LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze giuridiche
CERADI – Centro di ricerca per il diritto d'impresa

"Cooperative Commons" From Privacy by Consent to Privacy by Contract

Alfonso Papa Malatesta

Luglio 2013

Roma, Luiss Guido Carli – May 13/14- 2013

"Cooperative Commons"

From Privacy by Consent to Privacy by Contract

* * *

Good morning. The topic which I am handling as part of the research into Cooperative Commons being carried out by the Department of Political Science at LUISS concerns the processing of personal data. This refers, in particular, to the processing of the user data - that of each one of us - which is made available online.

The use of the internet involves the processing of digitalised information, most of which falls under the legal definition of "personal data". The Code regarding the protection of personal data (Legislative Decree no. 196/2003), derived from the EU, indicates what is meant by "personal data". It is a definition familiar by now to lawyers. It covers all the "information" relating to a natural person that allows him/her to be identified, even

indirectly. According to the law any information, even when it is non-identifying in nature, is "personal data" if through it other information can be traced that in the end make it possible to identify the natural person in question. Here is the definition contained in the Code.

Personal Data

Any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number

(Italian personal data protection code, Legislative Decree no. 196/2003)

Today personal data immediately evoke the issue of "privacy".

In turn, the "protection" of personal data calls immediately for the "protection" of privacy.

It should be noted, however, that "privacy", which in Italian is comparable to "confidentiality", is a term used for many purposes, many of which go well beyond the definition of "personal data" contained in this law and in its aims.

In common parlance, the reference to "privacy" can be used to indicate the "sphere of personal confidentiality", and thus the limit beyond which it is morally wrong, according to general attitudes, to meddle in the sphere of confidentiality of others. It can be used in relation to the right to "privacy", that is, in relation to the prerogatives of the legally guaranteed confidentiality of one's own actions or the legal obligations one needs to observe in order not to violate other people's right to privacy. It can also be used to refer summarily to an issue, a research topic as studied by various disciplines (including the law).

This variety of meanings, and the fact that the legal content of the definition of "privacy" has rather blurred and indistinct boundaries means also

that "reasons of privacy" could sometime be invoked as a pretext - that is, not being based on strict legal requirements - in order to deny access by third parties to information held by public bodies and private individuals. As it is, among the rights of individuals, especially as regards public administration, there is also the right, no less important than the right to privacy, of access in certain cases to the information that is held by them, understood as the custody of privacy, especially when not properly defined, which is destined to lead to conflict between opposing interests and goals.

I say this to point out that the terminology in common use lends itself to considerable confusion. And like such confusion, this socially detectable phenomenon also impacts on the awareness of individuals of the legal aspects relating to the matter. Indeed, the protection of "confidentiality", on one side, and "personal data protection", on the other side, move in different legal areas. All personal data, for example, are protected even when they do not have a confidential nature: personal data contained in public records, which are not reserved by definition, remain subject to the legislation on data processing. In fact, when correctly understood, the legislation is mainly directed at ensuring the "control" by individuals over the processing of their data rather than the protection of their privacy.

This state of affairs has not yet helped the public at large - and here we come to internet users - to fully understand the phenomenon of the use of the data which is collected and disseminated on the network, in order to then be processed, managed, stored, transmitted and retransmitted.

The lack of awareness on the part of the public does not help the formation of grounded requests addressed to legislators and governments for the subsequent formation of laws and policies.

I would like to say that the issue is being handled by appealing to a great deal of emotion, without the terms of the debate and the different implications of legal action being understood thoroughly, and without the different aspects in question being properly assimilated and weighed up among the public at large. Among these little considered aspects there is also, for our purposes here, the issue relating to the "economic value" of the data, and thus the value they have for those providing them, on the one hand, and for those collecting and managing them on the other.

Thus far a strictly "defensive" approach has prevailed. In fact, it is precisely the aspects related to the "protection" of personal privacy that are the

clearest and simultaneously the most clearly perceived by the public. And this has meant that legislative action has so far been devoted precisely to the "protection" of individuals' private sphere, based on the aforementioned overlap between the protection of "privacy" (confidentiality) and protection of personal data (lawful processing). The legal (and legislative) issue on the current agenda is and remains the "protection" of the data, which is considered by most to be the protection of confidentiality.

