ePrio

1/27/2011

National Telecommunications and Information Administration,
US Department of Commerce
141 Constitution Av, N.W.
Room 4725
Washington, D.C., 20230

Subject: Information Privacy and Innovation in the Internet Economy

Focused on the intersection of privacy and innovation, the green paper published by the Department of Commerce Internet Policy Task Force fully resonates with my personal and professional experience. Indeed, holding a PhD in Electrical Engineering and Computer Science from MIT, I have more than ten years of experience in "personalized Internet interactions in privacy" and have applied for three patents in this field. The first one has been granted as US Patent no 6,092,197. The other ones are pending US Patent Applications, respectively recorded as no 2006/0053279 and no 2009/0076914.

Founder of ePrio Inc. and operator of the site eprivacy.com, I am currently in the process of securing financing and acknowledge that my views are informed by the technologies I have developped and compatible with and favorable to, the commercial goals pursued by ePrio. Far from being a conflict of interest, this link enables me to credibly add my voice to the minority of those who believe there is no necessary opposition between information privacy and Internet innovation.

In this capacity, I fully concur with the agenda summarized by the DoC task force in its conclusion, especially its first three objectives

- (1) promoting entrepreneurship, innovation, and economic development
- (2) protecting informed choice and individual privacy in order to promote user trust
- (3) giving existing and emerging Internet companies more consistency, uniformity, and predictability in the privacy protections expected by consumers and required by law

Among the many good suggestions set forth by the green paper, I also want to single out its advocating safe harbors as an efficient mechanism which can significantly lower the costs and hence the risks related to information privacy, eprivacy in short.

However the green paper suffers in my opinion from a bias according to which eprivacy and innovation are in conflict and some acceptable trade-off must therefore be found. Such a position can only stem from a misunderstanding or, a possibility difficult to accept, a mistrust of free markets.

In the attachment below, I volunteer answers for 20 of the 42 questions put out for comment by the DoC. But this feedback will gain in clarity and force by being put back in the context of my own recommendations on how to resolve the apparent conflict between eprivacy and innovation, i.e.:

- (a) subject all collection and use of consumer data to explicit and equitable contracts
- (b) forbid the use of irrelevant criteria in targeted advertising with the help of a safe harbor mechanism
- (c) require organizations affected by security breaches to compensate the consumers concerned
- (d) make the willfull ignorance of these three civil contractual obligations a federal criminal offence

Respectfully submitted

Philippe Coueignoux PhD
President
ePrio Inc.

PS: Philippe Coueignoux is also the author of "Philippe's Fillips", a weekly blog in defense of individuals' data rights, and "Vulnerabilities and Liabilities in the Information Age", an MBA level academic course, both published on eprivacy.com.

ePrio

Comments to the Department of Commerce on Information Privacy and Innovation

Table of Content:

- Part I - A Free Market-Based Approach to Consumer ePrivacy

Consumer personal information is a good which, like any other, has a cost and a value. Because it acquires most of its value today when processed by computer algorithms, it is commonly described as some fluid whose "free flow" must be encouraged much like electricity running through electric motors or water through industrial plants.

Unfortunately the expression "free flow" is highly ambiguous as it can be applied to both physical and economic phenomena. In the case of electricity for instance, nobody has ever suggested that, because it was important to decrease the many obstacles by which physics impedes its flow, therefore its users did not need to pay the power plants for its production as such an economic imposition would prevent its users from maximizing the benefits they receive from its flow.

Yet consumers' wishes for power over their production of personal information, i.e. the right for information privacy, eprivacy in short, is widely considered as an obstacle to the "free flow" of information, requiring some kind of a trade-off, i.e., to quote Mr Cameron Kerry, General Counsel, "policy approaches that balance privacy with the free flow of information".

A better approach is to blame the absence today of free market mechanisms to enable the consumers, like power plants, to negotiate and receive a fair, market-based price recognizing their costs of production and their rights to a just profit. Nielsen compensates the households it recruits for its TV rating panels. So the issue is not one of principle but of implementation.

