Issued By:
Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)
Electronic Privacy Information Center (EPIC)
Privacy Rights Clearinghouse

Endorsed By These Organizations:
Electronic Frontier Foundation (EFF)
FoeBuD e.V., Big Brother Awards Germany
Constitutional Alliance
PrivacyActivism
[More to be added]
[See end of document for individual endorsements.]

Contents:

I. Introduction

As organizations and individuals committed to the protection of privacy and civil liberties, we have come together to issue this statement on the use of RFID in schools for the tracking and monitoring of students, teachers, and staff. In the following pages, we describe RFID technology, define the risks associated with its use, and discuss potential public policy approaches to mitigate the issues raised.

II. RFID Tracking Technology

Radio Frequency Identification (RFID) is a tracking technology with profound societal implications.

"RF" stands for "radio frequency." Like the radio waves that transmit sound to an AM radio, RFID radio waves can travel through walls and doors. "ID" stands for "identification," since RFID is designed to identify, track, and monitor physical objects.

RFID systems have two main components:

RFID tags and
RFID readers

RFID tags are tiny computer chips connected to miniature antennas that can be affixed to physical objects or living creatures. RFID tags can also be embedded in objects or injected hypodermically under the skin of humans and animals.

Typically, an RFID tag contains a microchip programmed with a unique identification number used to identify the tagged object or individual. In this way, RFID numbers are similar to Social Security numbers. But unlike Social Security numbers or bar codes which must be seen to be read, RFID tags can transmit data silently through the air, unhindered by doors, walls, backpacks, purses, or clothing.

RFID tags can be either passive or active. Passive RFID tags do not have a power source of their own, so they lie dormant until stimulated by a radio signal from an external reader device. Active RFID tags contain an on-board power supply, so they actively transmit their data.

The second component of an RFID system is the reader device. The reader either emits or picks up electromagnetic energy in a particular frequency to retrieve stored data from nearby RFID tags. In both passive and active systems, this request and response process is both silent and invisible.

Passive RFID tags can be read from a distance of less than an inch to up to 100 feet or more, depending on their frequency, the size of their antenna, and the power of the reader. Active (self-powered) tags can have a much longer read range.

Typically, the data collected by RFID readers is sent to one or more computer databases. The "Internet of Things" is a conceptual framework in which the unique ID number of a particular tag would serve as an address under which all known sightings and information about the tag and its owner would be stored. In this way, a tag could be tracked through thousands of readings by strategically placed reading devices. These readings can be recorded and analyzed to identify patterns of movement and behavior.

RFID may be used to trigger additional monitoring devices, like video cameras and audio recording systems. For example, a central database could be instructed to trigger a recorder when select RFID tags are identified in a specified location. This can make more in-depth tracking and monitoring of selected objects and individuals possible.

III. Threats to Privacy and Civil Liberties in Schools

RFID was initially designed as a very powerful inventory and animal tracking technology. RFID systems are now being marketed to schools as a way to extend inventory tracking to individuals. These proposed applications include incorporating RFID tags into school ID cards or mandatory clothing items, like uniforms, in order to track the attendance, whereabouts, and movements of

students, teachers and staff. RFID-tagged items (e.g. computers, library books, textbooks etc.) may be used to indirectly monitor individuals along with the items. RFID may also be used for cashless payment in cafeterias, vending machines, and transit systems, among others.

The 2003 ***Position Statement on the Use of RFID on Consumer Products***, endorsed by over 40 of the world's leading privacy and civil liberties organizations, clearly established that RFID should never be used for tracking people. We now come together to specifically address the inappropriateness of using RFID to track students, teachers, and staff in schools.

RFID tracking violates expectations of reasonable privacy and threatens civil liberties in our schools:

- Dehumanizing uses: While there is an expectation of supervision and guidance in schools, monitoring the detailed behaviors of individuals can be demeaning. For example, RFID reading devices in school restrooms could monitor how long a student or teacher spends in a bathroom stall.

- Violation of free speech and association. RFID tracking software can monitor associations of RFID tags, which could dissuade individuals from exercising their rights to freedom of thought, speech and association. For example, students might avoid seeking counsel when they know their RFID tags will document their presence at locations like counselor and School Resource Officer (SRO) offices.

- Violation of conscience and religious freedom. Many individuals object to RFID systems on the basis of their deeply held philosophical or religious beliefs. Schools are required to make accommodations for students on the basis of these beliefs.