And the issue of "protection" has been more easily understood because it has ancient origins, which are rooted precisely in the protection of privacy. In the latter half of the 19th century, the protection of privacy had already emerged as an issue requiring the intervention of the legislature, both in France and in the common law countries.

In the United States of America, the still-famous 1890 article by Warren and Brandeis analysed the issue of the protection of feelings, confidentiality and self-image against the invasions of others, especially on the part of the free press. The authors showed how the appeal to the inviolability of the right to property was natural but inappropriate, and introduced the most advanced concept of the right to the inviolability of the personal sphere ("the right to privacy").

The Right to Privacy

[...] the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more **general right of the individual to be let alone.** It is like the right not be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed -- and (as that is the distinguishing attribute of property) there may some propriety in speaking of those rights as property.

But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. **The principle which protects personal writings and all other personal productions**, not against theft and physical appropriation, but against publication in any form, **is in reality not the principle of private property, but that of an inviolate personality** [...]

Warren and Brandeis, *"The Right to Privacy"*, Harvard Law Review, Vol. IV, December 15, **1890.**

In our legal system this path, based on theories developed above all in Germany, has led to the recognition of the right to privacy as a personality

right (diritto della personalità). In Italy, this right has been fully recognised by case law, with some delay, from the 1970s.

The right in question, as is appropriate to the category of personality rights (think of, for instance, to the right to physical integrity), has thus risen to the rank of a fundamental right which is inviolable and inalienable. An original and absolute right, that is, which is acquired by the mere fact of existing as human beings, that all must respect and that may be invoked by anyone, without the need to sign prior agreements or contracts. And, as with personality rights, it is unavailable by the same right holder and does not expire, nor can it be waived. Personality rights are not subject to exchange, nor can they be assigned to others with a contract. They are often protected even against the will of their individual holders (who, for example, can be interdicted in his wish to waive the right to physical integrity).

This "unavailability" of personality rights, has as its corollary the fact that in dealings with third parties which could have an impact on the object protected by the right, the consent of the holder takes the form of a precarious authorisation. If authorised by the holder of the right, third parties can lawfully perform acts which affect the legal right protected within the limits prescribed by the law. However, the authorisation does not transfer the right and powers inherent therein: the owner can always withdraw the authorisation granted to the third party, and any agreement to the contrary would become void.

The unavailable character of personality rights does not exclude the possibility that the parties may agree on some pecuniary considerations linked to the object protected by personality rights. The authorised third party in affecting the protected personality right of others can agree with the holder of said right on the payment of a monetary consideration in their favour.

The financial side of the relations regarding the authorisation of the holder of personality rights is among the most discussed issues in legal literature. It is not easy to reconcile a legal position that appeals, ultimately, to values such as human dignity and essential moral values with the purely financial reflections inherent in the legal right being protected. In some cases, lawyers, and therefore the legislature, have come up with some useful logical distinctions. For example, in the field of copyright, the Latin-Germanic doctrine held separate the moral right of the author, an unavailable and inalienable personal right, from the right to economic exploitation of the works of the author. The first is a non-negotiable personality right, the second is a right of a patrimonial nature, and as such can be the subject of diverse

economic transactions. It is an experience we need to bear in mind in our research.

However, these distinctions have been the result of prolonged and controversial developments in legal thought, provoked by pressing practical reasons. In the area of personal data, the path is therefore still in its early stages. For now what prevails, as we have mentioned, is the "moral" instance, the protection of the individual's personality. The property-related aspects are little-developed, because public opinion, as we noted above, has thus far not identified them clearly. For example, the economic value that the processing of data can take on has remained a little-appreciated phenomenon until recently.

The prevalence of the need for protection justifies the prevalence of a specific approach to the issue, what I am calling in this discussion, to simplify matters, a "fear-based" approach to the problem of processing of personal data, based on the fear of violations of the fundamental right in question.

I will not dwell on the theme of the new frontiers in the processing of personal data which have been opened since the advent of computer technology, the digital sphere and the internet. Information can now be treated in ways that were unthinkable only a few decades ago, thanks to the use of computers. If we add to this the fact that over the internet the collection and circulation of information have reached equally unexpected and gigantic levels, we can perceive both the novelty and the scale of the phenomenon, which some of the speakers before me have already talked about.