- Part II - Obstacles to a Free Market and Subsequent Decrease of Innovation

The main obstacle to the creation of a free market on which consumers can negotiate their eprivacy is that the organizations with which they would be expected to negotiate have been allowed to use a wide array of inequitable practices to procure the same goods for free.

The most egregious practice is to bundle the right to reuse the personal information necessary to the fulfillment of a transaction desired by a consumer with this transaction. It is true that the consumer is not obliged to go ahead with the transaction but leaving someone the choice between one's life and one's purse has never absolved the persone making this offer from the guilt of highway robbery.

Another common practice is to compel the consumers to barter their information for a service touted as offering an equivalent value. While acceptable in principle, bartering represents a less advance stage of a market economy which, in particular, makes it easy for a party with a disproportionate power to impose inequitable terms on its counterpart as the absence of price information makes it difficult to compare competing offers, as would be the case on a normal market.

A third way to hoodwink consumers into delivering personal information for free is for organizations to promise to abide by some restraints and exercise a certain level of care, typically by granting their users the benefit of a "privacy policy", but to reserve the right to change this policy at will, thereby voiding the value of any promise made.

The absence of a free market has grave consequences for innovation. In itself neutral, innovation looks for new solutions in all possible human endeavors. It is however financed in proportion to its economic benefits. Unfortunately innovation which favors eprivacy cannot create value, as any investment in eprivacy would neither lower the cost to organizations of procuring what is already free nor bring benefits to consumers who cannot rise their prices. On the contrary the only innovation which can succeed is what increases the flow of free personal information from consumers to organizations as the latter invest to increase their benefits, i.e. the very developments which further threaten eprivacy.

The current and all too real opposition between innovation and eprivacy is thus but an artifact of the absence of a free market.

- Part III - The Arguments Against a Free Market Approach to Consumer ePrivacy

The organizations which have grown used to procure consumer information for free are naturally against a free market approach. Their arguments, as formulated for instance by Berin Szoka, Senior Fellow, The Progress and Freedom Foundation, to the FTC Privacy Roundtables (Dec. 7, 2009) deserve to be heard.

The first objection is a matter of principle. "*There is no free lunch*: We cannot escape the trade-off between locking down information and the many benefits for consumers of the free flow of information." This of course is but an example of the confusion about "free flows" discussed in Part I above. In equity, the only "free flow of information" which makes economical sense is what occurs on a free market, not what is to be had for free in the absence of a market. It is precisely the absence of a market which leaves the consumers the unpalatable choice between "locking down their information" or losing it altogether.

The second objection is rhetorical. "What exactly is the "harm" or market failure that requires government intervention?" Although this question implies that there is no market failure, Part II has made clear the market of consumer personal information is non existent and only government intervention can force organizations to negotiate with consumers.

Organizations are understandably wary to clearly put some other arguments in writing as they imply consumers are "lazy" and "stupid". In view of their lazyness, organizations must force consumers to "opt-out" rather than "opt-in" in order to acquire rights over their personal information. In view of their stupidity, consumers must be compelled to deliver their information for free as they are not smart enough to value "the many benefits" they derive from "the free flow of information".

These last two arguments are highly suspicious. If they do not deal with consumers, organizations have no standing to judge them. If they do, either because they sell something or sollicit donations, they behave towards consumers in the normal course of their business in a very different way. They know how to appeal to consumer self-interest and prompt them to actively seek whatever benefits these organizations offer to bestow on them. When it comes to acquiring personal information, it is more logical to replace consumer "lazyness" by the fact organizations do not offer them high enough a compensation, and consumer "stupidity" by the fact organizations are incapable of articulating real, direct, convincing benefits.

The last objection against a free market approach to consumer eprivacy is that it would impose a burden on commerce. For instance "tailored advertising increases the effectiveness of speech of all kind, whether the advertiser is "selling" product, services, ideas, political candidates or communities". Subject such "tailored advertising" to the costs of acquiring the relevant consumer information on a free market and, it is implied, you impair the effectiveness of commerce, nay of democracy itself.

This argument merits a detailed examination according to how organizations acquire and use consumer information.

