# Radio Frequency Identification Tags, Memory Spots, and the Processing of Personally Identifiable Information, and Sensitive Data: When There Is No Balance Between Right and Wrong

**Luca Escoffier**

University of Washington School of Law
William H. Gates Hall
Seattle, Washington 98195
Lucae@uw.edu

**Abstract**

Novel medical applications and devices will shortly play a critical role in the diagnosis and storage of medical information *in vivo* on the patient's body. Radio frequency identification (RFID) tags, and memory spots are probably going to be massively deployed on humans not just as a means to locate, and identify a subject but also to have access to sensitive information as medical records, genetic features, and pathological data. The role played by the advancement of technology in this sector is undoubtedly beneficial on the one hand because it solves many problems and deficiencies of the current situation, but on the other hand the collection of extremely sensitive data, like the genetic and pathological ones, must be treated with extreme caution, but probably even the most advanced safety features will not be sufficient to protect individuals from the illegal retrieval and processing of personally identifiable information and sensitive data. There will be a day in which striking a balance between what is useful, and what is too private to be known and disclosed will be extremely hard to accomplish for our decision-makers.

## What are personally identifiable information, and sensitive data?

"Personally identifiable information", "personal information", and "personal data" are usually the most common expressions to define a set of data concerning an individual or organization depending on the jurisdiction concerned.

For the purpose of this paper, I will use the expression "personally identifiable information" to define: information which can be used to identify an individual's or organization's identity, such as name, social security number, biometric records, etc. directly or indirectly by reference to an identification number or to one or more other factors.

"Sensitive data" is another expression, commonly used at the EU level to define: information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities. This kind of information is manifestly sensitive as it conveys information that is particularly intimate and that might compromise the individual's image or perception if disclosed in the wrong environment, especially if used to judge the individual's capacity or predisposition to achieve a certain result or ability to perform a task. Usually, regardless of the jurisdiction in question, this kind of data must be stored and processed with higher care and after having obtained the individual's expressed and informed consent for its processing and transmission. Genetic data, due to its capacity to inform the holder about current disorders or predispositions to potential diseases requires in most countries an even more restricted treatment by not just dictating rules for its processing, but also for the storage and transportation, and, most importantly, for the consented use. Many jurisdictions, for example, already consider as illegal the use of genetic information for allowing or denying insurance coverage, and entitle individuals to seek damages in the case of infringement.

## What is radio frequency identification?

Radio frequency identification is a system used to locate and recognize all kinds of items, human being included. A tag is attached to the item, and the reader is able to "read"

the data contained in the tag through radio frequency. There are three types of RFID tags; passive, active, and passive-active.

The first type has no battery and the signal that is transmitted cannot be read from too far because the tag needs to be activated by the reader.

The second type has a battery and therefore the distance between the reader and the transponder can be much greater.

The last type has a battery that is activated only when prompted by a reader.

Nowadays, RFID can be also used on humans, both in the form of a removable item, maybe attached to a bracelet or as an implantable device. They are apparently not harmful and the dimension of the tag is usually half of a rice grain. The most common implantable RFID system in the U.S. is the one marketed by VeriChip under the name VeriMed Health Link. The transponder contains a 16-digit code that once read by the reader from a physician or a nurse gives access, together with the passwords of the hospital to a secure database in which the personally identifiable data of the patient and her medical records are stored. The patient can have access to her folder and modify the information as and when she pleases.

Today, October 22nd, 2009, VeriChip and Receptors LLC in press release announced webcast details to unveil the most recent developments of a virus triage detection system for the H1N1 virus and *in vivo* glucose-sensing RFID chip. Practically, this novel technology should be able to detect toxins, microbes and viruses to detect potential bio-threats. The system should perform the detection, classification and identification of one or more viruses and then the RFID communicates to the reader the results of the exam executed by the implantable sensor.

This novel approach can let us think that in the future, not that far from now, the tags will be able to recognize several, maybe hundreds of viruses, microbes and other pathogens allowing physicians not even to perform, but simply get acquainted with the diagnosis performed by the transponder, with an embedded biosensor, which will ultimately send the information to a base or hand-held device. In this last instance, probably in the future everyone will own the portable reader to diagnose herself reading the data comfortably on a couch at home. This is a dramatic breakthrough that could completely change also the medical profession as in this case, physicians should just intervene in the therapeutical phase if the biomarkers, and diagnostic devices provide accurate results.