In the light of this new phenomenon, a fear-based reaction is natural, and there are some indisputably good reasons for it. Below I will limit myself to making a few distinctions which I think will be useful for our discussion.

A first type of danger can be found in the improper use of our data by private entities. This means businesses, especially those which are multinational and/or global, which collect and manage our data over the internet, essentially for economic and commercial purposes. They act for profit, as befits businesses in the marketplace. There are fears of abuse of several kinds, to the detriment of consumers and users.

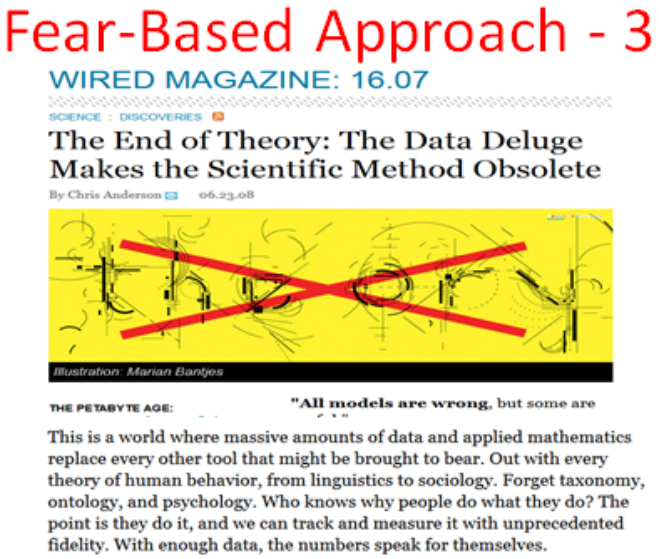
Fear-Based Approach - 1

A second set of dangers, such as the one that is most visible in the USA, relates to the use of data and possible abuses by public authorities; that is, by the government. The right to privacy is threatened by possible intrusions on the part of government agents, thus exposing individuals to profiling, controls and subsequent restrictions on their freedoms.

Fear-Based Approach - 2

A third group of fears, which explain the reaction to regulations in defence of individuals, relate to the usual concerns that we have regarding things that we understand little because they are still too recent. This is the fear of the new and of our ignorance of the possible effects it could have on our

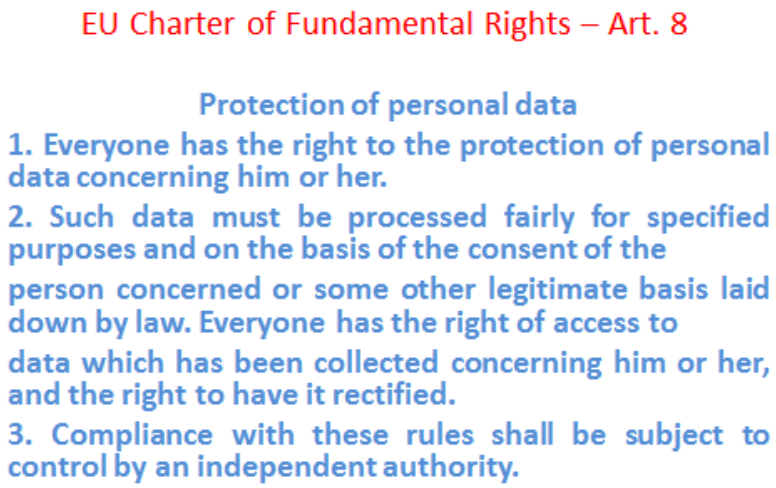
consolidated worldviews, patterns of life and relationships we are familiar with. The fear of the unknown, in short.



Naturally, the fear-based approach has resulted in the reaction of regulations in defence of individual prerogatives.

The regulations introduced in the European Union, since 1995, are a good example. Today, the EU Commission is calling for even more stringent legislation to protect our rights.

European Union legislature has also consecrated the protection of personal data in the Charter of Fundamental Rights, among other inviolable freedoms for European citizens.



It is interesting to note that the approach of the European Union, while guaranteeing the "protection" of the data, also notes, on the one hand, the inevitability of their processing and, on the other hand, "constitutionalises" the establishment of administrative authorities (which are independent of the executive power or governments) to preside over the specific protection of individuals. This is a vision (in my opinion, paternalistic) which is typical of the EU approach, which trusts in the establishment of an independent authority as a *deus ex machina* capable of solving the most sensitive issues, where necessary with neutrality of action compared to political powers.

