The Privacy Paradox
or How I Learned to Have Rights that Never Quite Seem to Work

Raffaele Zallone
Partner, Studio Legale Zallone, Milano, Italy
Contract professor of IT Law, Bocconi University, Milano, Italy
President, European Lawyers Association ITC Law Commission
Studio Legale Zallone, via dell’Annunciata 31, 20121 Milano, Italy http://www.studiozallone.it
e-mail:r.zallone@studiozallone.it

Abstract
The present privacy legislation continue to be drafted on the basis of the Strasburg Convention of 1981. The mere fact that present privacy laws are based on principles drafted 29 years ago, when the web did not exist, shows that privacy legislation need to make a quantum leap to be in line with the realities of to-day’s real life operating environment. If the status quo is kept, the law and its application shall face serious (and sometimes insurmountable) obstacles to its implementation, making compliance costly for private business, at the same time jeopardizing effectiveness of privacy protection for individuals. A new set of rules should be drafted and established, addressing the changed environment of information and communication technology, in order to allow free flow of information at the same time assuring due protection of personal data.

The web and the change in the substance of personal identity
The protection of privacy of a person is the legal means for modern society to protect the identity of that person. Until recently it used to be that personal identity was something on which each human being could exercise a reasonable degree of control. Personal identity can be defined as the mix of various factors and facts. It’s the path one person has followed in life: the studies, the schools attended, her/his jobs; her or his family, cultural associations, friends, etc. The mix of all these element have been the building block of the traditional concept of personal identity. All these elements were, to a significant extent, under the control of each individual (of course with all the limits that society and economy bring along). I am the one to choose my friends, the place where I will spend my vacations, the books or newspapers I read, the investments I make, etc. In sharp contrast with this traditional concept of identity, in to-day’s world personal identity has changed to something completely different. The bits and pieces of one’s life are no longer under that person’s control, but under someone else’s control. Assuming that I perform a transaction with my bank or if I use my credit card to by something through the web, etc, the information related to this purchase or the details of that bank transaction will be in the hands of (to name a few) the bank, the institution which manages the credit card transaction, the search engine that helped me find the site I accessed and where I ultimately bought something from. This, of course, does no include all kinds of other intermediaries that operate on the web and elsewhere and that make it possible for each one of us to shop, buy, pay, surf the web, send and receive mail, open blogs, participate to forum debates, etc.

Each one of these organizations holds users’ records and, as such, it has created a customer profile of each user. Whether this profile is accurate and carefully reflects that user’s identity is totally immaterial: what they have is a piece of someone’s life and, to them, that’s the person they think they have to convince to buy new products or services, or whose coordinates they will pass on to a “business partner” to have him try to do the same. In the process, personal identity has lost its personal nature in that it does not reflect any more the life of a person but only that micro-window that one transaction has opened. Each counterpart of every person (or each profile of every person) catches, stores and uses only the records that it has gathered and considers, for its purposes which are mostly marketing purposes), only those records. Obviously, we all know that most organizations do not stop here. Most organizations tend to divide their customers in clusters, generated through the analysis of perceived customers behaviour. If a user has bought product A, she/he will most likely buy product B, because average consumers behaviour shows that those who bought product A sooner or later bought product B. Thus, using this information, organizations target product A customers to market product B. In this way, personal identity is not just fractioned in countless mini-identities (so to speak); truth is that personal identity becomes totally immaterial because all the records gathered on one subject are used only to generate other records based not on that subject’s behaviour, but on the behaviour of others. At the same time, the behaviour of that subject will be added to existing data and used to predict the future behaviour of other users. This immediately...
shows what striking contrast does exist with respect to the traditional concept of personal identity. As I said above, in its traditional notion personal identity is the mix of all of one person’s characteristics. In the present environment, personal identity has lost its meaning, and the main thing that counts are the bits and pieces of personal life that generate data, that shall be subsequently associated with other data related to other subjects. And each of these micro-identities is controlled by a party who considers these data as its own. In fact, users data are considered a content of significant value to the organization that holds them. It is probably one of the most valuable items for any company that is somehow involved in marketing its goods or services. The originator of the data, the person to whom the data refer to (i.e. the one that we are used to define as "the data subject") has no control whatsoever over them.