## What is a memory spot?

A memory spot is a chip, which is capable of storing a huge amount of information (for now, up to four MB) that can be fetched by a reader. Memory spots have no battery as they get their power from the reader. HP Labs have developed a memory spot that is able to contain long documents and short videos. The reader can be embedded in a cellular phone and read the information by touching the memory spot, which is practically a chip so tiny that can be nowadays attached to an envelope or sheet. The potential applications are countless, from information on a certain product (instructions manual) or an event (if attached to a flyer) to the results of experiments to be attached to a laboratory sample, and patient's sensitive data if attached to a bracelet in a hospital. Also, the speed of transmission of data is already much greater than the one attainable with Bluetooth® devices. The major difference between memory spots, and RFID for now lies in the distance between the transponder or chip and the reader and data speed. In fact, for now, memory spots are able to convey information just if literally touched by the reader. More's law may well let us think that in the future these chips will be able to store a considerable amount of information. An increased distance between the chip and the reader will also be probably achieved.

## A day in an E.R. in 2020

December 10, 2020. In a cozy E.R. of a hospital in Seattle the nurses escort an injured and unconscious patient to one of the doctors. The patient is copiously bleeding, and there is no time for diagnostic exams or other tests. The nurse moves towards the doctor the flat display attached to the bed where the body lies, and all the relevant information pertaining to the patient appears in the blink of an eye. The doctor knows the name of the patient, his allergies, blood group, and medical records. There is also a video of his physician with other useful medical information on the man that can be played, if necessary. The display also shows the presence of bio-threats. In fact, the patient is also affected by a virus, and has a genetic pattern that will make some drugs not particularly effective.

The physician can now take the appropriate steps to start curing her patient knowing his medical past, present pathological conditions, what are the most appropriate drugs, and dosage that will achieve the best results in a rigorously, and incontrovertible way.

This story is just an example of the concrete future possibilities that will make the work of a physician easier, and more effective, and the life of a patient more secure, and astoundingly predictable.

## Undesired use of personally identifiable information and sensitive data by third parties

There will be a day in the near future in which our decision-makers will be obliged to take serious decision as to the processing of our sensitive data.

As we have seen, there are already devices that can be attached to the human body or implanted under our skin that can contain a huge amount of sensitive information concerning our status, health, predispositions, predictable response to drug, etc.

There will be a day in which our politicians will have to consider the interests of the population and our health on

the one hand, and on the other hand the threats that such information can pose if in the wrong hands.

In fact, let us imagine a world in which our biometric and genetic information, digitally processed, and stored could be retrieved from our body from readers that could be potentially in the hands of people or organizations that could use this data against us or, at any rate, without our necessary consent. The outcome of an illicit use of our personally identifiable data, and especially the sensitive data, as the genetic ones, can be disastrous. What if the sensitive data contained in our implantable devices will actually be used for unlawful purposes like, the denial of an insurance coverage or a job or the entrance to a public place because of our current or likely physical conditions? Or worse, what if a viral marketing bombards us on our smart-phones suggesting what to do or not to do for our health, and what drugs to buy and what to avoid?

Also, there is a proven generalized fear about future diagnostic devices that could inform us about our genetic predispositions or conditions since knowing in advance what might be our future or likely health conditions could change our habits, decisions and goals. What will be the reaction of the people thinking about the fact that this information could be seen, analyzed and stored by third parties without their consent?

## Conclusions

The future of the healthcare system follows a path, which has been constantly ameliorating patient's life. The story I depicted above is just an example of the future solutions that we will experience. But the flip side of this apparently platinum medal can actually contain a rusty future. Every system, for how secure it can be, will always be breakable. When there is a code, there is always a code-breaker out there, and the current devices are allegedly clonable with certain ease for now. Sure, there will be always the possibility to enact laws forbidding the unlawful use of sensitive data without consent in all the mentioned instances, and entitling the victims to seek relief and/or damages, but will this be useful when the number of tortious or criminal acts will be committed on a daily or even hourly basis? Will people spend their days in the waiting room of a privacy lawyer or, most likely, they will just be annoyed and frustrated?

Decision-makers will thus, in a non-distant future, decide whether or not this sensitive data that can potentially save our lives should be processed and stored on human bodies. The harm related to the unlawful retrieval and use of this data is as great as the benefit that the system will bring to society, and the decision to take will be one of the most difficult of the contemporary age as it might dramatically change our lives in ways that are completely opposite. Never, in recent legislative history, we have faced such a dilemma.

## References


Verichip website, http://www.verichipcorp.com/.

Verichip press release of 22 October 2009, http://www.verichipcorp.com/pressreleases/102209.html.

Presentation of the potential applications of memory spots, http://h30415.www3.hp.com/?fr_story=21835bfc0d3fbb5e01f499316c0f5e8bd2809b98&rf=sitemap.

Definition of personally identifiable information, http://en.wikipedia.org/wiki/Personally_identifiable_information.

Definition of personal information at http://en.wikipedia.org/wiki/Personally_identifiable_information.

Definition of personal data, http://en.wikipedia.org/wiki/Data_Protection_Directive.