

This is part two of the article “*Identity Linkage and Privacy*,” published in the *ISSA Journal*, April 2007, developing the concepts of identity linkage to all personal information collected on us and that we share, or that is shared on our behalf, knowingly *and* unknowingly.

# Identity Linkage and Privacy - Part 2

By Karen Lawrence Öqvist

**Where ever we go, whatever we do in our everyday lives, our personal information is being collected somewhere by someone or something, online and offline.**

**W**here ever we go, whatever we do in our everyday lives, our personal information is being collected somewhere by someone or something, online *and* offline. Sometimes we are aware of this, though more often, we are not. Dataveillance – the ability to monitor a person’s activities by studying the data trail created by actions such as credit card purchases, cell phone calls, and Internet use<sup>1</sup> – and advanced data-mining techniques enable entities, whether business or government, malicious or benign, to create profiles of our behaviors and tendencies in order to influence our actions. Additionally, the explosion of computing power has fostered an increasingly connected world of collaboration and social networks where even more personal information is gathered. The Information Age has arrived....

## Collecting and profiling

For years we have been “sharing” personal and often sensitive data with government authorities, and normally we do not have much choice in this. In the name of national security governments are busy collecting information on their citizenry in new and increasingly ingenious ways. And not just the government. Businesses easily entice customers to take out loyalty cards (store cards, air miles, etc.), fill out registra-

tion cards following purchases, and utilize numerous other means of digging into our personal lives. The information collector gets to know things about us, such as our buying and lifestyle habits, and can then use our habits against us – or for us, depending on whether you like what is being done or not.

Our personal data can then be aggregated, sorted, categorized, sifted and mined, resulting in individual profiles, linking our identities to consumer groups, political groups, recreation groups, etc. Our behaviors and tendencies can be pampered, exploited or abused. We become identified by what we do or have done, what we eat or wear, by our race, color, gender or creed, and decisions can be made about us upon which we have no control. Profiling by organizations can be used for retaining customer loyalty, i.e., customizing your buying experience specifically to please you. Amazon.com does this quite effectively. Profiling can be used to make our lives more comfortable as though someone is looking out for us, or quite unpleasant if the outcome is some form of discrimination or worse. The remaining article will focus on information collection devices and techniques, their benefits and dangers.

<sup>1</sup> Dataveillance: the ability to monitor a person’s activities by studying the data trail created by actions such as credit card purchases, cell phone calls, and Internet use. [www.wordspy.com/words/dataveillance.asp](http://www.wordspy.com/words/dataveillance.asp).



## RFID

Radio Frequency Identification (RFID) is promising a world where virtually every item we possess, from a packet of coffee to a car licence plate, will be communicating with transmitter-receivers embedded everywhere, from doorways to roadways to point-of-sale terminals, effectively turning the offline world online. And everything we do offline or online will be tracked.<sup>2</sup>

In 2005, Wal-Mart ran a pilot study using RFID tags in all its Texas distributions centers to track more than 10 million cases of goods. By March 2006 over 1800 RFID-related patents had been issued by the U.S. Patent Office.<sup>3</sup> The next foreseeable step is that all clothes have embedded RFID tags, so that even if your personal information is not available, the store can identify from what you wear certain information about you, e.g., are you wearing designer clothes? An RFID tag in this situation may hold as much, if not a higher degree of value than the designer brand itself! For example, it could be that you have on your person an RFID tag, replacing the loyalty card from your favorite supermarket, that profiles you as a vegetarian. Your supermarket and Starbucks are friends, i.e., they share information collected on you. Next time you enter Starbucks you receive a personalized invitation offering your favorite vegetarian snack, *just for you*.