The case of search engines: if only they knew…

The traditional notion that led to the Strasbourg Convention can be summarized as follows: computer have an incredible capacity to store, retrieve and compare data, by far superior to any other device previously known to man. Assuming that all data gathered is recorded for fair and lawful purposes, the association and process of data from archives set out for different purposes could create a “Big brother” that will know everything about everyone. It was perceived that, for example, government could use the data to discriminate or isolate persons that would not conform to certain criteria. In this vision, otherwise legally collected data could be used to reach unlawful means, by way of this capability to record, confront, sort and in any way process data. In many ways, search engines could easily be seen as the coming to reality of this vision. In many ways, search engines could easily be seen as the coming to reality of this vision. But, before we approach the problems that search engines (among others) pose to individuals’ privacy, we should go back to the Strasbourg Convention. Considering that a Convention is merely a international treaty, why bother with it? Well, for a number of reasons. First, the European Directive 95/46/CE is based mostly on the Strasbourg Convention. Second, the Strasbourg Convention was signed in 1981. Everyone with some experience in this field knows that an international treaty of this kind is between 3 to 6 years in the making. This means that the Strasbourg convention reflects the IT world of the mid-seventies. In those days the top of the heap was distributed processing, the first form of networking that developed in contrast to the dominance of the IBM mainframe architecture. If this is the case, and since as I said the European Directive is based on the Strasbourg Convention, one could infer that this is a first sign of why the European Directive is obsolete. The truth, though, is somewhat different. The data protection principles that were the building blocks of the Convention (hence, of the Directive) are still valid today. They are principles of law that protect human rights. They are machine independent, so to speak, in that they are not based on a technology, but on the rights that need to be implemented to protect the very nature of individuals, i.e. their identity. It’s the perspective as well as the mechanisms that are obsolete. The perspective in those days was to create the means to protect individuals from potential misuse of large data bases. The perspective was that the potential issues and problems where seen in the creation of these data bases from governmental organizations. Governs can discriminate and isolate individuals; indeed, this was what happened, in those days, behind the wall, in the communist-block countries. The Strasbourg Convention was a way for the then new-born Europe to give a message loud and clear to everyone wishing to hear: we, as western world, undertake not to misuse, steal, spy or in any way make unlawful use of information related to people. We are not the communist block, we are the free world and as such we shall respect you as a person. We shall not use our computers to discriminate, send to jail, deny human rights to anyone, and we shall make sure that no one uses the personal data we collect to pursue such ugly scope. The message was loud and clear and extremely important; it is my personal view that in no way such a fundamental principle can be regarded as obsolete. The fact is that in our world of to-day, the largest amount of data are not gathered by governments, but by private companies. Second, the data do not reside anymore in physically identified or identifiable storage devices under the jurisdiction of a single country. Data are now stored in clouds: in the 30-some years after the Convention, never anything has given a more serious blow to a fundamental piece of legislation as the expression “cloud computing”; a new technology in data processing that the IT stake-holders are using these days. If we cannot locate the physical place of residence of data (if one can use this expression), why bother with concerns about Governments and their use of data?

