Overview:

As law enforcement officials out first response to RFID technology must be that our primary concern is the safety and security of the citizens under our protection. At the same time, while we enforce the laws we do not create those laws. We will focus our efforts on preventing new forms of theft that RFID could make possible, while ensuring that any employment of RFID technology on our behalf will be done with the utmost respect for the rights and privacy of those we work to protect. Technology does not fundamentally change our mission to protect and serve.

That being said, RFID technology is certainly an issue with which law enforcement in the future will have to contend. Such technology creates a whole new spectrum of possible criminal attacks on an individual. Methods such as skimming, cloning and theft of RFID devices pose a property and information security risk that is different from any law enforcement has yet encountered. We would expect any vendors of RFID technology to employ appropriate cryptological and hardware specific safeguards in order to ensure that their products are not easily vulnerable to such attacks. We cannot know exactly when and where new criminal threats will develop, but as always when such crimes do occur we will be ready to apprehend those responsible.

RFID technology may also play a role in aiding our efforts to identify and apprehend criminals after they have committed a crime. The potential of RFID tags in aiding the identification of stolen property is an area that would greatly aid law enforcement. The Lowjack system, which is already in place, is demonstrably effective in this regard. Further advances in RFID technology may help us combat crimes such as counterfeiting and even kidnapping, by allowing us to identify and locate items and individuals more quickly than ever before.

Many people see such technology as the beginnings of a police state, but nothing could be further from the truth. While we will use any RFID technology to our advantage and work to prevent new avenues of theft created by such technology, we will not demand that items or individuals be fitted with any sort of RFID tags. Furthermore the use of such tags will be done with the utmost concern for the rights and privacy of the individual. In truth, most of the items we search for will not be RFID tagged and classic methods of investigation will continue to be the mainstay of law enforcement.

The next section will discuss the privacy implications of RFID in more detail and will be followed by some potential questions and answers intended to better prepare you for the coming interview.
Section 1: Privacy Implications of law enforcement and RFID

The primary concern of increased use of RFID tracking and surveillance technology by law enforcement is widespread and uncontrolled invasion of privacy arising from the capability to track and identify individuals based on their RFID-enabled personal effects. In the dystopian extreme of this vision, law enforcement could track the whereabouts and movements of all citizens at all times. We must convince people that this is neither the goal nor really within the capability of law enforcement's use of RFID tracking.

Primarily, RFID tracking for law enforcement purposes will be on extremely valuable items – high denomination bank notes, automobiles, collectibles, artwork, high end electronics, etc. Generally, these are items that are not carried on the person of an individual on a quotidian basis, and have worth such that most people will not mind if law enforcement knows of their possession if it aids in their recovery. However, there will be high encryption and verification standards used to ensure that random snoopers cannot scan the RFID signatures of the items in a house to “case” the house for robbery. The value of these items means that it will be cost-effective to use the most complex and robust RFID tags on them. With the added level of security provided by the requirement of owner approval or a court order to access these RFID tags, law enforcement tracking of valuables should not pose a significant privacy threat. Today, a similar version of this exists in Lojack car recovery systems, and has aided in the recovery of a large number of stolen vehicles.

A greater privacy concern arises from law enforcement piggybacking on widespread RFID deployment by other agents to perform searches on people without their knowledge. If manufacturers and other distributors of clothing, personal electronics, and other items begin to tag their products with RFID, a police officer armed with an RFID reader could covertly search an individual at range, without his or her knowledge. This can be used, for example, to discover if an individual is carrying any goods marked as stolen by a retailer, or if all firearms are required by law to be tagged, if the individual is armed. Few would object to the latter usage, but the former is where privacy concerns are most keenly felt. We feel that legal barriers regarding search and seizure should apply in the same way to RFID searches as they do to standard search – probable cause and warrants to perform more widespread and involved scans. Thus, officers in a tense situation, say a raid of a drug den, will be able to more effectively gather information about their situation, reducing danger to police and increasing likelihood of success, but will rarely have the need, and never have the legal permission to perform unreasonable covert searches on arbitrary individuals.

In essence, we believe that RFID does not present privacy concerns greatly exceeding current surveillance and law enforcement technologies, and when used legally and carefully, can provide in certain situations a great deal of help to law enforcement. We do not think it will completely revolutionize police-work, nor will it require complete overhaul of current legal strictures and protocol. It is perhaps best thought of as a technological innovation like better surveillance cameras or infrared detection.
mechanisms – it will become merely a tool effective in certain situations, but not more pervasive or privacy threatening than any other.

Section 2: Possible Questions about Criminal Uses of RFID

Question:
As RFID is deployed more widely, are there ways that criminals might attempt to make use or exploit this technology?

Answer:
As with any new technology we expect that criminals will imagine new ways to attack it and to misuse it. Some RFID technologies lend themselves to this more than others, so the specifics will depend to a great degree on the technologies deployed in our area of operation. Several attacks that we are already aware of include “skimming”, or capture of the information on an RFID tag without the knowledge of the holder; and “cloning”, or the duplication of an RFID tag, again without the knowledge of the holder.

When RFID technologies are deployed inside controlled areas, such as amusement parks or resorts, we expect that our job will be aided by the ability to control the ability of criminals to move RFID readers in and out of the area. This may become something that we search for on entry, or other forms of electronic surveillance may be able to detect these devices in use. When used outside controlled areas RFID technologies become far riskier. As law enforcement we expect we will be able, with the help of companies deploying these technologies, devise strategies to keep our citizens safe.

