TESTIMONY OF DANIEL J. SOLOVE
"RFID TAGS AND INFORMATION PRIVACY"

Before the Subcommittee on Privacy and Confidentiality of the National Committee for Vital Health Statistics

Hubert H. Humphrey Building, Room 705-A
200 Independence Avenue SW, Washington, DC 20201
Jan. 11, 2005
9:00 AM to 12:00 PM

RFID TECHNOLOGY

RFID – shorthand for Radio Frequency Identification – is a form of electronic identification that involves a small computer chip (called a "tag") placed into products, objects, and even people.[1] The tag involves a transponder that emits a signal. The signal contains information. A reader or decoder detects and reads the signal. The information in the signal is then deciphered.

Much of the RFID technology just signals an ID number, which can be linked to data in a database. However, it is possible to have the signal broadcast information in addition to the ID number. But either way, RFID works to identify and locate particular items or people and to link them up with a stream of information.

CURRENT REALITIES

The technology for RFID already exists. For a while, RFID tags were expensive, thus inhibiting their use. But the price of tags is coming down.

Another difficulty is the range of the signal the chips can emit. Many chips cannot transmit a signal long range. But it is not far-fetched to imagine that within time, the signal strength of RFID chips might improve drastically.

FUTURE POTENTIAL

RFID tags have many potential benefits, but they also pose a substantial threat to privacy. The future of RFID is vast and potentially very significant. If prices come down for the tags, they will increasingly be placed in products.

They can be made very small. The European Central Bank has plans to implant small RFID tags into bank notes. This will make currency traceable. RFID tags can be

[1] For more background about RFID tags, see David Kushner, *Just Another Chip in the (Privacy) Wall*, MIT's Technology Review (Nov. 18, 2004); Kenji Hall, *No Slipping in Late at Tokyo School; High-Tech Tags Log Each Student's Arrival, Departure*, Wash. Post, Nov. 14, 2004, at A29; Jonathan Krim, *Embedding Their Hopes in RFID; Tagging Technology Promises Efficiency But Raises Privacy Issue*, Wash. Post, June 23, 2004, at E1; Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (2004). The Electronic Privacy Information Center maintains an excellent webpage with extensive and useful information about RFID tags. *See* http://www.epic.org/privacy/rfid/.

placed in licenses, ID cards, and into virtually any item or product. Technology might improve the range of the signal, so that chips can be read from greater distances.

Suppose the police want to track a person. The police get a list of the products he owns and traces where each one is. And they trace his movements 24 hours a day with the RFID. The police might use an RFID reader to scan people's luggage or bags, and can get a full inventory of their contents.

Another potential use is a private company tracking people's RFID tags and beaming them individually-tailored ads wherever they go.

THREAT TO PRIVACY

I believe that RFID poses considerable dangers to privacy. Currently, there is still somewhat of a divide between the online world and the offline world. Online, our transactions are readily tracked. Everything we buy at stores like Amazon.com is recorded. Everything we peruse is recorded. Moreover, on the Internet, people's websurfing can be tracked with cookies and spyware. Only with great skill can a person achieve true anonymity online, and for many online transactions, anonymity is impossible.

However, offline, people can more easily engage in anonymous transactions. I can go to a bookstore, buy a book and pay with cash, and unless people remember my face – which is unlikely – I'll be able to buy the book with anonymity. This means that no record linking me to the book I bought is kept.

RFID threatens to change that. RFID chips can threaten to be a cookie or spyware equivalent in realspace, in the offline world. Therefore, RFID can become a very powerful information gathering tool. It can be a way to link information to particular people. It can also be a way to track people's movement.

The key problem is that our existing legal regulation of privacy is not prepared to deal with RFID. We have a weak regulatory infrastructure for repositories of information gathered by private sector businesses and institutions. RFID information will enter this realm.

DIGITAL DOSSIERS

To understand the full implications of RFID technology, we must understand the rise of digital dossiers and the legal regulatory infrastructure that protects our privacy. RFID threatens to lead to an unparalleled degree of information gathering.