RFID tags are so discrete that it is possible to embed them under the skin – this is happening today both on animals and humans.<sup>4</sup> There are some ethical questions concerning use on humans; however, the use of RFID has some very positive human applications, e.g., in the U.S. RFID has been used to help caretakers keep track of family members suffering from Alzheimer's disease. It could be a nightclub in Barcelona<sup>5</sup> offering VIP status – queue jumping privileges and free drinks – to customers willing to have an RFID chip implanted under the skin in their upper arm. Clubbers with the implants are enthusiastic about the freedom and convenience: no need to carry cash as it is loaded electronically on the chip. Other nightclubs are looking to do the same and the one RFID implant could work with all the nightclubs. The convenience, however, can have a nightmarish twist when a bad guy with a




---

**RFID tags are small wireless devices that provide unique identifiers which can be read by remote sensors. RFID tags can be active, emitting signals that can be sensed remotely, or passive, requiring reader proximity. RFID tags are small and discrete; hence, it is not obvious that you may have something with a tag transmitting information. Nor is it obvious that a reader in the proximity is picking up the data.**

---

rogue RFID reader locates the reveler and “steals” the device. Or a hacker reads the device and steals all the cash.

Just like satellite tracking devices, RFID device will make it possible for governments to mark individuals for surveillance purposes. They are using RFID tags today on criminals (minor offenders) effectively placing them in prison but free to continue working in their day-to-day lives: scanners are placed at the offender's home enforcing a type of “house arrest.” All movements are recorded to prison authorities. For example, offenders not registered as being home by 1700 every day will be under risk of having their sentences lengthened or even ending up in a traditional prison.

The general acceptance of such devices is driven by a growing desire for safety in our lives. Imagine if you are brought into an emergency room unconscious and a scanner in the hospital doorway reads your chip's unique ID. Your medical records will be released from a database, informing of your diabetes, penicillin allergy, etc.<sup>6</sup> Some U.S. hospitals are already offering this service. Early adopters are those suffering from epilepsy, diabetes, Alzheimer's disease and other life-threatening illnesses that impact how a patient should be treated. The vision for the future is that this service should be available in all hospitals, so wherever the patient turns up she will be scanned and treated accordingly. The only information kept on the chip is the patient ID which links to their medical

---

**It could be a nightclub in Barcelona offering VIP status – queue jumping privileges and free drinks – to customers willing to have an RFID chip implanted under the skin in their upper arm.**

---

records. This necessitates all hospitals to connect their databases so that regardless of where the patient turns up, the scanned ID will be presented to the treating (and authorized) doctor, independent of where the data was originally col-

2 “How RFID works,” Technovelgy.com, <http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=2> (visited June 2007).

3 M. Grimaila, “Security Concerns for RFID Technology,” ISSA Journal, February 2007.

4 “RFID for people,” Verichip, <http://www.verichipcorp.com/index.html> (visited June 2007).

5 “This chip makes sure you always buy your round,” The Observer UK website, [http://observer.guardian.co.uk/uk\\_news/story/0,6903,1391545,00.html](http://observer.guardian.co.uk/uk_news/story/0,6903,1391545,00.html) (visited June 2007).

6 “Providing your personal medical history when it matters most,” Verimed, [http://www.verimedinfo.com/for\\_patients.asp](http://www.verimedinfo.com/for_patients.asp) (visited June 2007).

lected and stored. It is not too farfetched to speculate that a natural progression is the extension of this type of service to ambulance services.

UK schools have just finished a pilot program on selected pupils, embedding of RFID tags in the school uniforms. The pilot was a success and parents agree with the schools to go the next step of embedding RFID tags in all school uniforms. Key motivators are eliminating truancy for the schools, and for parents, reducing the risk that a child's school blazer will be lost or stolen. This presents some questions that we may ask ourselves on what will happen next:

- Will we start *chipping* our children as social acceptance as the use of RFID implants spreads?
- What happens when RFID becomes linked to the GPS network?
- Imagine if your son or daughter became missing; the implanted chip could enable your child to be found quickly. Would you agree to your children receiving RFID implants in the name of safety even knowing that everything about their activities is being logged? Some parents do, and this service is being sold today in the U.S.

The arguments for RFID implants could become somewhat persuasive, just as the use of biometrics in passports has gained momentum and increased public acceptance since 9/11. However, there is still significant public resistance, given the speculated risks to our personal privacy, particularly with embedding chips in humans, though it is already done to our cats and dogs.

### RFID risks

So what are the immediate risks? With the health records example the chip itself holds a personal identifying ID linked to your personal data. There is a risk of rogue scanners that can scan you as you walk by and pull out this number; but what can be done with it? Nothing, unless the thief has authorization to access the hospital systems where your your personal data is stored; or he hacks in.