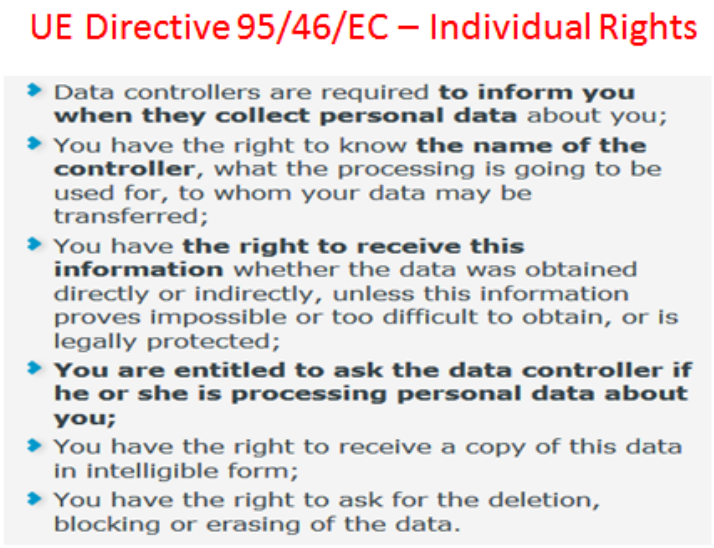
However, it is a vision which ignore the whole "economic" aspect of the processing of the data, because it is intended to protect personality rights, which are devoid of a financial nature.

We know, however, that the various Data Protection Authorities around Europe have been given significant powers of secondary legislation. Their intervention and their decisions have, and will increasingly continue to have, a strong impact not only on ensuring compliance with the regulations for the protection of the fundamental right, but also for the regulation of the economic sector that is being developed around the collection and management of data. The EU legislature has so far been shown to

underestimate - and not only in this field - the problem of the difficult and contradictory relationships between independent authorities and economic powers.

Nevertheless, these last few thoughts lie partly outside the scope of our argument here, which is why I am concerned instead with emphasising that legislation has so far been oriented to define the framework for the "protection", the "defence" of the individual, as required by the fear-based approach. It is thus a law that reflects (and at the same time feeds) the current debate and the common feeling of European citizens (by the way, what cannot be missed in the Commission's preface, in announcing the reform of the applicable legislation, is the fact that according to the Eurobarometer survey 70% of citizens are worried about how their data are processed; a survey that could perhaps have also have stimulated some critical reflection on the effectiveness of the Data Protection Authorities and the legislative approach which has already been in place for a couple of decades).

The legislative response has resulted in the issuing of EU Directives and their subsequent transposition within national laws.



The fundamental core of this legislation, highly articulate, is the introduction of the right of individuals to "control" the manner in which their data are processed by those who collect them (the so-called "data controllers") and the obligation of data controllers to provide processing which respects the interests of the individual. Which means, on the one hand, that there is an

obligation to provide information on the methods and aims of the processing by those who manage the data and, on the other, the recognition in favour of the interested parties of a number of powers, which include, for example, that of being able to ask for rectification of the data and to request its cancellation.

One important distinction concerns the processing of personal data by public authorities, which process data in order to fulfil the functions assigned to them by regulations, and the processing by private entities which are acting with aims which are of an economic nature or some other way not in the public interest.

For the processing of data by private parties there is a need to receive express prior authorisation from the interested parties. Accordingly, the "consent" to the treatment of data soars to a defining requisite in the full life cycle of processing (from the collection and circulation of data). In the relationships between private parties it is the authorisation given by the owner of the data, made in the conditions laid down by law, that makes the processing lawful (with some exceptions, which we do not need to concern ourselves with here).

