To: the European Commission,
Directorate-General for Justice
Unit C 3 Data Protection
B-1049 Bruxelles/Brussel

From Philippe Coueignoux
11 rue de la Cour des Noues, 75020 Paris, France
and Marc Leprat
c/o Port Parallèle, 70 rue Amelot, 75011 Paris, France

01/14/2011

Subject: Consultation on the Commission's comprehensive approach on personal data protection in the European Union

The present document is submitted to the consideration of the Commission in response to its call for comments from European citizens on personal data protection.

The "Communication" published by the Commission provides an excellent framework on the subject and we are in entire agreement with its focusing on the "impact of new technologies", "the internal market", "international data transfers", "effective enforcement" and "coherence of the data protection legal framework".

Therefore the authors have taken advantage of this framework to limit their feedback to specific points which reflect their professional expertise and personal experience. Their primary objective is to show how the Commission can use simple legal measures to achieve greater consumer protection through market-driven competition and innovation.

As further detailed in the following attachment, it is recommended that the Commission:

-A- forbid bundling consumer online interactions with unnecessary personal data processing
-B- forbid targeting advertising to refer to consumer profile criteria irrelevant to the advertised offer
-C- state explicitly the use of IP addresses in consumer marketing is enough to formally identify a consumer
-D- establish a schedule of payments due to consumers by data controllers in case of personal data breaches
-E- determine liabilities of data controllers according to their scale and the nature of their business model
-F- require data controllers to segregate the costs and revenues associated with unbundled personal data processing
-G- base criminal liabilities of data controllers for systematic or reckless failure to meet their civil responsibilies

The attachment develops sections A and B at some length as the associated recommendations and, indirectly, those in sections F and G, rest on the definitions we give to the terms "bundling" and "irrelevant criteria". On the other hand we want to stress these definitions are totally compatible with the common understanding of these concepts.

Respectfully submitted,

Philippe Coueignoux PhD
Marc Leprat

PS:
Philippe Coueignoux has more than ten years of experience in personalized Internet interaction in privacy. He has developped a US Intellectual Property portfolio in this domain and founded ePrio Inc. to commercialize it in the United States. He is the author of a weekly polemical blog, Philippe's fillips, focused on eprivacy in the Information Age.

Marc Leprat has more than ten years of experience in interactive marketing. He teaches this subject in several leading French business schools, including HEC Paris. His personal research includes the role of trusted third parties in furthering the interest of consumers online.

-A- forbid bundling consumer online interactions with unnecessary personal data processing

Perhaps the most important goal explicitly endorsed by the Commission is to "ensure informed and free consent" by consumers to the holding and processing of their personal data, as stated in paragraph 2.1.5.

We believe this requirement is easily evaded today by the wide spread practice of bundling, i.e. making such a consent part of a transaction desired by the consumer, even though this consent is not germane to the fulfillment of this transaction.

a real life example:

This undesirable practice is best illustrated by voyages-SNCF.com, an Internet site selling railway tickets online.

In the first quarter of 2010, one of us needed to buy a ticket from the United States in preparation for a trip to France. Despite our desire to avoid receiving marketing emails subsequent to this transaction, we were unable to find how to do so. Bundling an opt-in consent with the completion of a desirable transaction on which the site had a complete monopoly is clearly inequitable.

In its defense, voyages-SNCF may invoke two arguments:

- its site is but an additional way for buying SNCF tickets which users are free to forsake.

It may be indeed possible to buy SNCF tickets in France through other channels, however we could not do it from the United States. More generally online transactions have become the preferred selling method, as it eliminates many unnecessary costs. From this perspective, the above argument is disingenuous and backward looking. It can only damage the development of the electronic economy.

- the European Directive 2002-58-EC (article 13, paragraph 2) allows companies to send unsollicited emails when the user address has been obtained "in the context of the sale of a product or a service". Voyages-SNCF is free to avail itself of this derogation, which substitutes a so-called "opt-out" to the general "opt-in" principle adopted by the directive.

However the European Directive 2002-58-EC (article 13, paragraph 2) further specifies an "opt-out" has to be provided "clearly and distinctly [...] in an easy manner". As it happens, current online technologies make almost no difference between the latter "opt-out" and a genuine "opt-in". In both cases, the form which the consumer uses to confirm the order includes a cell informing the consumer the company will send marketing emails at the address declared to fulfill the electronic transaction. The only difference is that the "opt-in" cell is unchecked by default while the "opt-out" cell is checked by default.