What about replacing loyalty-cards with RFID? The risks here are basically the same as exist today: stores, airlines, hotel chains, all sharing our personal data as quickly as it is collected. The only difference is that you will no longer need to present a card; you just walk into the store, hotel, or airline ticketing counter and get your VIP treatment. You will be uniquely identified as a customer – to one or more of the services – and the type of customer you are. Your details will automatically present themselves to whichever personnel happens to be assigned to be at your service. Your profile – your customer type – will in most cases influence how you will be treated.

The biggest risk to privacy is the linking of the databases, which is the strength behind the compelling arguments for RFID. Wherever you go, if you are chipped, your activities can be logged and stored. Your ID is unique and links to all

data collected on you. So the greatest risk with RFID is not the chip itself, but that it uniquely identifies you – has become a part of you – and links you directly to data stored and collected on you wherever this may be. This may be fine so long as you trust whoever is holding this information on you.

### Publishing and sharing

Web 2.0 symbolizes the paradigm shift occurring in how we are communicating and socializing through the Internet, conveying a world in which we willingly share our personal information online with the rest of the world. This change in our online behavior brings a world embracing collaboration, social networking and blogs, a virtual community utilizing virtual space such as MySpace,<sup>7</sup> Flickr<sup>8</sup> and YouTube.<sup>9</sup> It is cool to have



a blog both professionally and socially, facilitating networking on a global scale independent of geography, race, color, creed, gender, age, social status or disability. We are communicating and collaborating on a scale never seen before, bringing equality in a way never experienced before!

We like to show the world that we exist, what we do in our lives, and what we think. We even publish photos and videos of ourselves online, and it is becoming increasingly common for young people to meet and date online. This creates a whole new connotation to the definition of “information exposure” in the domain of information security when applied within the context of social networking. Individuals publish private information about themselves, their families, their friends on the web knowingly and willingly, although perhaps naive to the potential risks. This information is unstructured in how it is organized and may or may not be linked to personal identity and could be formalized for the purpose of this article as “*Digital Information Residue*” – personal information that has been, collected or shared, and digitally stored somewhere by someone or something in Cyberspace, over which we have no control. Hence, this information in its unstructured format can be linked directly to our identity if we chose, though often even when we do not. Not all online activities that are digitally preserved are linked to our physical identity, but some could have a “dormant identity linkage,”<sup>10</sup> i.e., a link that is not an obvious link but can become active as a result of:

- Another physical identity's knowledge of specific personal information about the person (e.g., name change), hence, the aggregate of knowledge leads to identity-linkage and exposure that would not have otherwise been possible, largely because aggregations of data maybe more sensitive than the individual items alone.

7 MySpace, <http://myspace.com> (visited June 2007).

8 Flickr, <http://www.flickr.com> (visited June 2007).

9 YouTube, <http://www.youtube.com> (visited June 2007).

10 K. Lawrence Öqvist, “Identity Linkage and Privacy,” ISSA Journal, April 2007.

- Personal information that is shared under an alias becoming contaminated because within the same space there are links to their physical identity, i.e., in their *friends list* are *real, physical friends* that know their real name.

Personal or sensitive information on us found on the Internet, which has been posted by others, has the potential to impact our personal or professional reputation in the real world. This can be positive or negative. For example, today’s recruitment agencies *google* applicants during the screening process; some of us do the same when we meet a new acquaintance.<sup>11</sup> Exposed information even in this unstructured format can be mined for malicious purposes, including social engineering, fraud, enticement of children, and the collection of private information for spamming. Information exposure, within the context of *consensual information exposure*, is the exposure of personal information that is not accidental or a result of malicious activity and is difficult to mitigate with the use of traditional information security countermeasures.

Another example of where consensual information exposure is widespread – particularly for children and teenagers – is the mobile phone network. Photos can be taken, shared, posted and exploited, often without the knowledge of the subject. These photos are easy to distribute to multiple recipients via the use of multi-media messaging service (MMS).

