ePrio

1/31/2011

Federal Trade Commission,
Bureau of Consumer Protection
Room H-470
600 Pennsylvania Av, N.W.
Washington, D.C., 20580

Subject: Protecting Consumer Privacy in a Era of Rapid Change

"Policy making on privacy issues present significant challenges". By analyzing these challenges, developing a new framework in response and soliciting comments from all interested parties, the Federal Trade Commission faithfully discharges its duty to protect consumers on the market place. Likewise, given my personal and professional experience at the intersection of innovation and privacy, I cannot ignore my duty to answer the call of the FTC.

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 developed 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 objectives with which the FTC has structured its proposals:

- (1) covering personal data collection and use even if offline or not strictly personally identifiable
- (2) creating the necessary conditions for companies to
  invest in consumer privacy, simplify consumer choice and increase transparency

The FTC report further provides a rich and insightful methodology with which to reach these objectives. In particular by its repeated mention of section 5 of the FTC Act, it clearly points out that "unfair or deceptive acts or practices in or affecting commerce" may well be the lens through which to analyze the present state of consumer privacy.

However the FTC report may reflect a bias according to which eprivacy and industry are in conflict and some acceptable trade-off must therefore be found, "to protect consumer privacy interests effectively, while also encouraging the development of innovative new products and services that consumers want". Such a position can only stem from a misunderstanding of the nature of free markets. To protect consumers is also to fight for true market freedom, a good for industry as a whole, an evil for self-interested competitors.

In the attachment below, I volunteer answers for most of the 64 questions put out for comment by the FTC, giving them greater clarity and force in the context of my own recommendations on how to resolve the apparent conflict between eprivacy and industry and to free innovation in the process, 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 willful 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 Federal Trade Commission on Protecting Consumer Privacy

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. Implicitly accepting this judgment, the FTC staff defends the right of the FTC to protect eprivacy "despite the acknowledgements of [the] benefits [of free flows]".

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, "unfair or deceptive acts and practices" in the words of the FTC Act.

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 person 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, and hence for industry as a whole. 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 industry 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 laziness, 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 solicit 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 "laziness" 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, along the FTC methodology to "simplify consumer choice".

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 information for its own, "first-party" marketing, it can easily solicit the consumer consent for free as the current custom prevails. 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 burdenless given today's technology.

If an organization wants to re-purpose this 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 first approach used by the FTC to protect consumer privacy is called "the notice-and-choice model". It is designed "so that consumers can make informed choices" leading to "meaningful, informed consents". The following recommends how to implement it in a manner both forceful and enforceable.

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. 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. In no position to negotiate, the consumer has no choice 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 choose 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 competitiveness 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 FTC stated objectives:

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.

My recommendation does not only give the FTC a robust and enforceable implementation of its "notice-and-choice" model. By compelling organizations and consumers alike to acknowledge a "personal data contract" with an "affirmative, express consent", it also promotes greater transparency as it tears the false veil of pretend anonymization which organizations invoke to hide inequitable practices and deny consumers access to their personal profiles. In particular organizations with no direct contact with consumers whose information they store and use would have to sell the relevant "personal data contracts" through retailers in contact with consumers, e.g. the companies who feed them information about their own consumers.

On the other hand, I further suggest the FTC help ethical organizations by setting up a safe harbor mechanism whose mission would be to approve as equitable "Fair Personal Data Contract Models" developed and submitted by industry bodies and consumer advocates alike.

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

As promoted by the FTC, "Privacy by Design" includes "collecting only the data needed for a specific business purpose".

I believe that this principle should be 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. Enabling its users by design to engage in hidden and unnecessary data collection, it should be ruled out explicitly as an "unfair and deceptive practice".

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 subreptitiously 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 by some competitors in the hands of a regulatory authority but at the same time wide initiative is given to intermediate bodies representing the industry. It shows how self-regulation can, when properly channeled, 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.

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

The FTC complements its "notice-and-choice" approach by what it calls an "harm-based model" to account for the risks involuntarily generated by eprivacy related activities.

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, a challenge duly recognized by the FTC as "consumers may not know when they have suffered harm", let alone trace it down to the responsible party in a manner able to convince a jury.

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 had 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 due 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 and ensure the growth 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. Instead of a "harm-based model", the FTC may want to speak of a "failure of duty model". Indeed the FTC already considers "the idea that companies should provide reasonable security for customer and employee data is well settled". My proposal is simply to judge this duty on the basis of results rather than on costs.

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. It does not mean all data breach related payments must be equal as long as the compensation schedule drawn up by the FTC reflects objective factors published ahead of time.