Yet we were unable to find how to opt-out in this one-click manner. Further research done on January 9, 2011, shows the relevant information to be located in a so-called Privacy Policy ("Charte de confidentialité") which refers to a Help function through which the consumer must download a separate form to fill. This makes a mockery of the directive and is designed to compel consumers to leave their consents, neither informed, nor free, with the company, unless they cancel their orders.

Voyages-SNCF.com is but an illustration of many similar practices which tie together a desirable offer and the acceptance by the users of terms and conditions bearing on the use of their personal data beyond what is strictly necessary to accept, process and fulfill a transaction on this offer.

necessity of an equitable "personal data contract":

Most online transactions require the beneficiary party to communicate personal data to the other party to enable the latter to fulfill the transaction. This applies to the case the beneficiary is a consumer. The consumer is therefore giving an informed and free consent for such use to the personal data controller as the consumer confirms the transaction.

Beyond such use of one's personal data however, no one in one's right mind will "give one's free consent" without a compensation. Whatever its nature, the existence of such a compensation implies a contract between a consumer and a company.

We recommend personal data controllers be required by law, whenever they intend to store or process personal data beyond the fulfillment of ordinary transactions, to explicitly specify those terms and conditions pertaining to consumer personal data and its compensation according to contract law. We call the result a "personal data contract".

Indeed, in the absence of such a contract, a consumer cannot know to what he or she consents. If given, such a consent can be neither "informed" nor "free".

In particular no company should be allowed to use undefined or vague terms and conditions in this contract nor change them at will without entering into a new negotiation with each user concerned. Such a contract would be inequitable, its "change at will" clause an instance of what is called in French "clause léonine". This means that most, if not all, so-called Privacy Policies put forth by organizations do not qualify as valid "personal data contract".

inequitable bundling of "personal data contracts":

Bundling occurs whenever the above "personal data contract" is made part of a larger contract relative to some offer or service.

We recommend bundling be considered illegal as inequitable.

The inequity resides in the impossibility for an ordinary consumer to give a "free consent" as this consent is made a necessary condition for a transaction desired by the consumer although this consent is not necessary for the company to fulfill it. This acknowledges the consumer is in no position to negotiate and that ordinary competition has proved unable to provide credible alternatives.

Notice companies are wont to declare their use of consumer personal data benefits consumers. If so, they should not object to unbundling "personal data contracts" since, in exchange for the assumed benefits, consumers should be expected to freely accept the "personal data contract".

Again companies cannot argue our recommendations would create unnecessary administrative burdens. If companies serve consumers, they already know how to package their goods and services in a clear, concise, convincing manner. They would only have to do the same with their offer of "personal data services".

inequitable bundling by bartering:

Many online sites today explicitly tie the "personal data contract" to the delivery of a free service. From their point of view, this is not bundling. It is a legitimate "personal data contract" in which the free service is the compensation to the consumer consenting to whatever usage will be made of his or her data.

Between two individuals, this form of bartering is indeed perfectly acceptable. Between an individual and an organization, the same form is inequitable as, once again, the user is only given a "take it or leave it" offer in the absence of credible alternatives.

We recommend any barter which exchanges a free service for the consent of a consumer as part of a "personal data contract" be allowed only as part of an alternative offered by the same organization which delivers the same service at a price without the need for a "personal data contract".

Suppose for instance that a company offers a "free access" social network in exchange for some specific rights to repurpose personal data beyond consumer-controlled sharing. If the same company offers the same social network functionality for a set price without repurposing the consumer personal data, the consumer is thus free to accept or refuse the "personal data contract", dependent on the relative values put by the consumer on the service and the obligations set forth in the "personal data contract".

As long as this principle is followed, companies are free to offer multiple forms of bartering, each with its own price, personal data contractual obligations and paying alternatives.

This principle actually increases the competitivity of the market place. For example company A offers a barter for "social networking" and an alternative at price P. Company B, better at delivering value for personal data pays consumers in cash more than P for agreeing to the corresponding "personal data contract". Similarly company C, better at delivering value for "social networking" may charge consumers less than P for this service. By using the separate offers of companies B and C, a consumer can enjoy the equivalent of A's barter and earn extra money.

This principle naturally allows a company to offer a truly free service, i.e. one which does not repurpose any personal data and hence needs no alternative.

limits of personal data:

In order to apply the recommendation against bundling, care must be taken to distinguish consumer data from company data.