As anticipated, the authorisation is still not the origin of a private contract that concerns the processing of the data. It is always revocable. The third party is authorised to provide processing, without depriving the party concerned of his/her prerogatives of control and withdrawal of consent. Moreover, while the authorisation of processing requires adequate information about the purpose, methods and persons responsible for the processing itself, it does not bind the data controller to the actual performance of the activities for the purpose of which the use of the data was required, nor does it associate the interested party in any way in the management of the economic and legal handling of the data. It marks the limits of permitted use, but the data controller is not obliged to carry out the processing. It must carefully store the data, and if managing them must do so within the limitations of and in the manner required by law, but it is not required to report back on their use, especially in the aggregate, let alone provide an account of the operations (as long as they are within the scope of those previously allowed) that it has carried out (or not) with the data, or of the transactions (as long as they are within the context of those previously allowed) that may be carried out with the data. The economic value gained from the data management, and the legal transactions of any value exchanged on the market or within the business processes of the data controller, do not form part of the relationship with the

person who has consented to processing. In short, the possible economic use of the data is not in itself an arrangement which legally and economically involves the party to whom the data in question relate and which has given its consent to their processing.

The data controller authorised to carry out the processing can then manage the data, subject to compliance with the law and "consented" uses, without being in any other way bound by the parties who have authorised their use. The data controller can decide to make as much use as possible of the lawful management of the data.

And this, in general, is the other possible and different approach to data management, one based on the extraction of the value associated with their processing, which for simplicity I shall call the value-based approach.

The industry involved in the processing and supply of data, in the predictions and metrics made possible by this processing (Big Data) is in full development. For some, it is the real "new economy" of the near future.

Value-Based Approach

Therefore, another possible approach to the processing of the data is oriented towards highlighting the economic potential linked to the use of this resource, today more than ever made possible by new technologies and the internet.

This is true in the field of public administration, where processing can lead to savings and the provision of more efficient public services.

Value-Based Approach - PA

McKinsey&Company

Harnessing big data in the public sector has enormous potential, too. If US healthcare were to use big data creatively and effectively to drive efficiency and quality, the sector could create more than $300 billion in value every year. Two-thirds of that would be in the form of reducing US healthcare expenditure by about 8 percent. In the developed economies of Europe, government administrators could save more than €100 billion ($149 billion) in operational efficiency improvements alone by using big data, not including using big data to reduce fraud and errors and boost the collection of tax revenues. And users of services enabled by personal-location data could capture $600 billion in consumer surplus. The research offers seven key insights.

And obviously it also applies to the private sector, where it is there is still a rich market of intermediaries in the flow of data, as shown for example by the case of Acxiom, a little-known company which is nevertheless the leader of a multi-billion dollar industry (database marketing).

Value-Based Approach: Acxiom

The New York Times

Mapping, and Sharing, the Consumer Genome

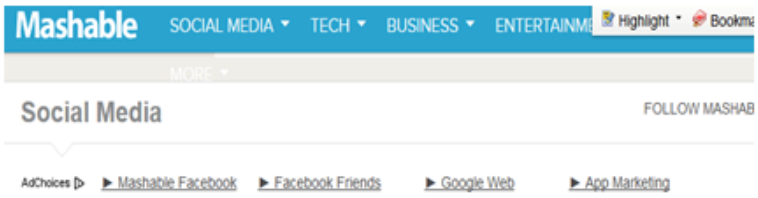
Justin Bolle for The New York Times

Acxiom's headquarters in Little Rock, Ark. Analysts say the company has amassed the world's largest commercial database on consumers.

By NATASHA SINGER
Published: June 16, 2012 | 92 Comments

The economic opportunities created by data-based marketing, from the profiling of consumers and users to the use of information collected for the intelligence purposes of business strategies and companies, for the conquest of markets and more efficient allocation of resources invested, are endless and are already the subject of abundant literature, as well as substantial investment, especially by companies within the information economy.