This is the reality of the technical piece of this difficult equation, and yet if the data protection principles are still valid, the mechanism have to be modified so that they could work also in this and future environments as well. Let’s look at the case of search engines. Any and all information available on the web about one person are easily tracked by the search engines, no matter where the data have been recorded and stored, and no matter as to how actual that piece of information is. The consequences of this are under everyone’s eyes. One real-life example is the case in Italy of one Ms X. Ms X was (and still is) a successful real estate broker. She and her husband manage a fairly sized real-estate brokerage firm, with a significant presence in the marketplace. Ms X was at one point somehow involved in a local scandal: the wife of a former minister was accused of bribing public officials and Ms. X allegedly was the person that physically gave the bribe money to such officials. She was arrested on bribery
charges. After two years she was acquitted along with all the other defendants: the court found no evidence whatsoever of bribery. The acquittal was confirmed by the Court of Appeals and later the Italian Supreme Courts rejected the motion to review the case. In good old times this would have been the end of it; this, alas, are not the good old times, these are the days of the Googles of this world. The first acquittal dates back to 2002: keep this date in mind for a few moments. As I said above, the case in which Ms X was involved was a national scandal; therefore, the news of her arrest was on all newspapers; of course, all newspapers have their Internet site, so the articles were accessible on Internet. At the end of 2005 Ms X started to act: on the basis of the right granted to the data subject (i.e. the person whose personal data are processed) under Italian law she started contacting all newspapers that still published on their web-sites the news of her arrest, asking them to cancel such pages from their website. The newspaper were also given, at their discretion, the alternative to simply modify the page by deleting her name and changing it to “a well known real-estate agent”. In this way the page would still show, but without Ms X’s name. The legal basis for such request is the rectification and blocking right, based on the privacy principle that personal data have to be kept “no longer than necessary in identifiable form” (something that is also known as the “right to oblivion”). A previous decision of the Italian Privacy Authority had stated, in the case of an entrepreneur fined for misleading advertisement, that after two years such decisions where not to be available to the general public. In the case of Ms X the legal rationale for her request was that if this right was granted in a case where the defendant was found guilty and fined, the more so if the defendant was acquitted. The newspapers whose pages showed the news of Ms X’ arrest were contacted and eventually accepted to cancel the pages with the articles at stake. Unfortunately here came the first issue: the pages that the newspaper had cancelled or modified were still found through Google. The fact is that Google makes a copy of every page it has indexed (i.e. what they call the “cache copy”); therefore, even after having been cancelled or modified, the original pages as well as the original snippet kept showing and popping up like nothing had ever happened. When contacted, Google denied any responsibility and initially refused to take any action. Google’s defended itself based on two arguments: in the first place, they raised the exception that they merely had collected what others had written. Secondly, since the organization who had to respond to the Italian Data Privacy Authority was Google Italy, they also claimed that Google Italy had no power whatsoever to operate and modify the search engine, whose operation and management are a power reserved of Google Inc, Mountain View, California, USA.

Of course Google failed to represent the fact that they still held a copy of the original page and that, therefore, they could have no longer relied on the first exception raised; in fact, once it makes a copy of any personal data, it becomes a data controller on his own. Google has no responsibility as to the accuracy or truthfulness of the original article, but once it makes a copy of the original page, Google becomes data controller of the data it has copied, and it has all the duties and obligations any controller has under the law. The Italian Data Protection Authority in its decision of January 18th, 2006, held that “it has been ascertained that the search engine does indeed process data autonomously, with specific reference to the cache copies of web pages copied from other sites and then stored”. The Italian Authority also stated that such processing “makes the search engine subject to the rights of the data subjects, assuming that Italian Law applies”.

Epilogue, but not a happy ending (yet) Let’s go back to the point I made above on personal identity. Ms. Rossi so far has not freed herself of the past, because her present identity is the one that Google has created by collecting and storing all these information about her. As far as you can still read using Google, her acquittal never took place and she daily can still see the news of her arrest. Her business contacts were getting weary about dealing with her (specially new prospects) so she had finally to change her name and use her husband’s last name instead of her maiden name, which she proudly had continued to use for years!

Our task now is to ask ourselves what were the issues and try to understand what can be learned from this case that can be used in perspective to help draft a new statute of data privacy rights. It is mandatory to act quickly and act well, because there is an additional point to consider. If we look at the history of computers, we can easily see that the era of information technology has just begun. If we look at the automotive market, it is a fact that internal-combustion powered engines appeared in the second half of the 19th century. Therefore, if we compare the history of computers to the history of cars, we’re just before the launch of the Ford T Model, more or less. The best is yet to come, and whatever we do now will have a decisive influence on the future; if we make mistakes now, the consequences of such mistakes shall be felt for years to come. This is why action is required now!