In my new book, *The Digital Person*, I discuss the unprecedented amount of personal information that is collected by businesses and the government and stored in gigantic databases.[2] Each person is living with a digital counterpart, a digital person who resides in a database. This digital person is not made up of flesh and blood – but of information fragments aggregated together.

Today, there are hundreds of records detailing an individual's consumption and lifestyle. These records are being assembled into gigantic databases of personal information on millions of people. Increasingly, personal information and computer profiling techniques are used to make very important decisions affecting our lives. Our

[2] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

dossiers are used to determine our financial reputations – whether we receive a loan, job, or license.

There are several problems with the rise of the digital person. First, our dossiers are kept woefully insecure. Companies do not protect personal data with adequate security. Identity thieves can readily steal a person's identity and pollute that person's dossier with erroneous information.

Second, personal information is traded and sold between companies. Some companies sell it to anybody who will pay a small fee for it. We have little control over how our data is used to judge us. Moreover, the government is tapping into our dossiers maintained by businesses.

The law has attempted to respond to problems of information privacy in a number of ways, but it has some major problems. Since the early 1970s, Congress has passed over 20 laws pertaining to privacy. Federal regulation covers records from federal agencies, educational institutions, cable-television and video-rental companies, and state motor-vehicle agencies. But it does not cover most records maintained by state and local officials, libraries, and charities, and by supermarkets, department stores, mail-order catalogs, bookstores, and other merchants.[3]

Moreover, many of Congress's privacy statutes are hard to enforce. It is often difficult, if not impossible, for an individual to find out if information has been disclosed. A person who begins receiving unsolicited marketing mail and e-mail messages may have a clue that some entity has disclosed her personal information, but she often will not be able to discover which entity was the culprit.

RFID AND MEDICAL DATA

There are some special unique issues involving the use of RFID in the medical context. RFID in the medical context has many potential benefits. People can either wear a bracelet or some item with an RFID chip or have one implanted in them. This will allow medical personnel to read the chip and locate health information about a patient. This might help diagnose unconscious patients or discover allergies. Many people might voluntarily want to use such technology. But there are costs that might inhibit the process.

THREAT TO PATIENT-PHYSICIAN CONFIDENTIALITY

There is a longstanding tradition of doctors maintaining patient confidentiality. The Hippocratic Oath, dating from around 400 B.C., states that doctors must keep patient information confidential.[4] In many states, patient information is protected by an evidentiary privilege. This is because, in the words of the U.S. Supreme Court, "the mere possibility of disclosure may impede development of the confidential relationship

[3] *See id.* at 67-72.

[4] The relevant portion of the Hippocratic Oath states: "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." Quoted in DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 217 (2003).

necessary for successful treatment."[5] One court expressed the rationale for the special privilege protecting patient-physician confidentiality best:

> When a patient seeks out a doctor and retains him, he must admit him to the most private part of the material domain of man. Nothing material is more important or more intimate to man than the health of his mind and body. . . . To promote full disclosure, the medical profession extends the promise of secrecy referred to above. The candor which this promise elicits is necessary to the effective pursuit of health; there can be no reticence, no reservation, no reluctance when patients discuss their problems with their doctors. . . .[6]

The problem, however, is that there is currently great uncertainty in existing law about the degree to which medical information can remain confidential. The HIPAA regulations provide that a covered entity may disclose health information to a law enforcement official in compliance with a subpoena or court order, as well as an administrative subpoena or demand.[7] Subpoenas have a very low level of protection – much less than a search warrant.

It is unclear whether the Fourth Amendment would apply when the government seeks a patient's medical information from a physician, hospital, or other caregiver. Under what has become known as the third party doctrine, the Court has held that the Fourth Amendment does not apply when a person divulges information to a third party.[8] Thus, despite the fact that bankers often promise that a person's bank records are confidential, the Fourth Amendment does not require the government to get a warrant to see them.[9] The logic of the third party doctrine appears to apply to information held by health care providers. After all, these are third parties.