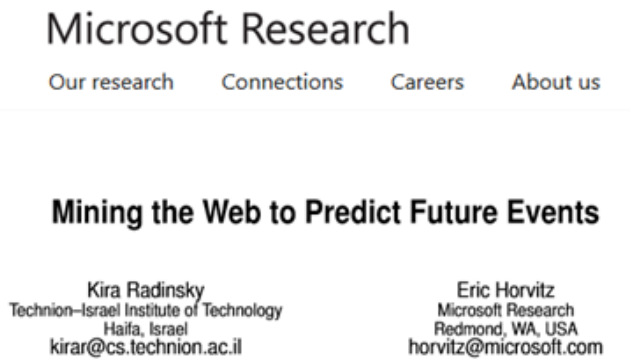
Value-Based Approach / Predictions



Google Invests in App that Predicts the Future

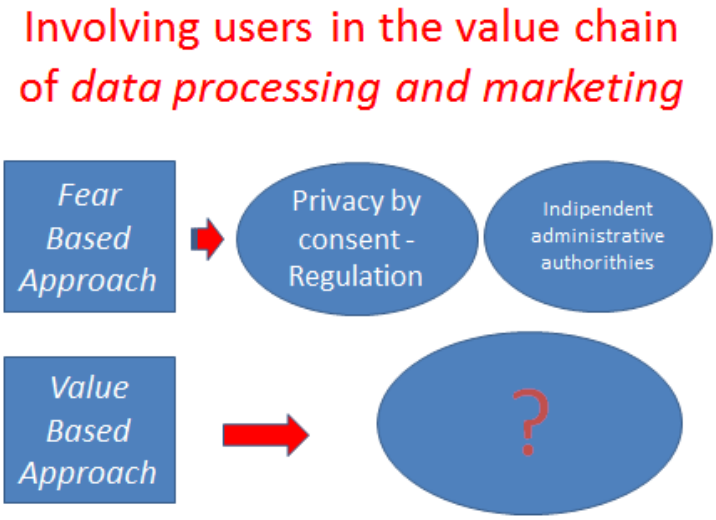
As a counterpart to the fear-based approach, the perspective in question (value-based approach) lets us glimpse ever more fascinating uses, right up to the development of techniques to extract the prediction of future events from the web.

Value-Based Approach - Predictions



But the, what is the role of individuals, those whose data are collected and used in the context of the value-based approach? The fear-based approach has offered its legislative guarantees, going as far as enshrining fundamental

rights and the creation of independent administrative authorities dedicated to the control of the processing of their data. But what is the position of individuals with regard to the economic use of this resource?



Research on "cooperative commons" carried out by the LUISS aims to investigate this profile, not only in terms of its legal and economic aspects, but as part of a broader perspective, triggering a cultural debate that goes beyond the fear-based approach to see individuals, people and the community involved in a more active, and not merely a defensive, role.

In fact, the interactions over the internet, the main instrument for the collection of personal data, make up a framework in which fragments of our personality are continuously being used by third parties, without the true involvement of the interested parties. It is as if behind the scenes of a public performance taking place on social networks, on the internet, there was a little shadow moving around, a collection of other actors and forces that are not interested at all in that performance, but rather are coldly committed to collecting and processing the information derived from it to exploit it for their own exclusive purposes (economic, government, scientific, etc.).

Moreover, it is natural that a profound rethinking of the phenomenon should be in place, given its size, the speed of its evolution and the social and economic importance that it is taking on.

The purpose of the research project is therefore to explore a different approach from that which hitherto has mostly studied instances of protection of the interested parties.

Indeed, many are looking for new models and answers to regulate the industry.

Data Protection Governance
For Business Entities

- Privacy by Consent
- Privacy by Self-regulation
- Privacy by Design
- Privacy by Contract?

The European model of protection of personal data as a guarantee of personal freedom is being challenged by the need to balance the interests of trade and industry: companies need to leverage data within global competition, and laws that are too restrictive, which are determined by red tape, or that fragment the European market by imposing multifarious and expensive obligations for the processing of the data, could hamper the competitiveness of companies and their efficiency, ultimately increasing costs which are also borne by consumers and users.

Other options have been proposed which emphasise self-regulation (especially in North America) or the identification of standards for the protection of data to be integrated preventively into the engineering of business processes and information technology (the so-called "privacy-by-design" proposed by Dr. Ann Cavoukian, in Canada).

As regards private individuals, this is a study of how the "privacy-by-consent" model adopted by the European legislation could be integrated, giving individuals a role in the value chain generated by the data processing. This requires supporting both the moral protection of the individual to whom the data relate and the recognition of rights and prerogatives of an economic

nature. As mentioned earlier, a significant precedent is reflected in the field of intellectual property, in the area of copyright, for example.

Moreover, within the scope of legal relations with financial content, it does not seem applicable to delegate the representation and management of the interests of the individual to public authorities. In a market economy, the decentralisation of trade is expected to remain at the base of the model of relationships that we are aiming to enshrine in a regulatory structure. To use a slogan, we would like to study forms of "privacy-by-contract", creating a concept that considers the user's data as a "common asset", belonging to individuals who participate in interactions on the internet. Hence, as we will see shortly, the idea of cooperative commons.

