

RFID IN ID CARDS



- ▶ Could enable the remote identification, tracking and stalking of RFID-equipped cardholders.

RFID Use for Identification Threatens Personal Safety

Today's RFID technology is too crude to protect private information from unauthorized access. Privacy protections are needed.

People Should Know When Their Data Is Read

Unlike ID cards equipped with barcodes or magnetic stripes, an RFID-equipped card does not have to be physically given to an individual wanting the card's information. Instead, personal information can be secretly read through wallets, pockets, backpacks, or purses by identity thieves, pickpockets, government officials, and others. People would never know if their identity information were stolen, or if they were being targeted, tracked or stalked.

People Should Be Able to Choose Who Sees Their Information

The RFID technology touted for today's ID cards does not allow individuals to authorize the sending of their personal information. With RFID, cardholders' movements could be tracked, sacrificing anonymity at political meetings, protest marches, or private activities.

(Continued on back)

What Is RFID?

Radio Frequency Identification (RFID) tags store and broadcast information to reader devices. Developed as a way of tracking products, RFID raises serious privacy and security concerns when incorporated into identification cards. When information traditionally printed on an ID card – such as name, address, Social Security Number, or driver's license number – is stored on an RFID tag, it forces individuals to broadcast their personal information without any notice or choice.

RFID Tags:

- ▶ Do not notify an individual when information on the tag is read;
- ▶ Do not typically allow individuals to easily turn them off or block the sending of their information;
- ▶ Could be a source for identity thieves harvesting personal information such as name, date of birth, address, digital photos, fingerprint images, etc;



More Secure Alternatives Exist

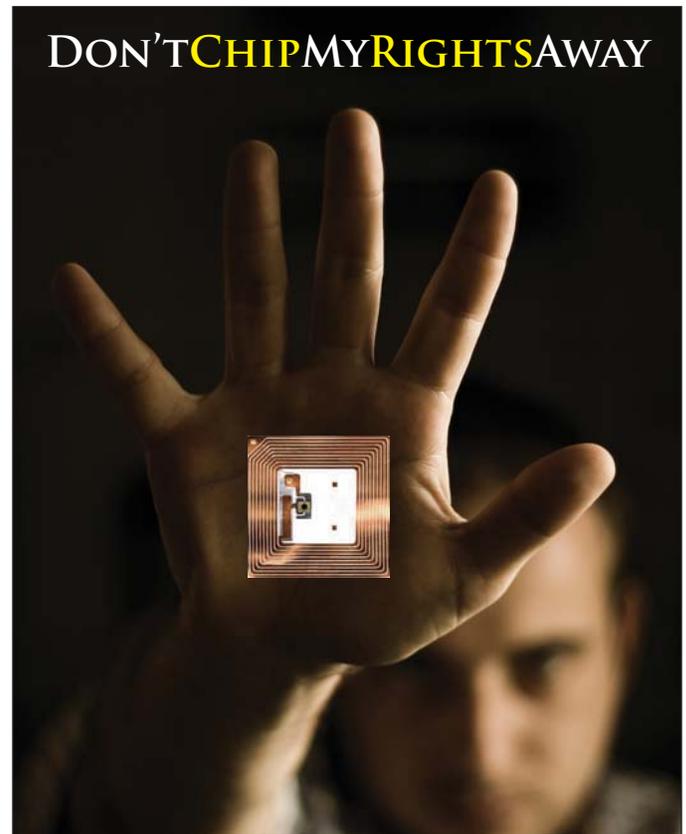
Existing alternatives, like barcodes or magnetic strips, make information more secure than RFID. RFID's advantage is remote access to information – precisely what would make RFID-enabled ID holders less safe and less secure.

Oppose RFID Use in Identification Documents!

Personal information stored on drivers licenses and other government issued IDs should be protected and secure, and not put the ID holder at risk for tracking, stalking, or identity theft. RFID should not be used on ID documents unless the technology protects data privacy and allows people to control when their data is read.

As use of RFID spreads, we urge policy-makers to:

- ▶ Resist using RFID in government-issued identification cards, such as driver's licenses or student ID cards.
- ▶ Provide guidelines for RFID use for personally identifiable information, including an individual's right to be notified when someone reads his or her information and the ability to block unauthorized reading.



Oppose RFID in ID Cards!

