanyard and emitted a pulsed constant frequency which could not be turned off by the students, effectively broadcasting the student's, or the tags, whereabouts 24-7. Andrea's refusal resulted in her being expelled from John Jay High School after [losing a legal appeal](#) to stay at the school untagged. She attended another school not using RFID tags for a short period of time. She returned back to John Jay High School after the RFID tracking system was scrapped in July 2013 as it was not cost effective.

In the first instance of [implemented active RFID student tracking in the UK](#), students at [West Cheshire College](#) were [tagged from 2010 to 2013](#) with an active ultra wideband (UWB) RFID tag worn around their neck on a lanyard for a Real Time Location System (RTLS), supplied and pioneered by [Zebra Technologies](#) for the [IEEE 802.15.4f](#) standard ([approved February 2012](#)), also [compatible with 433MHz](#).

This UWB RFID was installed [at the college by Honeywell](#) and was [admittedly used by college staff to study peer-relationships](#) amongst school children. After a series of [Freedom of Information requests](#), sent late 2012 and early 2013, in which the college could [not provide evidence](#) of gaining consent from students (or parents) to track the students, the brand new IEEE802.15.4f standard ultrawide band RFID was scrapped in February 2013. West Cheshire College was instructed by the UK Information Commissioners Office, which oversees the Freedom of Information Act, to provide

answers to Freedom of Information requests after receiving complaints about the procedures followed implementing this RFID Real Time Location System.

Also venturing into the schools market is [GuardRFID](#). They [recently announced](#), May 2013, of their [plans to provide](#) active (433MHz) RFID to schools. These tags can be worn on a lanyard "[or be attached to a student's garment or knapsack](#)". GuardRFID, who [joined the DASH-7](#) alliance in 2010, [also supply](#) the "*US Department of Defense for Active RFID applications that empower the military to manage global logistics and assets*". They are also "*currently driving the global standards for IEEE 802.15.4f and ISO18000-7 and is well-positioned to deliver standards-compliant RFID infrastructure and tags*". This is the technology students can look forward to carrying with GuardRFID's foray into the education sector.

A month later in June 2013, Oregon passed bill [HB2386](#) specifically allowing schools to use active RFID to track students, paving the way for its use in Oregon's education system even though no schools in that state yet use RFID student tracking technology. These events, along with an ever increasing use of RFID to track school assets and school buses, indicate a significant turn in the market for RF based student's location systems.

With 433MHz ISO18000-7 being used to track the next generation, what are we dealing with here? This 433MHz is active RFID and has many features. Unusual for active RFID, DASH7 433 is able to receive as well as transmit, with an ability to cover long [distances of 1-2KM](#) (up to 10km in some circumstances). 433MHz also has the capability to communicate with passive RFID at 13.56MHz, the contactless smartcards we carry in our wallet such as cash cards, travel cards, biometric passports and Near Field Communication RFID devices in 'smart' phones. The reason being is that 433.92MHz is harmonically compatible with 13.56MHz – 13.56 multiplied by the number 32 is 433.92 -

DASH7 RFID can utilise the same antennae used by 13.56MHz.

DASH7 433 also gives a new sense of visibility, [readied for the Internet of Things](#), with its capacity for internet Protocol Version 6 ([IPV6](#)). Everything on the internet will have its own IP address. In preparation for this, IPV6 allows for 3.4×10^{38} (340 trillion, trillion) unique IP addresses whereas the current IPV4 only has approximately 4.3 billion. The visibility of this frequency and the global network it can utilize is far reaching and something to bear in mind when interacting with 433MHz and 13.56MHz.

Radio Frequency technology is here and is ever more becoming part of our society. As with all newly emerging 'tools' we can manage those tools if aware of what it is we use. If are we to carry RFID tags we can at least inhibit their ability to communicate by enclosing them inside metal foil, in [RFID safe wallets](#) – more difficult though to apply this to active RFID tags sewn into [school garments](#), [rucksacks](#) and [wristbands](#). Unless we resist this, we will become subject to ubiquitous surveillance.

RFID is a silent, hidden technology where we

place reliance and trust in the information given to us with regards to the sharing capacity of the devices we carry. With this technology there is a constant and subconscious interaction, unlike any interaction with data sharing we have had before.

There is a global network of RFID sensors using sympathetic and harmonic frequencies capable of interacting with the RFID we carry and it seems that the youngest in our society are being habituated to its use, much as they are with [their use of biometric technology](#) in schools.

When we or our children have an item that 'magically' interacts with other pieces of technology perhaps start questioning what it is we carry and trust, hope, that we are being given the full and correct answer. However, taking steps to measure or refuse interaction with this technology is an option available to us and the power of how we relate to it is in our hands.

Read our website for more details and put a stop to our children from being used as surveillance test-rats.

Pippa King

Parent from the UK whose children were nearly fingerprinted in 2005 when they were 6 and 7 years old for a school library system. After asking the Head Teacher when the school was going to obtain consent from parents she was told that the school did not need to ask our permission to take her children's fingerprint. The Head Teacher was correct.

The UK [Data Protection Act 1998](#) does not consider biometric data as [Sensitive Personal Data](#). In order for UK schools to store and process a child's Sensitive Data, parental consent must be sought. As biometric data is not considered to be 'sensitive', schools in the UK can take a child's biometrics without informing parents.

She campaigned from 2005 along with other parents, with the help of privacy sector organisations, for parents to have openness and transparency from schools with an option to 'opt in' and schools not to presume parental consent by (sometimes) offering an 'opt out'.

The [Protection of Freedoms Act 2012](#) was passed in May 2012 which requires, in [chapter 2 clauses 26-28](#), for schools to gain written parental consent if they wish to store/process a child's biometric data as of 1st September 2013.

Against RFID in schools www.rfidinschools.com
'Biometrics in schools' blog www.pippaking.blogspot.com