I would now like to give a specific example of another possible approach, inspired by a very common operation, which I think has been undergone by anyone who has ever subscribed to an online service in Italy, in which they register and have to provide personal information to the service provider.

The three slides that follow contain extracts from a typical "privacy policy" that the user encounters when trying to register for a service offered via the web. The information on data processing required by law, in this case has been broken down by the owner of the website into four main sections (from A to D, in our example), depending on the different purposes of the processing itself.

Privacy-by-Contract
Sample Consent Form

- **The personal information you provide to the Owner may be used:**
- **(a) (Registration) to provide consent for and manage your registration on the Site;**
- **(b) (E-commerce) for the management and execution of your possible purchase orders;**

Privacy-by-Contract / Marketing

(c) (Marketing) for the sending of informative and commercial communications, or those of a promotional nature (including our newsletter), advertising material and/or offers of goods and services, by any means (known or otherwise) including, by way of example and without limitation, post, internet, telephone, e-mail, MMS, SMS, from Italy or from abroad (including countries outside the European Community) by the Owner, by parent companies, subsidiaries and/or affiliates thereof, as well as by physical or legal entities bound contractually to the Owner and/or which, in any case, collaborate in the business of the owner;

Privacy-by-Contract / Profiling

(d) (Profiling) to provide consent for the processing and completion of statistical and market studies, as well as for the analysis of the tastes, preferences, habits, needs and choices of consumption by the Owner, by parent companies, subsidiaries and/or affiliates thereof, as well as by physical or legal entities bound contractually to the Owner and/or which, in any case, are commercial partners of the Owner.

As one can see, the person who needs to collect the data also establishes, unilaterally, the subdivision of the purposes and methods of processing based on the requests for consent that need to be obtained from the user, a consent which may be granted for certain purposes and denied for others. All this takes place in a framework outlined by the law and the practices allowed by the Data Protection Authority.

On the basis of the information thus prepared the site in question (or rather, the data controller) requires permission ("consent" to the processing of personal data). The user can grant it or not, but cannot negotiate, not for a clearer indication of the purpose, nor for a more analytical subdivision of the

forms of processing. He/she has no way to obtain a broadening of options to choose from for the providing of consent. He/she needs to join (or not) the scheme that has been prepared by the data controller.

Imagine if a negotiation was nonetheless possible. In the two slides that follow, in the left column we can see the model established unilaterally by the data controller; while on the right there is a hypothetical form based on negotiation.

In the hypothetical negotiation, a first difference could result from the greater fractioning of the types of processing to be authorised, arising from a request to that effect by the user. The user providing the data may thus have more possible choices. It may be preferable for him/her to agree only to some of the processing purposes/forms, having more options than the data controller tends to offer when acting unilaterally. Differentiation appears to offer several advantages and not necessarily only for the user. An economist would know how to formalise this intuitive result.

In the presence of an effective possible negotiation, of bargaining for the scope of consent to processing, while remaining within a framework laid down by law, we could also imagine that those collecting the data, having an interest in obtaining them since they have a "value", would be willing to provide some form of incentive (if not a fee) to guarantee their release by the user. I will try to show this in the following slide:

So, in the hypothetical "negotiation" of privacy-by-contract, the parties segment the modules for the provision of consent. In addition, those collecting the data may provide incentives for the provision of consent, increasing in proportion to the greater availability given by the user in terms of the processing aims or methods, or even as a possible function of the increasing amount of personal data the user is prepared to provide. The incentives could take on various forms. Imagine a hypothetical accumulation of points in order to obtain discounts on the purchase of goods or services offered by the site.

In practice, often in an implicit way, forms of incentives already exist (for instance, those who register at a site providing authorisation for the processing of their data generally receive additional services, although often these can also be provided in the absence of registration).