Whenever consumer information is necessary to fulfill a transaction, the consumer's closing the sought after transaction naturally conveys the required consent. No extra "burden" needs to be attached to this transaction besides the normal duty for the organization receiving the information to keep it confidential and abstain from using it for any other purposes unless explicitly required by law.

Whenever an organization wants to re-purpose this consumer information for its own marketing, it is easy to sollicit the consumer consent for free as the current custom prevails. The "burden" of putting a short explanation to this effect next to the consumer order confirmation, with a cell pre-checked for an opt-out or unchecked for an opt-in, is inconsequential given today's technology.

If an organization wants to re-purpose this consumer information or acquire any other consumer information for any other usage, including "tailored advertising", it cannot be considered a "burden" on commerce nor on democracy to require a contract to be freely established and signed by both the organization and the consumer, no more than paying one's own suppliers. Imagine a world where importers in the United States stopped paying their Chinese suppliers, where the Recording Industry Association of America had to accept music can be freely copied and where political candidates could commandeer TV stations at will.

Fourth case, an organization barters access to a free service against a consent to give away some rights. This is a true contract, offering a real, direct compensation to the consumer. Requiring this contract to be equitable, free from deceptive clauses, can only facilitate commerce. Further requiring the organization to offer the same service, perhaps against some payment, but without any cession of consumer rights beyond what is needed to provision the service, increases market choice and thus commercial activity.

Therefore the only valid argument against a free market approach is to doubt such an approach can be implemented.

- Part IV - The Implementation of a Free Market Approach to Consumer ePrivacy

- (a) subject all collection and use of consumer data to explicit and equitable contracts

"The majority of respondents" to a preliminary inquiry by the DoC has expressed the need for "transparency and informed consent" and its task force repeatedly endorsed this finding as it suggests "the broad adoption of comprehensive Fair Information Practice Principles" (FIPPs). The following recommendation simply proposes a general and enforceable implementation.

necessity of an equitable "personal data contract":

Most online transactions require the beneficiary party, when this party is a consumer, to communicate personal data to the other party to enable the latter to fulfill the transaction. As the consumer confirms the transaction, he or she hereby gives an informed and free consent for such use to the information receiver .

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 the information receiver.

I recommend information receivers be required by law, whenever they intend to store or process personal data beyond the fulfillment of ordinary transactions and any subsequent legal obligation, to explicitly specify those terms and conditions pertaining to consumer personal data and its compensation and obtain the consumer's explicit approval according to contract law. I call the result a "personal data contract".

In the absence of such a contract, a consumer cannot know to what he or she consents to. If given, such a consent cannot be "informed" nor "transparency" achieved.

Furthermore no company should be allowed to use undefined or vague terms and conditions in such a contract nor change them at will without entering into a new negotiation with each user concerned. This would be inequitable. This means that most, if not all, so-called Privacy Policies put forth by organizations do not qualify as valid "personal data contract" even if they were to receive the consumer's explicit consent.

inequitable bundling of "personal data contracts":

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

I recommend bundling be considered illegal as it is inequitable.

The inequity resides in the impossibility for an ordinary consumer to give a "free consent" as this consent, although not needed to fulfill a certain transaction desired by the consumer, is turned into a necessary condition by the company to accept the transaction. The consumer is in no position to negotiate and normal competition has proved unable to provide credible alternatives.

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 its assumed benefits, consumers should be expected to freely accept the corresponding "personal data contract".

Again companies cannot argue my recommendation would create unnecessary burdens. They already know how to package their consumer goods and services in a clear, concise, convincing manner. They would have only 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 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 without any credible alternative.

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

Suppose for instance that a company offers "free access" to a 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 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 my 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 requested 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 does not engage in an inequitable barter.

link with Fair Information Practice Principles (FIPPs):

The Federal Trade Commission (FTC) has received the mission to insure contracts with consumers are free from deceptive clauses. It would therefore be natural for the FTC to enforce my recommendation and it arguably needs no additional mandate to start acting upon it. For clarity, it should publicly document any current practice which violates equity and rule it out after an appropriate transition period.

On the other hand the DoC task force is correct to stress the power of safe harbor mechanisms to help establish practical models and thus bring about "consistency, uniformity, and predictability" to the industry.