### The identity linkage matrix

Our personal information can be collected and stored in a structured or unstructured format; this information may or may not be linked to our identity. The Identity Linkage Matrix (Figure 1) takes examples of information that is collected on us, and information that we share. This is mapped into the matrix, dependent upon linkage to identity and how the personal information is organized. The mapping of information that is gathered on us, or that we share, can tell us in a simple way the potential impact on our life. The matrix has two axes and four quadrants: the higher the information is in the quadrant, the stronger is the link to our identity, the further to the right of the quadrant the easier it is for our personal information to be mined.

- The horizontal axis represents information gathered or shared and how well structured it is
- The vertical axis represents linkage of information gathered or shared to the real identity
- Information shared or gathered and placed in the top two quadrants is linked to our identity and has the potential to be mined with our identities
- Information shared or gathered and placed in the bottom two quadrants is not linked, but there is potential of linkage via a dormant identity linkage, i.e., contamination of unlinked information, or access to another information source that is linked
- Information linked directly to our identity and gathered using structured methods is placed in the *hot* quadrant, the top right-hand corner. This data a.) is worth most to others apart from ourselves, and b.) can cause us the most damage if used inappropriately. This quadrant is also the most interesting quadrant for government authorities and hackers.

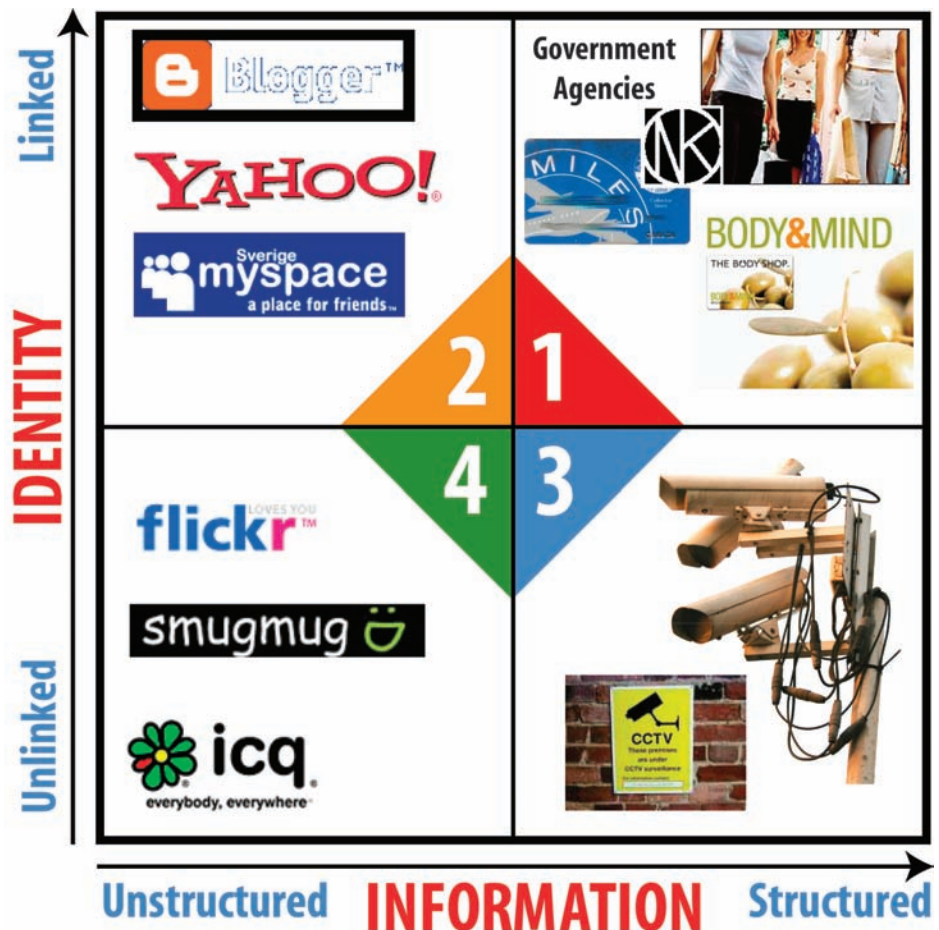


Figure 1 – The Identity Linkage Matrix<sup>12</sup>

11 “Business Information Search Engine ZoomInfo Unveils PowerSearch 2007.” Zoominfo website, [http://www.zoominfo.com/About/news/press-release-article.aspx?articleID=01\\_30\\_07](http://www.zoominfo.com/About/news/press-release-article.aspx?articleID=01_30_07) (visited June 2007).