The first point is to put some discipline as to the flow of data. There is no question that data have to flow freely, but each new subject that uses the data has to be clearly held responsible for her/his use of such data and this independently from the source of the data. Presently, the law requires that the original data controller has to communicate any changes made to the data to all other subjects to whom it communicated the original data. This is a cumbersome and costly burden on any subject. On the other hand most organization do retrieve data from any available sources: the originator of the data may never be aware that they have been searched, retrieved and stored by
someone else who wants to process them. Search engines do not list the pages independently from the awareness of the site owner. Technically here there is no communication of data, because data are simply caught by the spiders and shown as search result. How can a subject who manages an internet sites know what search engines have sent their spiders to retrieve its pages? How can anyone know what data have been retrieved from whom? Therefore anyone that does retrieve and store data on its own, whatever the purpose may be, must inform the data subject of this operation. As the decision from the Italian Authority stated in the Google case related to Ms X, these organizations cannot anymore state that they only show what others have written: they are controllers of personal data on their own, whether they like it or not, and they have to comply with the data protection principles.

Second, and most important: can the mere fact that a piece of hardware is located in one country be a valid waiver of jurisdiction? The sliding scale approach established in many US cases (among others: Minnesota Vs. Granite Gate Resorts, 568 N.W. 2nd 715 (Minnesota Court of Appeal, 1997) and U.S. vs Thomas, 1996 FED App. 0032 P (6th Circuit)) can be a valid legal theory and basis to establish rules of jurisdiction; it should be taken as a legal basis for a new statutory provision in this area. If a given geographical market is clearly addressed by a given legal person, then jurisdiction in that market (i.e. country) must be granted. Were this not to be the case, anyone could just place her/his server out of the national border in a more lenient jurisdiction to avoid the rules and obligations of the law of her/his country: all the crooks of the world would immediately take this golden opportunity to make some more dirty money.

The third point to address is the issue of liability, and this time it has to be addressed with a very determined approach. It used to be that any company that wanted to do business and derive revenue by selling its products in a given country had to comply with the laws of that country: simple as that! No cars or appliances can be sold in any western country if they fail to comply with the laws of that country, be it product-safety or environmental laws. This basic legal principle cannot be repealed now; if a company’s business is to sell or make available information and if these information qualify as personal information, there should be two consequences. First, the law of the country where those information originally come from must be complied with; second, the law of the country where information are sold or used to derive revenue must also be complied with. The immaterial nature of information does not change the nature of liability deriving from its use or misuse, and the same principles that apply to material products must apply here.

These are only examples: there are other areas of the law that need review and update: we must understand that the present European Directive and the different national legislations are clearly showing the sign of times. Action must come now, to avoid widespread abuse and fear about the use of Internet.

Having said all of the above, it is clear to everyone who has practiced law in the area of privacy/data protection, that in the future the main problem is not going to be what kind of statute or regulation we will need, but how to ensure uniform implementation of the new rules. How do we punish those controllers that do not comply with the law? What measures can be used as an effective deterrent to avoid misuse? What remedies a data subject has against a data controller located in a different country? Americans and Europeans have a completely different approach to privacy. The US has repeatedly stated that they prefer self regulation to statutory regulation; this brought to the long negotiation with the EU that finally produced the so called safe-harbor principles. I believe it is clear to all of us that the safe-harbor do not work, mainly because enforcement is basically non existing and there are no easy remedies to the data subjects. Assuming that the safe-harbor rules are violated, does anyone really believes that Miss X (to go back to our lady) could have sued a US based company in the US? She might have had a cause of action, but suing a US based company somewhere in the US, with all the expenses that it brings along, is certainly possible, but it is just as clear that it is very unlikely to happen.

On the other hand, in our global world unilaterally-imposed privacy rules are bound to fail. Only a global and uniform approach can give some assurance that the rules shall be complied with. This is, and will be for sometimes in the future, the most difficult hurdle to overtake.

If this double-pronged dilemma (self regulation vs statutory regulation and local vs global approach) is not coped with, I think I am not being pessimistic but simply realistic in saying that we have to live with the awareness that for some time to come the status quo shall remain unchanged. If this shall be the case American companies and European privacy authorities or judiciary will continue to clash, as we have seen other times in the past in case involving the web (Yahoo vs. LICRA says it all). Europeans will inevitably try to assert jurisdiction over US-based companies and servers. The usual debate we have seen before shall follow for some time; may be as a result of that sooner or later Europe will end up up-dating its rules, but that shall not be enough. If a global approach is not pursued, effective protection of personal data is a long way ahead, yet.