I therefore recommend FIPPs, i.e. "Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, Accountability and Auditing", be used as the basis for Fair Personal Data Contract Models. This will implement the first recommendation of the DoC task force, i.e. to "Enhance Consumer Trust Online Through Recognition of Revitalized Fair Information Practice Principles". I further suggest such equitable contract models be developed by industry bodies and consumer advocates alike and submitted to the FTC to receive its "safe harbor" approval as to their being equitable. This will implement the second recommendation of the DoC task force, i.e. to "Encourage the development of voluntary, enforceable privacy codes of conduct in specific industries through [...] collaborative efforts"

Organizations should naturally remain free to draw their own contracts, although the use of any practice officially deemed inequitable by the FTC or by any subsequent case law would invalidate such contracts at the onset. Ultimately the consumers would be the judge as they accept or reject the unbundled contracts put to them while competition unleashed on this newly freed market encourages business innovation catering to their interests.

- (b) forbid the use of irrelevant criteria in targeted advertising with the help of a safe harbor mechanism

One of the FIPPs is "Data Minimization", meaning to "only collect the [personal information] that is directly relevant and necessary to accomplish the specified purpose(s)".

I 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 unknowingly disclose their profiles satisfy this criteria.

how not to control targeted advertising:

Forbidding the use of so-called sensitive criteria in targeted advertising is easy to do but 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.
A charitable organization for AIDS prevention should similarly be allowed to target users based on their sexual preferences.

- the list of sensitive criteria is potentially very large.

In the rental market or for job recruiting, the candidate's current address can enable covert 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 certain types of comic books, correlating this criteria with other information available in this user's profile can be enough to ascertain the user is less than 12 years old. This criteria can then be used to subrepticiously target protected minors with offers in contradiction with the code of conduct ostensibly followed by the company.

the principle of legitimate targeted advertising:

Principle, practice and enforcement are the three aspects to a sound control of targeted advertising.

In line with the principle of "data minimization", I recommend targeted advertising based on irrelevant criteria be forbidden.

practical definition of criteria irrelevancy:

I 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, I recommend to set up a Federal Data Authority authorized to issue safe harbor decisions on request.

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 DoC task force wishes to encourage to produce "voluntary, enforceable codes of conduct in specific industries", 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 Federal 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.

economic considerations:

The company whose algorithm targets the profiles, by design, has direct operational access to all the elements to be audited. It can inexpensively record this information for auditing purposes given today's low cost of digital storage.

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 do 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.

link with the Privacy Policy Office:

The DoC task force suggests the creation of a Privacy Policy Office (PPO) "focus[ed] exclusively on commercial data privacy" in the context of a safe harbor mechanism. I therefore suggest the PPO be considered a likely implementation of the Federal Data Authority recommended above.

- (c) require organizations affected by security breaches to compensate the consumers concerned

In its fourth recommendation, the DoC task force proposes to "Ensure Nationally Consistent Security Breach Notification Rules" subject to enforcement by "the FTC and individual States".

I 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:

- receivers of consumer data normally bear no marginal cost as a result of a data breach, even if notification is made mandatory, as it can be implemented through cheap 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.
- it is rarely possible to directly link a specific data breach to a specific wrong suffered by a consumer.

real life examples:

Contrast this situation with the special case of credit card companies.

Because I use my credit card for many online transactions, I have been the victim of multiple credit card id thefts. As a result, the average duration of my card is six months, instead of its nominal two years. Recently my card had to be replaced less than three weeks after having been issued.

Due to legal obligations and commercial practice, I bear no cost besides the inconvenience of having to change my card. On the contrary the card operator and associated parties risk significant liabilities if my 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 significant 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.

Further consider the case of the airline industry.

When an airline denies boarding to a passenger with a valid ticket due to overbooking, the current practice is to offer the passenger an appropriate compensation, be it a free ticket, a free hotel night or even cash, for the inconvenience.

By compensating the individual concerned, the airline amends its failure to fulfill the contract it hd made with the bumped off passenger.