12 The matrix builds upon the concept of the Janus identity model, originally published in ISSA Journal April 2007. The identity linkage continuum – online activities stored/ logged somewhere in the past – are timeless and have the power to impact, either positively or negatively, an individual’s reputation in the real world today and in the future.

## Identity Linkage Matrix Impact examples:

Quad	Information	ID linkage	Consequences	Existing examples
1	Structured	Yes	Intelligent data-mining is possible by authorized personnel. Profiles attached to identity. Potential consequences today and in the future are influencing decisions that you make, or choices being made for you. Risk of personal information exposure when information holder has insufficient security measures in place.	Government authorities, store cards, frequent-flyer programs, congestion controls (RFID linked to car license plate which is in turn registered in your name).
2	Unstructured	Yes	Can be mined by interested parties, e.g., recruitment agencies. Information exposure, identity theft, on-line grooming of children, on-line bullying/ harassment.	Blogging and social/ professional networking spaces, forum activities, etc., using real name.
3	Structured	No	Limited. Potential dormant identity linkage, e.g., police have the authority to mine CCTV and other tracking technologies to link an identity.	CCTV, travel card paid by cash, etc.
4	Unstructured	No	Limited. Potential dormant identity linkage, thus same risks as when linked.	Blogging and social/ professional networking spaces, forum activities, etc., using an alias.

If we take a couple of examples from the matrix and see what this means.

### Closed circuit TV surveillance

CCTV (closed circuit TV) is positioned in the matrix as information gathered in a structured way although it is not linked to our identity. This dislocation to our identity is because the person accessing the information collected by CCTV does not also have access to digital data that has our identity directly linked, i.e., a store card or RFID. If this were the case and he did have access, then our movements on camera could be linked directly to our identity (dormant identity linkage). A good example is the surveillance cameras in the London Underground. If you use a travel card (Oyster Card) that you have chosen to link to your identity (you can choose to use Oyster anonymously today), it makes the jobs of the police easier when tracing someone as they can see on the camera the exact time the card was swiped and by whom.

### RFID surveillance

The use of RFID in surveillance and tracking has the potential for growing acceptance as has been demonstrated in the use of cameras for surveillance in the UK and the U.S. Likewise, the decision to permit RFID to be included in the school uniforms of UK has been approved. This enables children's movements to be tracked wherever there are sensors. A related vision for the future in the UK is the linking of national databases holding residents' personal information into one or more master repositories that can be mined and leveraged to improve government services and fight crime more effective-

ly.<sup>13</sup> In the UK and the U.S. there are plans to merge hospital databases on a national level. Hence everything we do in our everyday lives will have the potential to not only be tracked but also be mined. More personal/sensitive information that is accessible by the use of a unique ID linked directly to our identity makes it all the more interesting a target for tomorrow's hackers and those involved in the growing trend of cyberwarfare. Information that can be effectively mined can be used to influence choices and decisions we make in our lives both knowingly and unknowingly, today and tomorrow.

### Social networking

Social networking spaces are where we share our personal information in blogs and online networking communities in an unstructured format. We cannot be sure of what happens to information once it has been shared online. If we change our mind about any published material, it is too late. It has most likely been copied and replicated to another server or indexed and cached by some search engine. This information has the potential to be mined – even though it is unstructured – by interested parties. Stories of pedophiles profiling their victims are some of the most publicized examples.

