RFID, GPS, and 3G: Radio Wave Technologies and Privacy

Lori Bowen Ayre (lori.ayre@galecia.com)
The Galecia Group

I recently read an article in *Wired* magazine[1] about the decision to suspend the plan to embed RFID (radio frequency identification) chips in California driver's licenses. A driver's license with an RFID tag in it is call ed an Enhanced Driver's License (EDL).[2] The argument in favor of the EDL plan was, of course, convenience. The argument against the plan was, of course, privacy. And like many conversations about convenience versus privacy, a big dose of facts would be helpful.

Proponents of the plan said it would reduce wait times at border crossings because they would allow agents to easily pull up information about the person crossing the border without having to key-in information. Also the EDL could be used in lieu of a passport. The opponents of the plan worry that carrying an EDL in your wallet or purse would enable you to be tracked and stalked without your knowledge or consent. Others worry that state law enforcement officials might start "tapping into the chips" and doing more with the data than was originally intended.

While I wouldn't argue that there is nothing to worry about, I would argue that some of the expressed concerns represent a misunderstanding of the technology. In fact, generally, people seem to have a hard time understanding the differences between the many "radio wave" technologies we interact with each day such as RFID, Wi-Fi, GPS, and 3G/4G. But it is important to understand how they differ, and also, how they are the same, especially when it to comes to deciding what you should be worrying about and how to balance your convenience vs. privacy interests– and how you help your patrons do so as well.

The RFID "chips" intended for California drivers' licenses are passive UHF tags. These are like the ones that now appear in our US passports (e-passports). Technically, "chips" are just one part of an RFID "tag." RFID tags are composed of a chip and an antenna. Libraries use HF tags which are similar to the EDL tags except they operate at a lower frequency – High Frequency (HF) vs Ultra High Frequency (UHF). HF tags have a shorter read range than UHF tags, but they are both a type of RFID tag.

RFID tags can store information. So, if there was personally identifying information on a tag, theoretically someone with an authorized RFID reader could read that information. However, according to the Department of Homeland Security (DHS), the EDL tags only contain a unique identifier that is meaningless on its own. It only has meaning if you also have access to the DHS database. The number on the tag allows border agents to easily pull up a record, in the DHS system, about the person at the border. It saves them from typing in a number. It doesn't change the fact that the person has a file at DHS or that their border crossing is being recorded. It just makes the whole process happen faster and more efficiently.

So, the worry that state law enforcement would "tap into the chip" doesn't make any sense. If agencies other than DHS were to tap into the DHS database, then there could be problems. But if you were able to read the tag, all you'd see is a short number string. Not very interesting. You might recall that this was the same worry about library RFID tags….that they'd carry information about our patrons. Of course, they do not. And while we may have information about the book itself (e.g. a code indicating the library that owns it, its format type, and other coded information that improves materials handling), the only way to associate that item with a patron is to have access to the integrated library system (ILS) that was used to check-out that item.

The e-passport, on the other hand, contains the passport holder's name, nationality, gender, date of birth, and digitized photo. For this rea-

son, the tags are encrypted, require the reader to authenticate itself as an authorized e-passport reader, and the cover of the passport includes shielding (tin foil?) so you have to open the passport to read the tag.[3]

"Tracking" was another worry expressed about EDL, but all the RFID tags we've discussed so far contain passive tags. Passive RFID tags don't emit a radio signal on their own. They only respond to a request from an authorized reader so the only way to track someone with a passive RFID system is to follow them, with an authorized reader in hand. With library RFID tags, you'd have to stay within two feet of the person to read their RFID tags. With EDL and e-passport tags, you could be as far away as 20-30 feet. Either way, to track someone with passive RFID, you'd have to have a lot of readers installed or a lot of people involved.

Active RFID tags are another matter. These types of tags have batteries so they can emit a signal without waiting for the reader to "ask" for the information. Depending on the battery used to power the tag, the read range can be quite a bit longer. So far, active RFID tags are not widely used because they are much more expensive.