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

Organizations in receipt of consumer data can be classified 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.

The risk run by affected consumers is the third element recommended in setting up the compensation schedule, taking into account such subfactors as the use of encryption and the sensitivity of consumer profile elements, thereby balancing section (b) above, which downplays the need to forbid the use of so-called sensitive criteria in targeted advertising.

- (d) <u>make the willful ignorance of these three civil contractual obligations a federal criminal offence</u>

While it might be beyond the scope of the FTC to update criminal statutes, it is logical to open a discussion on the need to back violations to the "notice-and-choice" and "harm-based" models by the threat of federal criminal prosecution beyond the current power of the FTC.

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 FTC Questions for Comments

Scope

1- Are there practical considerations that support excluding certain types of companies or businesses from the framework - for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?

No. Consistent with section IV above, no organization should be allowed to engage in "unfair or deceptive acts and practices" or otherwise escape its civil responsibilities under the excuse it is only "a little bit unfair".
The implementation of the "notice-and-choice" model recommended by section IV-a imposes no practical burden on organizations engaged in ordinary transactions or "first party" marketing. To store or use consumer data beyond those activities is an informed choice which represents the free consent of the organization to the associated responsibilities.
On the other hand the implementation of the "harm-based" model recommended by section IV-c does recognize the need to adjust the compensation due to consumers in case of a data breach according to objective factors which specifically include the number of consumer profiles held and the sensitiveness of this profile data.

2- Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?

Yes. The FTC is right to acknowledge it is no longer possible to ignore non "personally identifiable information". No organization would store or use personal consumer data if it did not profit from it either to address its target, i.e. "a specific consumer, computer, or other device" or because it profiles a genuine target even though addressability has been lost to anonymization.
When addressability is maintained, identification is assured, even if indirectly. When anonymization destroys addressability, the associated data still represents :

- from the "notice-and-choice" model, the product of the target activity
  and its procurement should not escape from the obligations imposed by a free and fair market
- from the "harm-based" model, a risk of later re-identification
  given the permanent potential for positive correlations with other sources of information

Organizations engaged in market research may legitimately claim they, themselves, have lost the ability to make the re-identification of their anonymized data and therefore can send neither data breach notification nor its associated compensation as recommended in section IV-c. However the full implementation of section IV-a above would precisely compel them to enter into a contract with the corresponding consumers so that their excuse could not hold.
This is not to say that data anonymization has no merit. By contracting a third party to manage the consumer relationship for them at arm-length, a practice similar to blind trials in healthcare, an organization could for example lower the insurance premium paid to cover its liabilities in case of a data breach at either facility as recommended in section IV-c.

3- How should the framework apply to data that, while not currently considered "linkable," may become so in the future?

Research by Arvind Narayanan and Professor Vitaly Shmatikov from the University of Texas at Austin has demonstrated how seemingly anonymized personal data can be re-identified. A science-based approach is therefore to assume all profiles of genuine consumers are "linkable" at some point in time even when anonymized.
As explained in the answer to question 2 above, the case of anonymized data does not present any difficulty as long as "personal data contracts" are made mandatory as part of the framework. This would only extend common practices in market research, the main user of anonymized data, which pays a compensation when hiring consumers to participate in focus groups or audience measurement panels.
Compensating for the use of anonymized data is bound to limit the scale at which market research samples consumers. This issue however has long been addressed by scientific market research, e.g. in political polls which actually use a tiny sample of all voters.

6- What technical measures exist to “anonymize” data and are any industry norms emerging in this area?

Data anonymization on genuine profiles cannot be achieved on a consistent, provable basis as explained in the answer to question 3 above.
Techniques exist however which modify each profile so that it no longer represents a specific individual while preserving the desirable statistical properties of the sample. For an example, see the work of Professor Xiaobai Li at University of Massachusetts at Lowell.

On the other hand, when the goal is to target a profile according to specific criteria, e.g. for targeted advertising, or to extract a specific statistic for a certain population, e.g. for market research, the author has developed an original, contrarian approach which provides a total guarantee of personal privacy as detailed in US Patent no 6,092,197 and US Patent Applications no 2006/0053279 and 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 elicit 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 simply to reverse the flow of information. Instead of sending their profile to the organization, the consumers download a suitable external agent from the organization. The role of this agent is, as need be, to prompt a consumer to declare his or her profile to their confidential environment and to

- either verify the profile is on target and deliver an appropriate sales pitch or ad to the consumer
- or ask the consumer to explicitly agree to increment counters centrally set up to tally up the statistics, through a proxy for better protection

As a result, the organization has no need, and indeed cannot, access the consumers' profiles, which fulfills the same function as anonymization, without either the risk of re-identification or the distortions brought about to defeat it.