Notice that the airline could argue the booking was a simple promise on its part to make its best efforts to find a seat on a particular flight. In this perspective consumers would not be able to show any specific wrong and not be entitled to any damage. It is obvious however that holding flight reservations to be no more than promises would seriously "undermine consumer trust" in the industry and severely impede commerce.

personal data breaches:

These real life examples show that, whenever companies bear a cost due to data breaches, they invest in their early detection and prevention and that, whenever companies want to keep the trust of consumers, they compensate the consumers they failed in some way.

Therefore I recommend to establish a schedule of minimum mandatory payments by the organization at which the data breach occurred to the consumers concerned, representing the compensation due to consumers for the failure of the organization to keep the consumer data confidential, so as to "maintain consumer trust [which] is vital to the success of the digital economy".

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.

By creating 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. The creation of a criminal liability as suggested below should be sufficient to prevent most organizations from taking this additional risk.

compensation schedule:

The principle of minimum mandatory payment makes for a simple, national, consistent rule, bringing predictability to the industry. On the other hand the DoC task force correctly mentions "the numerous merits" of a sectoral approach in introducing much needed flexibility. The minimum payment could for instance depend on the industry to which belongs the organization victim of a data breach.

In the same spirit, I further recommend this payment be made proportional to the means of the organization, its business model and the risks incurred by the consumers.

I further suggest to classify organizations in receipt of consumer data 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) above:

- holding personal data solely for the purpose of fulfilling an offer or a service, no "personal data contract" needed
- re-using personal data held for fulfilling an offer or a service per 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 as consumers are confident 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.

This market mechanism would effectively rebalance innovation which otherwise, as shown in part II, ignores and therefore increases consumer risk.

Section (b) above downplays the need to forbid the use of so-called sensitive criteria in targeted advertising. However the sensitivity of consumer profile elements involved in a data breach should be a third factor in establishing the compensation schedule, reflecting the risks run by affected consumers.

link with Privacy Impact Assessment (PIAs)

The DoC task force devotes a great deal of attention to "Privacy Impact Assessments" and asks several questions about them. It is expected that such documents would indeed become the natural tool to inform the negotiations of organizations with their insurers relative to the risk of security data breach compensation.

It is likely that the insurance industry would quickly develop and share appropriate methodologies and schedules as common in other risk-based assessments.

- (d) make the willfull ignorance of these three civil contractual obligations a federal criminal offence

The DoC mentions the existence of criminal sanctions in conjunction with the Electronic Communication Privacy Act. While it might be beyond the scope of the DoC to discuss how to update criminal statutes, it is logical to open this discussion to implement the "strong enforcement" needed to "provide effective commercial data privacy protection".

The previous sections have recommended three obligations be imposed on organizations holding or processing personal data:

(a) - drawing an explicit "personal data contract" with consumers
- eliminating all inequitable clauses in such contracts as created through bundling

(b) - eliminating all irrelevant criteria for targeted advertisements

(c) - reporting all data breaches and paying a civil penalty to each user concerned

I recommend that any attempt to knowingly bypass one or more of these obligations in a systematic or reckless manner be made a criminal offense. I 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.

- Part V - Responses to DoC Questions for Further Discussion

(1) Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or other means, to address how current privacy law is enforced?

Consistent with section IV-a above, one should distinguish three levels:
- legislative, as far as contract law and enforcement against deceptive practices are concerned
- regulatory, in documenting specific practices as instances of forbidden deception
- cooperative, when drawing specific Fair Personal Data Contract Models

The latter recasts comprehensive FIPPs as "personal data contracts" whose equitable character could be verified by the Federal Trade Commission (FTC) according to a Safe Harbour mechanism.

(2) How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?

Consistent with the previous answer to question (1), enforcement should follow the legal framework:
- injured parties could sue in court against deceptive practices
- the FTC could fine organizations for violating Section 5 of the FTC Act or rules forbidding specific practices

The role of non-governmental entities should remain indirect:
- either as publishers of Fair Personal Data Contract Models approved by the FTC under a Safe Harbor mechanism
- or as watchdogs representing consumers and pursuing redress in court based on evidence of deceptive practices

Giving a non-governmental entity explicit power of enforcements over individual agents would run contrary to antitrust statutes as curtailing the freedom of market participants to innovate and compete on the terms of "personal data contracts" while staying within the law. However see the answer to question (19) below for another perspective.
Consistent with section IV-d above, willfull ignorance of corresponding civil responsibilities should be made a federal criminal offense.