For instance, when a consumer uses the keyword "France" on a search engine, the fact that this consumer searches "France" belongs to the consumer but the page of links on "France" sent in response to the request belongs to the search company. As a result, the latter may very well include paid advertisements, even if they are related to the keyword "France"as long as this response is totally independent of others consumer profile items beyond the use of this keyword. The company is equally allowed to tally how many times "France" has been requested by consumers and other such statistics on its own offer. If this search company does not repurpose the individual consumer search, linking "France" to the requesting IP beyond the need to respond to the search and defend itself against hackers, it does not need to draw a "personal data contract" and, assuming its search service is free, does not engage in an inequitable barter.

-B- forbid targeting advertising to refer to consumer profile criteria irrelevant to the advertised offer

In paragraph 2.1.3, the Commission sets forth the principle of "data minimization", i.e. "the limitation of the data controllers' processing in relation to its purposes".

We believe that this principle should be explicity applied to online targeted advertising, whether through behavioral tracking or another form of user profiling, as this is expected to be a major economic activity in the future. To use a targeting criteria irrelevant to the advertised offer is clearly beyond the purpose of selecting a suitable target and should be considered a violation of the "data minimization" principle.

an academic example

As related last year in the media: Marketers Can Glean Private Data On Facebook, by Miguel Helft (New York Times) - October 23, 2010; "researchers from Microsoft in India and the Max Planck Institute for Software Systems in Germany found that it was possible for an advertiser to find the stated sexual preference of Facebook users".

The way to do this is straightforward: target an ad to any criteria in a user profile, e.g. a car ad to Facebook users based on religious practice or sexual preference, and all users responding to it willy nilly disclose the fact their profiles satisfy this criteria.

how not to control targeted advertising:

It may seem an easy fix to forbid the use of so-called sensitive criteria in targeted advertising. This however is ill advised for three reasons.

- even so-called sensitive criteria can be usefully and legitimately targeted.

Suppose a company sells kosher or halal food. It should be allowed to target users based on their religious practices.
In the same way a charitable organization focused on AIDS prevention should be allowed to target users based on their sexual preferences.

- the list of sensitive criteria is potentially very large.

In job recruiting, it is well known that the candidate address can be a factor for discrimination, for example when it signals a neighborhood with a high proportion of socially or economically disadvantaged minorities.

- even the most innocuous profile item can be abused in conjunction with other profile elements

If a user is known to like reading comic books, correlating this criteria with other information available in this user's profile can be enough to ascertain the user is less than 18 years old. This criteria can then be used to subrepticiously target minors with offers in contradiction with the code of conduct ostensibly followed by the company.

the principle of legitimate targeted advertising:

There are three aspects to a sound control of targeted advertising: principle, practice, enforcement.

In line with its principle of "data minimization", we recommend the Commission forbid targeted advertising based on irrelevant criteria.

practical definition of criteria irrelevancy:

We further recommend criteria irrelevancy be made a practical matter, decided on a case by case basis rather than on general rules. In order to minimize legal procedures and expenses, we recommend to set up a European Data Authority and authorize it to issue safe harbor decisions on request. If legitimate, such decisions might account for specific country law.

For example a car manufacturer association could publish a list of criteria and petition the Authority to pre-approve it for car advertisements. To eliminate any liabilities on innovative but potentially suspicious criteria not included on this list, an individual car manufacturer, or a advertising network could further request a private pre-approval from the Authority on such special criteria. However nothing would prevent a bold entrepreneur to forsake the safe harbor and freely advertise in an uncensored way, accepting the responsibility of such decisions.

In this example the decision may be freely left in the hands of a regulatory authority but wide initiative is given to intermediate bodies representing the industry. It shows how self-regulation, which the Commission wishes to develop per paragraph 2.2.5, may be used efficiently in a manner which does not hurt the interest of the consumers.

enforcement of targeted advertising criteria relevancy

Enforcement should be based on the joint responsibility of:

- the advertiser who decides on the criteria to target for an ad
- the company holding the profiles to be targeted
- the company whose algorithm is used to target the profiles
- the site on whose pages the targeted ad is displayed

The responsibility would include the maintenance of an auditable process of all targeting requests and their associated ads.

The European Data Authority would have the power to make periodic or spot audits at any of these parties and refer any problem it uncovers for legal prosecution according to section G below.

economic considerations:

As the company whose algorithm is used to target the profiles, by design, has direct operational access to all the elements to be audited, its recording the information for auditing purposes will be inexpensive.

The more formal the process of managing targeted ads, the easier it will be to enforce the principle and benefit from safe harbor decisions. This will spur investments and innovation towards the development of such processes, in which a process master is able to prevent any rogue client from straying from pre-arranged and pre-approved criteria. For instance if it is illegal to discriminate job candidates by age or sex, no recruiter would be able to target a recruitment campaign on these criteria if he or she had to use a form controlled by the process master on which these criteria did not appear.