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

Incorporate substantive privacy protections

7- Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?

There is a need to distinguish among the protections of Section V(B)(1) of the report between those pertaining to the "notice-and-choice" model and those pertaining to the "harm-based" model.
The latter are almost unlimited as they depend both on innovation in terms of security and privacy and on ever evolving threats. The lead in terms of prescribing appropriate protection according to a cost/benefits analysis should be taken by the insurance industry via the premiums charged to insure against liabilities in case of a data breach, as recommended in section IV-c. However the FTC should, on an ongoing basis, recognize practices which have become commonly known to lower consumer risk, such as encryption, to determine the data breach compensation due to consumers.
Within the scope of the "notice-and-choice" model, Section V(B)(1) of the report establishes the principle of data minimization relative to the business purpose. As suggested in section IV-a, a proper implementation calls for the FTC to rule specific practices to be inequitable in terms of "personal data contracts". This might include:

- asking consumers to give away obviously more data than is necessary for the stated purpose
- declaring purposes so vague or open ended as to justify unlimited data collection.

From this perspective, a cost/benefit analysis does not apply. On the other hand it is also recommended the FTC sets up a safe harbor mechanism so that, while remaining the ultimate judge, it effectively gives the industry the lead for innovation in terms of better contracts, including data minimization.
Targeted advertising should be considered an important case of the data minimization principle. As explained in section IV-b, the use of irrelevant targeting criteria should be forbidden, and a special safe harbor mechanism created.

8- Should the concept of “specific business purpose” or “need” be defined further and, if so, how?

I recommend the following definition: "a specific business purpose" is the creation of a value to be recognized

- either externally by selling it as part of a specific offer to another party, which may be the consumer him or herself
- or internally by decreasing the cost/benefit ratio of a specific internal business process

If the FTC were to be more specific on either this definition or its application in ruling against data minimization, it would stifle industry innovation. Whether a particular case is equitable or not should be judged either after the fact, through the judiciary system, or before the fact as recommended in sections IV-a and b, via a safe harbor mechanism.
On the other hand it is also believed that genuine competition on a free market would push organizations proposing "personal data contracts" to demand less data of consumers as a selling point. Similarly the need to pay insurance premiums for data breach liability as recommended in section IV-c would keep organizations from needless data acquisition.

9- Is there a way to prescribe a reasonable retention period?

This is a special case of questions 7 and 8. There should be no attempt by the FTC to provide positive prescriptions but it should retain both the right to prosecute obvious abuses as inequitable or pre-approve reasonable practices via a safe harbor mechanism.
Data retention periods are in fact related to:

- the time necessary to fulfill an ordinary transaction and any associated legal obligation
- the duration of a "personal data contract"
- the span of time covered by a safe harbor approval
- the speed at which innovation and threats evolve

Consistent with the recommendations of section IV-a, the FTC could

- write rules precluding clearly inequitable, such as:
  - retaining data past transaction fulfillment and legal obligations without a "personal data contract"
  - writing clauses in a "personal data contract" extending data retention beyond the duration of the contract
  - omitting termination clauses in a "personal data contract" allowing the consumer to break the contract,
  - imposing unreasonably onerous termination clauses on consumers wishing to break the contract,
    e.g., to pay punitive penalties or to go offline even though the contract was approved online,
  - extending "first party" marketing beyond two years after a consumer left checked a pre-checked opt-out cell
- require any safe harbor approval to lapse, subject to renewal, after a time commensurate with the speed of innovation

Within this context, it would be interesting to find out from academic experts for how long a search engine company really need to keep search logs from single IP's, whether anonymized or not, for defending itself against hackers, knowing a search transaction can be timed out in a matter of minutes without losing response speed.

10- Should the retention period depend upon the type or the sensitivity of the data at issue?

Not directly. As explained in section IV-b, data sensitivity should normally be justified by the "specific business purpose", independently of the retention period.
However it is expected that increased data sensitivity calls for increased consumer compensation as specified by "personal data contracts", according to section IV-a, and increased data breach compensations and insurance premiums for data breach liability, as recommended in section IV-c

11- How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?

There should be no particular provisions for legacy systems, assuming all rules include a reasonable transition period, for example a two year delay. Consistent with the recommendations of section IV, this delay will be needed to set up new systems to manage the "personal data contracts", an important task with little or no overlap with current data systems.

12- When it is not feasible to update legacy data systems, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems?