(3) As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rule?

The FTC may not need a new mandate beyond the FTC Act to enforce contractual law against deceptive practices and to issue new rules fordidding specific practices. However a new legislative mandate against bundling "personal data contracts" with a transaction whose fulfillment does not require the corresponding transfer of consumer data rights, as recommended in section IV-a above, may be valuable in making the current authority of the FTC more explicit.
On the other hand a new statute might be necessary to grant the FTC power to act as a Safe Harbor for Fair Personal Data Contract Models submitted to its approval.
The overall effect should be to give the FTC clear authority to forbid what is inequitable while leaving the free market participants complete freedom to invent new ways of doing business and giving them a simple means to voluntarily seek and obtain prior assurance from the regulator.

(4) Should baseline commercial data privacy legislation include a private right of action?

Adopting the Safe Harbor mechanism described in section IV-a above would establish an efficient balance between:
- the right for consumers and their advocates to seek redress in court
- the need for organizations to be protected from frivolous lawsuits

(5) What is the best way of promoting transparency so as to promote informed choices?

Based as detailed in section IV-a above on free and informed consent given by consumers to equitable "personal data contracts" beyond the fulfillment of ordinary commercial transactions, a free market would naturally encourage competition among organizations interested in acquiring further rights to consumer information. Forbidden to use deceptive practices, free to innovate and obtain protection from frivolous lawsuits, motivated to get consumers to sign "data contracts", the competitors would naturally promote transparency about their "data offers". Consumer Reports and the like would further increase this transparency by doing comparative studies as they do in the course of ordinary commerce.

Transparency also calls for forbidding the use of hidden, irrelevant criteria in targeted advertising as detailed in section IV-b above, such as, albeit as an academic illustration, targeting car ads to consumers based on religious practice or sexual preference. An efficient implementation of this specific requirement calls for a different Safe Harbor mechanism specifically devoted to targeted advertising and which could be assumed by the Privacy Policy Office (PPO) proposed by the task force.

(6) What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

As detailed in section IV-c above, requiring organizations affected by security breaches to compensate the consumers concerned is a powerful incentive. Compelled to insure against a direct, measurable financial risk, organizations would invest in security measures and encourage any innovation which promises to lower their premium. Meanwhile insurance companies would develop and share appropriate methodologies and schedules, as common for other risk-based assessments.
Similarly as organizations seek to secure coverage against the liabilities relative to deceptive contractual practices and irrelevant criteria based targeted advertising, as detailed in sections IV-a and IV-b above, insurance companies would prod them to seek the benefits of corresponding safe harbor mechanisms.
Safe harbor mechanisms are typically financed by fees charged to the applicants, who retain complete freedom to act in their best interests. Such incentives therefore would neither burden the federal budget nor dictate the "right way" in which to do business.

(7) Who should define [the] elements of a meaningful PIA in the commercial context

As explained in the previous answer, the insurance industry would be ideally equipped for this task.

(11) What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves data from multiple sources being presented through a single user interface?

The two related issues are to manage the technical integration of data from multiple sources and to divvy up potential liabilities in case of a leak. The author has contributed a novel solution to this problem as detailed in US Patent Application no 2009/0076914.

The basic idea is to equip the point of contact used by the consumer, e.g. a personal computer or smart phone, with a so-called confidential, interactive environment. The latter can receive and store personal data. External agents downloaded to it can locally interact with this personal data but can report no information back to the organizations which send them, nor to any other third party. In other words a confidential, interactive environment is a one-way valve which enables the consumer to have total control over his or her data while reaping all the benefits of personalized interactions.

The principle of the solution is to let such a confidential environment aggregate a profile from all the sources offering to feed it with personal information as they are interact with the consumer. Thus information sources do not need to engage in profile aggregation themselves and hence incur no liabilities. Yet the environment tracks the later reuse of each item they contribute and credits them for it. Because the consumer has access to his or her own profile at all times, this process is totally transparent and any erroneous information can be edited or at least viewed and contested as appropriate. Information sources need not concern themselves with presenting personal data to the consumer as they all share the single interface of the environment, acting as profile manager.