- Unauthorized use. While RFID systems may be developed for use in a school, the RFID tags may be read covertly anywhere by anyone with the right reading device. Since RFID reading devices work by silent, invisible radio waves and the reading devices can be hidden, unauthorized or covert uses can be nearly impossible to detect. In addition, information collected on systems could be shared or compromised without individuals' knowledge or consent. For example, a student's location could be monitored from a distance by a jealous girlfriend or boyfriend, stalker, or pedophile. Individuals run this tracking risk any place they carry or wear a school-issued RFID tagged item—even miles from the campus.

- Hidden placement of tags. RFID tags can be embedded into/onto objects like books 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. Monitoring tagged items could amount to unreasonable search.

- 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 in

bathroom fixtures, floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into shelving and counters, making it virtually impossible for someone to know when or if he or she was being "scanned."

- Dangerous misinformation. Relying on RFID for security rather than human observation creates new security risks. Hacking, spoofing and metal can easily defeat these systems. Wrapping an RFID tag in tinfoil or putting it in one of the latest metal wallets can make it unreadable. Hacking, spoofing, and tag loss are also risks. For example, a student could be counted as present on campus by virtue of his or her RFID identity tag, but be miles away before his or her disappearance were noticed. It would be possible for a kidnapper to abduct a student and the system to be unaware if a student's RFID tag were left on campus. In another example, a student could frame another student by placing a copy of another student's tag in the vicinity of a campus crime. RFID security experts have demonstrated that RFID tags can be cloned within seconds.

- Potential health risks. RFID systems emit electromagnetic radiation, and there are lingering questions about whether human health might be affected in environments where the reading devices are pervasive. This concern and the dehumanizing effects of ubiquitous surveillance may place additional stress on students, parents, and teachers.

- Conditioning to tracking and monitoring. Young people learn about the world and prepare for their futures while in school. Tracking and monitoring them in their development may condition them to accept constant monitoring and tracking of their whereabouts and behaviors. This could usher in a society that accepts this kind of treatment as routine rather than an encroachment of privacy and civil liberties.

IV. Framework of RFID Rights and Responsibilities in Schools

This framework recognizes a school's responsibility to keep students safe while respecting individuals' rights to maintain their dignity, privacy, and civil rights. To mitigate the potential harmful consequences of RFID to individuals and to society, we recommend a three-part framework.

First, RFID systems proposed must undergo a formal safety, technology, and privacy impact assessment, and schools should not implement RFID systems until this assessment takes place.

Second, RFID implementation must be guided by Principles of Fair Information Practice.

Third, certain uses of RFID should be flatly prohibited.

Safety, technology and privacy impact assessment. RFID must be subject to a formal safety, technology, and privacy impact assessment process, sponsored by a neutral entity, perhaps similar to the model established by the now defunct Congressional Office of Technology Assessment. The process must be multi-disciplinary, involving all stakeholders, including parents and students.

Principles of Fair Information Practice. RFID technology and its implementation must be guided by strong fair information practices (FIPs). The Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) (http://www.oecd.org/) provides clear guidance, as does the White House Consumer Privacy Bill of Rights (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf). We agree that the following minimum guidelines, based on these documents, must be followed if schools choose to adopt RFID systems:

- Public Warnings/Openness. RFID reading devices and RFID tags in schools should be clearly identified and their uses explained. Warnings should be posted in any areas where a device that could be triggered by an RFID system is located. For example, an RFID triggered recording device should be clearly labeled. Schools must detail the intended uses of data collected through RFID systems and how and where the data will be stored.

- Awareness/Purpose Specification. All stakeholders, including students, parents, and school employees, should be informed about how RFID systems work and the implications of having RFID systems deployed in schools before they are asked to consent to RFID tracking. This must include information about intended uses of the RFID systems and potential unintended consequences, like unauthorized access to databases and off-campus tracking.

- Choice/Consent. Schools should obtain informed, express written consent from individuals who agree to participate in school RFID tracking systems. In the case of students, both the parent and the student should provide consent. This consent should remain on record. Schools should also provide a way for individuals to revoke this consent.

- Collection/Use Limitation. The collection of information should be limited to that which is necessary for the purposes at hand. Information should only be used for the stated purposes.

- Access/Participation. Participants in school RFID tracking systems must be given access to data collected about them through these systems so they can ensure it is accurate and complete. Access to the data should be simple, timely, and at no charge. Participants must be provided a simple and timely mechanism that will allow them to correct data and products created from that data, like attendance and surveillance reports.

- Security Safeguards/Integrity. Schools should implement redundant managerial and technical measures to ensure the accuracy, security, and integrity of RFID systems and data. These measures should include an annual independent audit of each school's RFID systems and its compliance with fair information practices. Results of these audits should be made publically available to all stakeholders, including parents, students, and school employees.