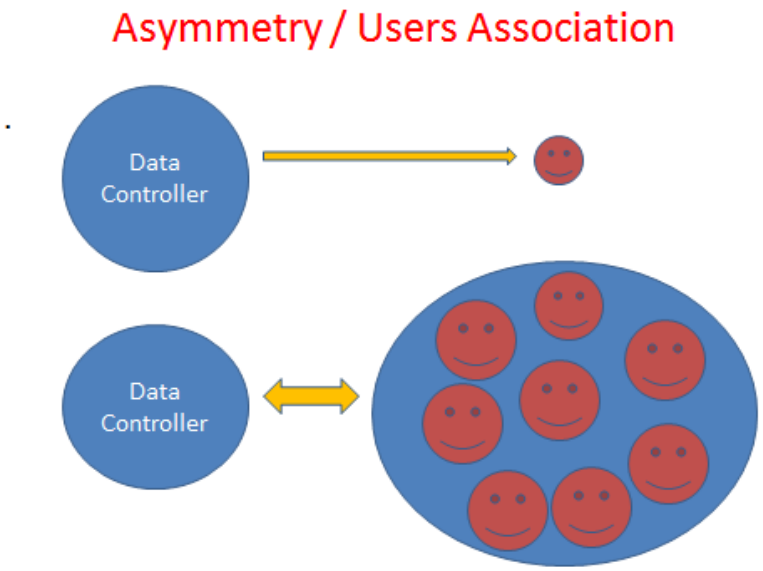
This is just one example. The underlying logic is that if personal data have a value, there should be a way to exchange that value with private negotiations and tools, which allow the creator of the data to retain a portion of the value that the data contain.

Obviously, the weak point of such a reconstruction - even before looking at the legal obstacles - is that the user is a contractor with no negotiating power. Given the other transaction costs, those collecting the data (the so-called "owner", or controller, of their processing) has no interest, nor even an opportunity, to engage in an indefinite number of negotiations or agreements with individual users. In addition, considered in isolation, the

personal data of each individual user have a value which is almost insignificant. The scheme, in short, poses a hypothetical negotiation without taking into account the fact that the parties to it are in an asymmetric position.

Hence there is a need to reduce this asymmetry, in order to provide contractual weight to the weak contractor and greater value to the data, as well as simplifying the negotiating schemes in order to reduce transaction costs.

These needs could be met through partnerships between users.



The website operator would thus deal not with the individual user, but an association of users. It would not deal with the individual's personal data, but with a significant set of data. The pooling of data and the interest in the management of their value would reduce the asymmetries and make the possibility of negotiation less unlikely.

Furthermore, the association could define standardised forms for the provision of consent, establishing predefined clusters of processing aims and methods, to be affirmed on the market as a standard for the granting of permits. The various modules could also be graded according to the number and the quality of the data to be provided.

The association, then, could take care of representing the members in the negotiation phase, or of monitoring, on behalf of the local community, the interest in the proper processing of the data and respect for the agreements reached in the interest of its members.

Finally, within privacy-by-contract, the traditional cooperative company with mutualistic purpose could be a proven tool for the representation of parties which are contractually weaker in the management of the service in question on the market. The members of a cooperative take part in the company for purposes which are not directly for-profit (i.e. intended to obtain the remuneration from the risk capital provided), but rather to receive other benefits that the market cannot offer to non-organised individuals. These are companies whose operation often also uses the egalitarian model of one man, one vote.

For these reasons, in our project we use the definition of "cooperative commons": we imagine that the organised cooperation of users, gathered together in societies, could manage a service on behalf of the community of users, whether they are members or not, for management of the authorisation for use of a common asset, that is, their personal data. These users gain value as a collective and the individuals realistically take on strength and dignity as a negotiating party, only delegating to a person to represent them as an organised group for the management of asset profiles relating to the processing of personal data. The cooperative movement has a long tradition in the representation of consumer demands and of individuals who have a weak position within the logic of the market. This is fertile ground and therefore ideal for taking on this new mission.

These are the main aspects of our research, still in its infancy, but during the continuation of which any and all contributions are welcome. In the next slide I will try to summarise the actions I think could be taken, without aiming to be exhaustive, but rather to provide a working outline.

Thank you.

Cooperative Commons – Actions

- Layer 1: *Joining keen citizens and experts into a cooperative*
- Layer 2: *Developing tech and legal tools*
- Layer 3:
- a) *Engaging scholars and citizens in the debate*
- b) *Agency towards Data controller*
- c) *Advocacy with law-makers*
- d) *Monitoring compliance*

(Alfonso Papa Malatesta)