Such a solution can deliver practical personalized services, e.g. targeted advertising. Each targetable ad is downloaded within the local confidential environment where it interacts with the consumer profile to find whether it is on target or not. The consumer device needs therefore to receive the unfiltered flow of all targetable ads but such a flow consumes little bandwidth and power as targeting instructions can be efficiently encoded and processed while ad contents can be fetched just in time when an ad found to be on target is to be displayed.

More details, addressing legitimate concerns raised by such a brief synopsis, are provided in the patent application. The main point to be remembered is that such an innovative approach to eprivacy clearly separates four complementary roles:

- information furnishing, with no liability relative to aggregating or re-using consumer personal data
- profile aggregation by a software under each profile owner's sole responsibility
- service personalization, with no liability relative to holding consumer personal data
- service auditing, performed on the local journal maintained by the environment

In this context:

- "personal data contracts" as recommended in section IV-a above become very simple to write, explain and sell
- participating organizations shed almost all liabilities related to consumer personal data
- enforcement of recommendations of sections IV-a, b and c is made easy

In particular a data breach involving a specific consumer can only occur via the mishandling of a personal device and personal software whose integrity is under this consumer's sole control and responsibility.

(12) Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?

The solution outlined in the answer to question (11) above only requires a minimum user interface option to enable the consumer to access his or her local profile.
However running the necessary confidential, interactive environment requires underlying security features at least equivalent to what is provided today by the support of a Sun Java Virtual Machine with its Java security library and the abilitity to handle so-called trusted Java applets, which may or may not be available on all personal devices.

(13) Are purpose specifications a necessary or important method for protecting commercial privacy?

It is not possible to draw an equitable "personal data contracts" as recommended in section IV-a above without specifying to what use the personal data will be put no more than to draw a legal employment contract without specifying the nature of the job. Slavery has been outlawed. Data slavery must be too.

(16) What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

As detailed in section IV-a, subjecting all collection and use of consumer data to explicit and equitable contracts would compel all organizations concerned to sell their data-related offer on a free market. The motivation to sell together with market competition should quickly provide the necessary encouragement.

(18) How can purpose specifications and use limitations be changed to meet changing circumstances?

A change in a contractual relationship requires the assent of both parties. However a consumer who has already been sold a "personal data contract" by an organization is most likely to accept any change which is obviously to a mutual benefit. On the other hand an organization which asks for a change which is not in favor of the consumer can hardly expect his or her consent and should not be allowed to dispense with it.

(19) Who should be responsible for demonstrating that a private sector organization’s data use is consistent with its obligations? What steps should be taken if inconsistencies are found?

From a traditional perspective, an organization should not have to prove it is innocent. On the contrary the burden should be on the consumer, the consumer advocates, the companies charged with auditing its practices, the FTC itself to prove this organization has been delinquent.
On the other hand it is recommended in section IV-d above that a willfull ignorance of the civil responsibilities incumbent on an organization be made a federal criminal offense and it might be appropriate to have the CEO or the CIO of public corporations above a certain size annually certify the compliance of their organizations under their own signature.
From a more innovative perspective, the adoption of a formal system which controls the use made of consumer data can provide an organization with a simple, inexpensive and advantageous way to provide proof positive, for instance to get lower insurance premiums, discourage frivolous lawsuits and increase consumers' trust.

For an example of such a formal system, see the work of Winnie Cheng, whose PhD dissertation "Information Flow For Secure Distributed Applications", 2009, is available from MIT at:
http://hdl.handle.net/1721.1/46700

The so-called confidential, interactive environment developed by the author and briefly presented in the answer to question (11) above also provide such a mechanism.
All personal data use by an organization under this approach is mediated by an external agent, which can be implemented in one of three ways.
- as a program which can be audited, certified and sealed under the signature of a bonded third party such as an accounting firm, thereby preventing the organization from modifying the behavior of the agent once it has received the approval of the third party.
- as a parametrizable macro driving a macro-agent which has been certified and sealed as indicated above and is pre-packaged with the environment itself. Being simpler, macros can be inspected on sight and their successive versions archived in a secure and auditable way, minimizing the cost for the publisher of maintaining a positive proof over time.
- as a set of parameters configuring a parametrizable macro as indicated above. Because by construction of the macro, no parameter set can modify its behavior in an improper way, using a parameter set is in itself proof positive for the organization.