Joint responsibility will indeed ensure that companies with deep pockets and reputable brand names will police the many parties with whom they deal and provide seals of approval to reliable subcontractors or clients. This calls again for efficient industry self regulation.

-C- state explicitly the use of IP addresses in consumer marketing is enough to formally identify a consumer

In paragraph 2.1.1, the Commission recalls the importance of consumer identity, using the expression "identified or identifiable person, either directly or indirectly".

While we agree with the Commission on the importance of keeping this definition flexible, we recommend it explicitly declare an Internet Protocol address (IP) as one specific mean "likely reasonably to be used either by the controller or by any other person to identify the said person'.

Since most online activities associated with a "personal data contract" as defined in section A are based on associating a profile with an IP, either by using cookies implanted at this IP, or by recording the IP of consumers in a central database, this is a capital determination.

This measure is necessary to fulfill the desire of the Commission "to ensure a coherent application of data protection" as called forth in paragraph 2.1.1 since, for example, the so-called HADOPI law in France has established that an IP is sufficient information to hold a consumer liable of copyrights infringements. Indeed equity requires consumer protection not to be inferior to consumer liability.

-D- establish a schedule of payments due to consumers by data controllers in case of personal data breaches

In paragraph 2.1.2, the Commission opens the possibility of extending mandatory "personal data breach notification" to data controllers beyond the telecommunication sector. On the other hand it lists "effective enforcement" in section 1 as one of its major goals.

We believe the most effective enforcement is, whenever possible, to rely on market mechanism as long as the market participants bear the real costs of their actions. In this regard the issue with personal data breaches is twofold:

- it is rarely possible to establish a direct link between a specific data breach and a specific wrong suffered by a consumer.
- consumer data controllers normally bear no marginal cost as a result of a data breach, even if notification is made mandatory, as it can be implemented through electronic means. Even the negative impact on their reputation is minimum as, due to breach fatigue, data breaches generate no media coverage unless some new record is broken.

a real life example:

We contrast this situation with the special case of credit card companies.

One of us resides in the United States. Because he uses his credit card for many online transactions, he has been the victim of multiple credit card id thefts. As a result, the average duration of his card is six months, instead of its nominal two years. Recently his card had to be replaced less than three weeks after having been issued.

Due to legal obligations and commercial practice, he bears no cost besides the inconvenience of having to change his card. On the contrary the card operator and associated parties risk significant liabilities if a card id theft is not immediately spotted. As a result the card operator has invested in an excellent alert system, able to spot suspicious transactions, even the small fraudulent ones which card id thieves use to validate the information stolen, prior to reselling it at a much higher price.

Even with this alert system, the card operator incurs the cost of replacing each compromised card. The merchant picked by the thief to validate the stolen card id may also lose the value of the transaction. This creates a strong reason for these parties to invest in the protection of card ids, especially when used online.

personal data breaches:

The issue mentioned above can be solved by analogy with pollution. When the pollutant is a common result of overall economic activity, it is in general near impossible to hold one particular polluter responsible for harming one particular consumer's health. Yet effective mechanisms have been put in place or advocated by European authorities to encourage pollution control.

Therefore we recommend the Commission establish a schedule of mandatory payments due to consumers concerned by the data controller at which the data breach occurred. Their level are further discussed in section E below.

These payments, or civil penalties, are independent of any compensation a particular consumer may be entitled to seek and receive, were a direct link provable between a specific data breach and a specific harm sustained.

Rather the goal is to internalize the global cost of personal data violations among all possible organizations which contribute to this phenomenon and therefore create a direct, measurable financial risk for these organizations. It is expected the latter will find economical to insure themselves against it and strive to lower the corresponding insurance premiums. This in turn will spur investments and innovation in consumer data protection.

Because this recommendation creates a simple civil liability, it is to be expected that some organizations may under-report privacy breaches. However such a behavior will not have a significant positive impact on their bottom line unless it becomes systematic. In this case, section G recommends the creation of a criminal liability sufficient to prevent most organizations from taking this additional risk.

-E- determine liabilities of data controllers according to their scale and the nature of their business model

In section 1, the Commission acknowledges the impact of "unprecedented scale" on the issue of personal data protection and in paragraph 2.2.1, the Commission sets itself the goal of reaching "a level playing field for data controllers".

In line with these two considerations, we recommend that, in establishing the payment schedule discussed in previous section D, care should be taken to account for two factors, the scale of the data controller's operation and its business model.