GPS (global positioning system) is another radio wave technology. Unlike RFID tags which contain static information (e.g. a barcode or DHS record number or passport data), the GPS tag is really a receiver. GPS technology works by interpreting radio signals that are being transmitted by satellites. Its job is to use satellites orbiting the Earth to determine its location. Because the GPS system must be in constant communication with the satellites, it requires a battery to operate.

GIS (Geographic Information System) isn't a radio wave technology but it is important to this discussion because your GPS really needs GIS to be useful. GIS provides the maps your GPS needs to actually locate you in terms of latitude, longitude, and altitude which is how you get plotted on a map. Your car's navigation system needs both GPS and GIS to get you to your location and to tell you what is around the next corner. Depending on your navigation system, your car may be tracked. It's just a matter of capturing the signals from your car's GPS receiver. This is a positive feature for many navigation systems. For example, OnStar automatic crash response system claims "specially trained Advisors are available 24/7 to send help to your exact location. You don't have to do a thing." Cars may be driven by more than one person so tracking a car isn't quite the same as tracking a person.

Then there are cell phones and smartphones which use another form of radio wave technology. 3G (and 4G) are marketing-speak for the different telecommunications networks. These networks can carry both data and voice signals over radio wave signals. Your cell phone communicates with the nearest cell tower that matches the telecommunications network of your provider. Because you are personally linked to your cell phone which is communicating with cell towers, your cell phone is essentially locating you personally. When you receive a call, send that text, or update your Facebook status, *you* are communicating with a specific tower. In fact, your location would be part of that metadata that NSA is mining when they get records from your cell phone company. However, cell towers can be pretty far away so it isn't like you could be tracked that closely….or does it?

If your phone is equipped with a GIS receiver, you are now trackable to within a few feet. Remember the job of the GIS receiver is to pinpoint its location, via satellite, at all times. So if you keep your GIS app running, that information is in your smartphone.

And this is where it gets interesting. If you add Internet access to your smartphone, you've added the ability to communicate all these disparate pieces of data about you and your location. You can use the 3G/4G system to get Internet access or you can do it via WiFi. With WiFi, your phone communicates with a specific access point that is very nearby. Depending on who operates that access point, this is another opportunity to specifically locate you.

The point is that the smartphone makes it easy to connect a lot of data points together about a

person. Someone hacking into your smartphone can get to everyone in your contacts list, get to everything in your Facebook account, access your Dropbox files, read incoming and outgoing emails, read your e-books, and access pretty much anything that doesn't have additional password protections on it. Once you have access to the Internet with your smartphone, all sorts of data sharing about your location and what you're doing can now take place depending on what you've authorized your apps to do. Apple clearly recognizes how vulnerable we are if our smartphones get into the wrong hands. Just this month they released the iPhone 5S that includes TouchID – a mechanism for authenticating authorized users of the iPhone via their fingerprints.

So, what does all this mean for privacy and a librarian's commitment to protect patron privacy? It means keeping oneself informed and helping people understand the technologies that really do threaten their privacy (e.g. smartphones) versus technologies that just sound scary (e.g. RFID "tracking chips"). It is easy to jump onto the Big Brother bandwagon and wrap everything in tin foil but the fact is that a lot of these technologies improve our lives, even save lives. Also, more and more people appreciate the convenience provided by these various technologies more than they worry about the implications for privacy. It is important, therefore, for librarians to help our patrons become educated consumers so they can make choices that strike the right balance of privacy and convenience for themselves. It's complicated but the distinctions are important to understand in order to make informed decisions.

Endnotes

[1]http://www.wired.com/threatlevel/2013/09/drivers-license-rfid-chips/

[2] For more information, see http://www.dhs.gov/enhanced-drivers-licenses-what-are-they

[3]http://www.rfidjournal.com/articles/view?1951