The existence of such formal systems offers an opportunity to revisit the answer given to question (2) above.
Assume for example that a non-governmental association develops a macro for which it receives a Safe Harbor approval from the FTC or the PPO as the case may be, as detailed in section IV. Assume further this association allows all its members to configure this macro at their own convenience. The association can be said to enforce a form of "personal data contract" over all the members which freely choose to configure the macro of the association, since the formal system ensures they respect the contract implemented by the macro.

(20) Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?

As developed in the answer to question (19) above, formal systems can help consumers to make such a verification. However it remains more intuitive for a consumer to check the content of his or her own profile as provided for instance by the so-called confidential, interactive environment developed by the author and briefly presented in answer to question (11). When it comes to prove an external agent uses the consumer profile as claimed, the consumer is bound to rely on third parties. While some level of verification can be done locally by using a special external agent from a trusted party to check the audit trail recorded by the environment, consumers will depend more on the prior code inspection performed on the external agent by third parties which then put their own signature on it for consumers to know. This is a certification, not a verification.

(23) What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?

As detailed in section IV, companies would have a natural interest in seeking the protection either of a Safe Harbor or an insurance contract. If the corresponding Safe Harbors fees and insurance premiums are decreased whenever the companies adopt the type of formal systems described in the answer to question (19) above, this should be incentive enough.

(25) How can the Commerce Department best encourage the discussion and development of technologies such as ''Do Not Track''?

The author has explained elsewhere that a "Do Not Track" approach will not be efficient as it is very difficult to enforce. See my "comments relative to the FTC November '07 workshop on Ehavioral Advertising: Tracking, Targeting, Technology" at http://www.ftc.gov/os/comments/behavioraladvertising/071112eprio.pdf
As behavioral advertising is a prime example of a use of consumer data requiring the consumer to accept one or several "personal data contracts", as detailed in section IV-a, it is far more efficient to reverse the mechanism and develop "Do Track" registries allowing quicker audits of the practices of the contracting parties.
The author further recommends the organizations presenting targeted ads on their pages be required to give consumers free, instant, online access to their profiles. This measure, which promotes transparency, is easy to enforce as explained in section IV-b above. For an implementation, see the solution developed by the author and briefly presented in answer to question (11).

On the other hand, as detailed in section IV-d, organizations caught practicing illegal tracking should be subjected to federal criminal prosecution, much in the same way as spammers. While tracking spammers, who can operate from foreign or stolen resources, is notoriously difficult, tracking illegal tracking is made easier by its reliance on the organizations whose pages present the targeted ads. Such organizations are known to the consumers and need to keep their trust. It would be an unacceptable risk for them to be found responsible for illegal tracking, as proposed in section IV-b above. Therefore the more powerful ones would audit the whole chain of parties providing their ads. The less powerful ones could then rely on the parties approved by the more powerful ones.

(29) What should be the scope of FTC rulemaking authority?

As detailed in section IV-a above, the FTC should have two roles, one based on section 5 of the FTC Act against deceptive practices, perhaps strengthened per the answer to question (3) above, the second to set up a Safe Harbor mechanism relative to Fair Personal Data Contract Models, an enhanced form of FIPPs.

(31) Should non-governmental entities supplement FTC enforcement of voluntary codes?

see the answer to question (6) above, about the role of insurers.
see the answer to question (19) above, about the role of industry associations.

(32) At what point in the development and of a voluntary, enforceable code of conduct should the FTC review it for approval?

As detailed in section IV-a above, this should be part of a Safe Harbor mechanism.

(36) Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matter, leaving states free to regulate emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

For consistency, preemption provisions should copy what is determined in section 5 of the FTC Act relative to deceptive contractual practices.