- Accountability. Schools should provide a simple and effective way for individuals to address any grievances with a school's RFID systems, its compliance with stated policies, and its adherence to fair information practices. Parties harmed by school RFID systems should have the right to seek legal remedies and compensation for injuries, whether or not they provide informed consent to participate in these systems.

Prohibited RFID Practices

1. RFID systems on school grounds should not be used to track individuals or items associated with them without their informed, express, written consent. In the case of students, both the parent and the student must consent to the tracking.

2. No school should require or coerce an individual to provide consent in order to receive education services, employment, or participate in any school activities or incentive programs. Refusal to consent should not result in any punishment or other disciplinary action.

3. Individuals who refuse to participate in RFID tracking systems based on their belief systems should not be discriminated against or ridiculed for their beliefs.

4. Unless they opt into RFID systems, individuals should not be required to carry or interact with RFID-tagged objects. The implantation of an RFID tracking device should be prohibited.

5. RFID devices should not be covertly installed or hidden.

6. There should be no secret databases or secret sharing of data. Data should not be used for any commercial purpose or be shared with any outside entity or organization, including government entities.

7. System participants should not be denied reasonable access to their data, the right to correct their data, or the right to seek remedies should they be harmed by RFID systems or data.

V. Conclusions

Because of the serious privacy, health, and logistical downsides of RFID in schools, we believe there should be a moratorium on its deployment unless there is sufficient evidence of its safety and effectiveness. Children should never be used as test subjects for technology, no matter what their socio-economic status. If schools choose to move forward without complete information and are willing to accept the associated liability, they should have provisions in place to adhere to the principles of fair information practices and respect individuals' rights to opt out based on their conscientious and religious objections to the technology.

VI. BIBLIOGRAPHY

[1] Position Statement on the Use of RFID on Consumer Products. November 2003. Available online at http://www.spychips.com/jointrfid_position_paper.html.

[2] Katherine Albrecht & Liz McIntyre, Spychips: How major corporations and government plan to track your every purchase and watch your every move. Plume, October 2006.

[3] Youth Rights Manual. American Civil Liberties Union of Texas. July 2012. Available online at http://www.youthrightstx.org/e-books.html.

[4] Roger Brentnall, SE Horizon Scanning Intelligence Group Short Report. United Kingdom Health and Safety Executive. May 2007. Available online at http://www.hse.gov.uk/horizons/downloads/rfidsfreport.pdf.

[5] P.J. Hawrylak, N. Schimke, J. Hale, & M. Papa, Security Risks Associated with Radio Frequency Identification in Medical Environments. J. Med. Syst. November 2011. Available online at http://www.ncbi.nlm.nih.gov/pubmed/22048780.

[6] Human Inventory Control. Scientific American. April 25, 2005. Available online at http://www.scientificamerican.com/article.cfm?id=human-inventory-control.

[7] Katherine Albrecht, How RFID Tags Could Be Used to Track Unsuspecting People. Scientific American. September 2008. Available online at http://www.scientificamerican.com/article.cfm?id=how-rfid-tags-could-be-used.

[8] Radio Frequency Identification (RFID) Systems. EPIC. Available online at http://epic.org/privacy/rfid/.

[9] The Madrid Privacy Declaration. The Public Voice. November 2009. Available online at http://thepublicvoice.org/madrid-declaration/.

[10] Deborah Pierce, Networked: Carabella On The Run. 2009. Available online at http://www.nbmpub.com/comicslit/networked/.

VI. Signatories

Katherine Albrecht, Director, CASPIAN, http://www.spychips.com/
Media Inquiries: (877) 287-5854, kma@spychips.com

Liz McIntyre, Director of Communications, CASPIAN, http://www.spychips.com/
Media Inquiries: (877) 287-5854, liz@spychips.com

Marc Rotenberg, Executive Director, Electronic Privacy Information Center, http://www.epic.org
Media Inquiries: (202) 483-1140 x 106, rotenberg@epic.org

Beth Givens, Director, Privacy Rights Clearinghouse, http://www.privacyrights.org
Media Inquiries: (619) 298-3396, bethg@privacyrights.org

Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation, http://www.eff.org/
Media Inquiries: tien@eff.org

Katina Michael, University of Wollongong

MG Michael, uberveillance.org

Claire Wolfe, Author and Freedom Advocate

Edward Hasbrouck, Author, The Practical Nomad

Rena Tangens & padeluun, FoeBuD e.V., Big Brother Awards Germany,
http://www.foebud.org/, http://www.bigbrotherawards.de/

Deborah Pierce, Executive Director, PrivacyActivism, http://www.privacyactivism.org/
Media Inquiries: (425) 736-7319 , dsp@privacyactivism.org

[More to be added]