### Apathy vs. privacy and choice

Each of us lives in an environment of controllable and uncontrollable factors, and lying in between are gray areas where we theoretically have the power to influence decisions made on how our personal data is being managed on a national level in democratic societies. However the use of gathering mecha-

13 "Dilemmas of Privacy and Surveillance," The Royal Academy of Engineering (ISBN: 1-903496-32-2), March 2007.

nisms to learn about us, both by government authorities and other interested parties, has grown. Public resistance is marginal. Some of the factors influencing this apathy are the following:

- The overriding motivation for a safe society outweighs the personal costs to our privacy, e.g., surveillance vs. terrorism
- We have for the last 20 years been sharing our buying habits willingly and knowingly with our supermarkets and favorite stores. This is migrating to online stores where it is not clear how much personal information we are sharing with the use of cookies. Although we as consumers are aware of, and have some concerns on this practice, we feel that in general the benefits, i.e., the personalized buying experience and convenience, outweigh the personal cost to privacy.
- Increasingly, we are sharing our lives with others online through blogs, social networking spaces, etc. In fact, this trend is changing public perceptions on personal privacy.

Hence, the Information Age has unleashed a surveillance society, and we are on the cusp of a new type of surveillance era: today we can see the cameras and other tracking mechanisms; tomorrow we will not. We will not be aware of when and where we are being surveyed or tracked. The technology is here with microscopic surveillance, tracking technologies and sensors that turn the offline world online. In this world we may not be aware of if or when we are being surveyed. Our children will not think to question its logic because they have grown up accustomed to the notion of being tracked as the norm. In fact, we could be the last generation to question the rational. Coupled with the social networking revolution that we are in the throes of, is questioning the very concept of privacy and what it really means today. And what will it mean in the future, if anything at all?

## In a perfect world

Imagine a world that is able to anticipate your needs based upon what it knows about you. Today's passive world will increasingly become an interactive world. Your online experiences today are influenced by what you do online. Sometimes you know what is collected on you, sometimes you do not. Turning the offline world online will effectively map the offline world to the rules of the online world. Imagine an environment that adapts automatically to you based upon what it knows about you:

- A car that pulls over to the side of the road when a retinal scan detects that you are too tired to drive
- A home that adapts the environment to you when you walk into a room, e.g., light is dimmed, your favorite music or TV program playing
- Walking into your favorite department store and being immediately directed to where you want to go

It sounds like a utopian world. The cost is difficult to quantify, but equates to your personal privacy, the choice to choose your preferences, and make your own decisions. If we continue to permit ourselves to be tracked in the offline and online world without enforcing our right to know what is being tracked and how our personal information is being used, what will be the long-term consequences? Is there technology today that could make it possible to know who or what is tracking us? Do you mind being tracked? Do you mind not knowing? If you do not mind, think of your personal, sensitive information that has been collected and stored having the potential to be damaging to what you want to achieve today, tomorrow, or sometime in the future? Could it be somewhat disturbing that by not having control of your identity and privacy today, you will become profiled and your choices will be made for you based upon information that has been collected and stored on you?

*Meet Hal...the friendly update manager who takes over your computer to make sure you have the latest anti-virus protection, the latest digital rights management software to ensure you only do what you are allowed to do with the music you buy.*

*Meet Hal...your new cell phone, that will decide when it will turn itself on and on off, and when it will report your geographical location to the authorities.*

*Meet Hal...your new refrigerator that reorders the food as it expires...or not, depending on what your health care provider stipulates.*

*Meet Hal...the chip that gives you the coordinates of your children.*

*Meet Hal...the robot that is looking after your mother in her assisted-living apartment, nagging her to take her pills, monitoring her blood sugar, her caloric intake, and her mood swings.*

*Meet Hal...your car, that decides if you are fit to drive or not.....*

*Meet Hal...*

Nevertheless we do not need to be too concerned really; when it happens, it will impact our children more than you and me. And when it does happen, nobody will be troubled about "threats" to personal privacy: when our children become adults, they will not care about privacy because in their world it would have become obsolete.

## About the Author

*Karen Lawrence Öqvist, MSc Information Security. A Security Solution Architect, International Expertise Team (IET), Consulting & Integration (C&I) EMEA, Hewlett-Packard. She has nearly 20 years experience in IT and over 10 years in identity management. She has previously worked for Novell and CERN. She hosts a blog at <http://mysecuritybox.blogspot.com>, and can be contacted directly at [karen.lawrence@bcs.org](mailto:karen.lawrence@bcs.org).*