---

[5] Jaffee v. Redmond, 518 U.S. 1, 10 (1996).
[6] Hammonds v. AETNA Casualty & Surety Co., 243 F. Supp. 793 (D. Ohio 1965).
[7] The regulation provides:

> (f) *Standard: disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official . . .
>
> (ii) In compliance with and as limited by the relevant requirements of:
>
> (A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
>
> (B) A grand jury subpoena; or
>
> (C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
>
> (1) The information sought is relevant and material to a legitimate law enforcement inquiry;
>
> (2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
>
> (3) De-identified information could not reasonably be used.

45 C.F.R. § 164.512(f).
[8] *See* Smith v. Maryland, 442 U.S. 735 (1979) (pen registers); United States v. Miller, 25 U.S. 435 (1976) (bank records). As the *Miller* Court stated: "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Id.* at 444.
[9] United States v. Miller, 25 U.S. 435 (1976) (bank records).

On the other hand, there is a longstanding tradition of doctors maintaining patient confidentiality. If the Court were to apply the doctrine here, it would almost seem farcical to claim that a person has no reasonable expectation of privacy in her medical records.

I think that this is an issue that the courts will have to confront. But until that time, there is a big question mark in the law. And these open questions will make people more reluctant to use RFID technology. Many people might not want to use RFID if their information can be gathered and used for purposes beyond their treatment. People might fear their RFID being used by law enforcement to track them. Or people might fear the data collected from RFID might be turned over to the government. Or kept insecurely. RFID chips will also harm those who unwittingly use the technology in the false assumption that their data is provided adequate legal protection.

Our law isn't ready for RFID technology. We have a lot of laws that regulate privacy, but we still need to address their many gaps and flaws. We could enjoy the benefits of RFID and deal with the costs if we had a better legal foundation. But bringing RFID into our existing information privacy regulatory regime is a recipe for trouble.

We need protection not just at the stage of gathering data from RFID chips, but also after the information is gathered and stored. Otherwise, we could severely damage the patient-physician relationship and make people reluctant to use chips for medical purposes. How do we prevent RFID tags from being read by others? How do we protect the security of RFID information?

There are also dangers that RFID tags will be used to track people's movements like a GPS homing device on a person. Since RFID can be implanted in products and clothing, or in watches, bracelets, or jewelry, they can work like a tracking device.

The Supreme Court has held that the Fourth Amendment does not apply when a beeper tracks a person's movement in public. In one case, a beeper was attached to an item placed in a person's car, and the police tracked the car's movements. This was not a Fourth Amendment violation.[10] The danger is that the police might use RFID to track people in public. There is little regulation of what the police may do with tracking technologies such as RFID. The Supreme Court has left a big void, and Congress hasn't filled it.

And this is just the law enforcement use of RFID. There are many open questions about what restrictions are on people or businesses who might try to read others' RFID tags.

CONCLUSION

The problems, then, don't end with the collection of data from RFID tags or the implantation of RFID tags. Merely getting people's consent at these stages is not sufficient enough protection. The problem is what happens to all that data that is stored. We need better downstream protections of the data from RFID tags. We need a way to

[10] United States v. Knotts, 460 U.S. 276 (1983). Although tracking devices in public are not protected, the Court has held that such tracking within the home is covered by the Fourth Amendment. United States v. Karo, 468 U.S. 705 (1984). The Washington Supreme Court, in interpreting the state's own Constitution, came to a more enlightened conclusion than *Knotts* by holding that the police need a warrant in order to attach a GPS device to a vehicle to track its movement. *See* State v. Jackson, 76 P.3d 217 (Wash. 2003).

ensure that the tags can be permanently deactivated. We need a way to ensure that the tags are not read by unauthorized persons. And we need a way to ensure that when people agree to use an RFID tag, that the tags or the information are not later used for different purposes without that person's consent.

The technology of RFID is not malignant or benign in and of itself. It all depends upon how we regulate it. Right now, our law protecting personal information needs to advance much further in order for RFID to be of net benefit to our society.