Question:
Can you comment on the ways that RFID extends or alters the current capabilities of criminals?

Answer:
This is a difficult question to answer outside of the context of a specific RFID technology. We are worried, however, about the ability of criminals to access information stored on RFID devices without the knowledge of their carriers. If poorly deployed, this could really offer a way for a thief to “pick your pocket” without having to touch you or even get near you.

Question:
Can the deployment of RFID technology for business purposes create opportunities for criminals?

Answer:
Of course. RFID technologies create opportunities for criminals regardless of how they are deployed.

Question:
How do you imagine RFID technology changing your tasks as a law enforcement officer?
Answer:
As law enforcement we are continually faced with new challenges as criminals evolve. We expect to be able to deal with this threat. This might involve some of our officers having to learn some new technologies. We have a lot of technology-literate people on the force and we'll be leaning on them to help the rest of us as we address these sorts of issues. But at the end of the day we expect to get the job done.

Section 3: Possible Questions about Law Enforcement use of RFID

Question:
How will law enforcement be able to fully utilize RFID technology as the infrastructure develops and its use becomes more widespread?

Answer:
Obviously, as RFID technology becomes more affordable, and subsequently more widespread, law enforcement will be forced to keep pace. We understand that law enforcement must keep up with the technology so as to fully exploit the advantages it has to offer. In order for this to be achieved law enforcement personnel will need to be trained and taught to fully understand the technology. Following an initial training session personnel will be evaluated to determine those who are most qualified to continue training in RFID technology. These people will become part of a subgroup of law enforcement whose primary goal is to ensure that law enforcement is using RFID technology to the best of its ability. Furthermore, there will be a special innovation group, within the subgroup of law enforcement, whose goal will be to broaden the possible uses of RFID technology within law enforcement. One of our primary goals is to ensure the competency of our law enforcement so that no possible advantages of RFID technology are lost due to lack of knowledge or skills.

Question:
Are there significant cost issues associated with RFID technology in law enforcement and the training necessary to fully take advantage of the benefits it could offer?

Answer:
When addressing a question such as this one should first briefly highlight the advantages that are to be gained from using RFID technology within law enforcement. These advantages will provide justification for any costs we may incur. By utilizing RFID technology law enforcement will be able to track items of great value, including currency, with greater ease. Not only will this type of surveillance better deter theft, it will also minimize illegal transactions. The advantages do not stop here and certainly not all of them can be addressed within the interview. However, it would be appropriate to note some of the advantages when faced with a question such as this. Given its certain advantages, it seems appropriate that federal funding and tax revenues should be devoted to the implementation of the technology within law enforcement. However, it is not anticipated that costs will be exorbitant. The technology will allow jobs that once
required many personnel to know require few. Downsizing within law enforcement personnel will allow for more funds to be allocated towards RFID technology within law enforcement.

Section 4: Questions about Law Enforcement’s Role in Protecting Privacy with Respect to RFID

Question: How will law enforcement’s role in protecting privacy change as RFID is deployed more widely? Will there be legal barriers in protecting individuals from evidence gathered using RFID technology? What about protecting individuals from each other?

Answer:
The role of law enforcement is not to determine what is right or wrong. That job is left to the legislators. That being said, it is our job to enforce the rights of the people under the existing framework as RFID becomes more widespread and to be prepared to incorporate new laws that may arise from the increasing awareness and usage of this technology. Law enforcement’s essential role in protecting privacy will remain the same as before, it is really a matter of applying an existing framework to new situations that may arise. It is important to note that members of law enforcement has their own bounds and limitations and that it is as much a responsibility of us to respect those bounds as it is our responsibility to protect the populace.

RFID poses new threats in that it may make certain crimes easier to carry out, such as identity theft or present new issues with existing crimes such as counterfeiting. These do not change how law enforcement tackles these problems however. In these cases, RFID may change how these crimes are carried out, or introduce a new component to them, but they do not change the essential nature of the crime itself and existing laws still deal with these situations in a reasonable manner.

There are certain instances that may be unclear as to how the law applies however. Again, while it is our job to protect individuals, the decisions as to whether scanning someone’s possessions and harvesting information from them without their consent is criminal or not is not really up to law enforcement. Let us say an individual goes by peoples’ houses and starts scanning the RFID tags on items lying around on a person’s lawn. While we could possibly arrest this person for trespassing, the judgment as to whether the scanning is illegal or not lies essentially as a judiciary and legislative concern, and not one of law enforcement. It is our duty to enforce when the law requires and enables us to.

The advent of RFID does allow for new potential revenues for gathering information and evidence. It is important to keep the technological and practical limitations of RFID in mind when addressing this issue (question 2). Law enforcement use of RFID information can be beneficial, but like any police method for searching, it has its own limitations. Scanning the RFID tags on people going into an airport may help catch contraband items,
but for the most part the practicality of such scanning is reduced by the fact that any intelligent would-be criminal or terrorist would be sure not to tag their contraband. RFID in a situation like that however, is barely more intrusive, and hardly more effective than current implementations. Consider another scenario however, where police set up an RFID scanner in a discreet location to monitor an individual’s possessions as he or she walks past a point near his house. What arises here is then mostly a 4th Amendment issue, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” It would be imagined that RFID scanning, like any other search, although non-intrusive, still falls under the category of a “search” and thus is applicable to the same restrictions as a physical police search or a wiretap.