We further propose to classify data controllers in four groups according to the number of profiles held:

- below 10,000 small scale
- from 10,000 to 1,000,000 medium scale
- from 1,000,000 to 100,000,000 large scale
- above 100,000,000 very large scale

Legitimate business models in turn can be classified in three categories using the "personal data contract" concept of section A:

- holding personal data solely for the purpose of fulfilling an offer or a service not requiring a "personal data contract"
- repurposing personal data held for fulfilling an offer or a service according to an unbundled "personal data contract"
- holding personal data solely for the purpose of fulfilling a "personal data contract"

Penalties should be set so that current insurance premiums would not rise significantly for small scale operations and business models which do not rely on "personal data contracts". The development of ordinary online commerce would in fact benefit from a rise in consumer confidence as they would know their personal data receive the level of protection they can reasonably expect.

On the other hand, large scale advertising networks solely dedicated to the fulfillment of "personal data contracts" on behalf of their clients should be held to a payment high enough to prevent the network from padding its profit by refusing to shoulder the full cost of the best protection offered by state of the art technologies. As a result, such economic actors would gladly support investments in any innovative technology or business model which would lower the cost of such protection.

Through this market mechanism, the Commission would effectively rebalance innovation which otherwise, as shown in its section 1, ignores and therefore increases consumer risk. With this same mechanism, the Commission would also promote "privacy enhancing technologies" as set forth in paragraph 2.2.4, without having to dictate any specific development.

In section B, we downplayed the need to forbid the use of so-called sensitive criteria in targeted advertising. However it would be in the spirit of the present section if the Commission, following the proposal of its paragraph 2.1.6, were to take the storing of such sensitive criteria into account as a third factor in establishing its payment schedule.

-F- require data controllers to segregate the costs and revenues associated with unbundled personal data processing

In paragraph 2.2.1, the Commission sets itself the goal of reaching "a level playing field for data controllers".

In section A, and again in section E, we have recommended to segregate consumer data related activities subject to the implementation of a "personal data contract" agreed to by consumers from those necessary to the normal operation of electronic commerce.

In section A, we have further recommended that any so-called "free service" which is delivered to consumers in a barter against specific consumer data rights be given an explicit equivalent price.

We now recommend that organizations which engage in activities covered by "personal data contracts" clearly account for them in their financial reporting, with segregated costs and revenues.
In particular any "free service" which is in fact a barter should be accounted for as bringing revenues measured according to the full and explicit value of the barter.

This recommendation contributes to a level field among all organizations with regard to liabilities derived from financial reporting, such as taxation.
Assume for instance social networking services are subject to a VAT. Whether such a service is bartered as "free" or for a fee, the tax will be the same.
Note that all the costs of providing such bartered "free services" are already accounted for as expenses by the service provider.

This recommendation not only levels the field but also leaves organizations free to set their own price and encourages the discovery of realistic prices through competitive markets.

If a company sets too high a price for its equivalent barterless service, it will inflate the tax bill on its bartered "free service" and encourage more efficient companies to offer the same barterless service at a lesser price and thus steal away many of the consumers who initially felt compelled to pick its barter.

On the contrary if, in order to minimize the tax bill on its bartered "free service", a company sets too low a price for its equivalent barterless service, it might incur a loss on the latter as consumers flock to this more advantageous proposal.

-G- base criminal liabilities of data controllers for systematic or reckless failure to meet their civil responsibilities

In paragraph 2.1.7, the Commission leaves open the introduction of criminal sanctions to strengthen the "enforcement" of data protection rules.

The previous sections have recommended several obligations be imposed on organizations holding or processing personal data:
section A:
- drawing an explicit "personal data contract" with consumers
- eliminating all inequitable clauses in such contracts as created through bundling

section B
- eliminating all irrelevant criteria for targeted advertisements

section D
- reporting all data breaches and paying a civil penalty to each user concerned

section F
- segregating costs and revenues associated with unbundled personal data processing

It is proposed that any attempt to knowingly bypass one or more of these obligations in a systematic or reckless manner be made a criminal offense. It is further proposed any associated civil or administrative penalty be trebled if a guilty verdict is handed down. This creates a powerful enforcement mechanism relative to these obligations.

For example, a company could
- persist in subjecting its users to inequitable clauses in a systematic manner
- fail to report personal data breaches and pay the corresponding civil penalties
- take a decision contrary to common data protection practices and be later found material to a subsequent data breach.

If the complaint of a specific user results in a criminal case and a guilty verdict, it is highly likely that the incriminating behavior has affected many more users and will prompt them to start a civil proceeding, as their hope of compensation has increased and the burden of proving their case has decreased, both significantly. The company concerned would therefore have a strong financial interest in avoiding such a risk.