According to section IV above, there is a need to distinguish between the contractual aspect, independent of the legacy systems in almost all cases, and the data risk, which will be better managed by the insurance industry.
The data breach compensation schedule, to be set up by the FTC, should be independent of legacy systems so as to avoid dictating the rate of innovation adoption.

Maintain comprehensive data management procedures

14- How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies

According to section IV above, the two basic incentives will be the business imperatives to:

- compete on a free market for "personal data contracts"
- lower insurance premiums for data breach compensations

In this manner the FTC does not need to dictate the any specific technical innovation.

15- What roles should different industry participants - e.g., browser vendors, website operators, advertising companies - play in addressing privacy concerns with more effective technologies for consumer control?

Once privacy-enhancing innovation is made financially attractive by the mechanisms described in the answer to question 14 above, many different industry participants will help bring this innovation to market.
For instance today's browsers are strongly biased to make privacy invasion far more user-friendly than privacy preservation:

- defaulting cookie management for lesser privacy
- imposing no demand to warn users on pages which require cookie approval
- leaving many security holes for virus and other malware to slip in unnoticed
- but slapping threatening warnings on security conscious applications, such as trusted java applets

If organizations were made to benefit from enhancing consumer privacy, it is expected that browsers would be quickly upgraded to meet their needs and integrate privacy-enhancing innovation in the most seamless way into the user experience.

Companies should simplify consumer choice

Commonly accepted practices

16- Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

The methodology behind "commonly accepted practices" is excellent and has also been adopted in sections III and IV above.
Comments on "first party marketing" are differed until questions 18 to 22.
However the category "internal operations" should be dropped from the list as a needless and capital loophole.

First the category is almost universal. Most consumer oriented organizations constantly try to upgrade their internal operations, obviously with the consumer in mind.
Second consumers may not know. Such organizations use consumer data in ways not as immediately transparent to the consumers as the fulfillment of a desirable transaction or the receipt of a marketing message.
Third consumers may not benefit at all. Despite any declaration to the contrary, the organization is designed to first serve those who control it, be they shareholders, members or trustees, not the consumers. It is therefore not assured that the consumer will benefit from a decrease in the cost/benefit ratio of an organizational process.

On the other hand, consumer data can be used internally by organizations to create new value to

- consumers, e.g. in the form of an automatic recommendation such as delivered by Amazon or Netflix
- the organization itself, e.g. in the form of market research to develop new products and services

In both cases, as recommended in section IV-a above, it is possible to formulate a "personal data contract" spelling out the data supplied by the consumer, its limited purpose and the compensation due to the consumer. It is further equitable to require the free, explicit assent of each consumer to this contract.

When the value is proposed to the consumer as part of a new offer such as recommendations or other personalized services, it is a new genuine transaction which requires the data asked for, and as such falls back under the category "product and service fulfillment", but with its own separate confirmation process.
Otherwise the compensation proposed should have a clear cash value, even if offered in kind, for example a free ticket also available for a price. This is a case of equitable bartering as explained in section IV-a.
Nothing of course prevents an organization to offer no compensation at all as long as the consumer remains free to accept or not at no penalty to him or her. To reuse the example of the FTC report in market research, I am not denied food at a restaurant if I decline to fill up their satisfaction survey. On the other hand market research pays consumers to participate in focus groups.
As in real markets, the low cost to the consumer to produce the data, such as when he or she navigates the site of the organization, should not be reason enough to deny this consumer a compensation against his or her will, no more than the zero cost of copying a digital file prevents a music record company from requesting the consumer pay for a digitized song. The contrary is an act of piracy in either case.

17- Are there practices that should be considered "commonly accepted" in some business contexts but not in others?.

No. The list set forth in Section V(C)(1) of the report should be understood as exhaustive, with the category "internal operations" struck out and the category "first party marketing" amended per the answer to question 18 below, independently of the business context.

18- What types of first-party marketing should be considered "commonly accepted practices"?

By definition "first-party" marketing should be limited to the permission given by a consumer to an organization in one click on a cell either checked (opt-out) or unchecked (opt-in) next to the confirmation of a transaction with this organization and clearly labeled as authorizing this organization to send its own generic marketing solicitations to the consumer in the future at no cost to this consumer.
Any other interpretation, such as making it more difficult for a consumer to opt-out, or enlarging the business purpose to more than sending generic mail to the consumer at no cost to this consumer or for more than what is offered by this organization should be ruled out as inequitable unless explicitly approved under an appropriate "personal data contract".

19- Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?

As explained in section IV-b above and the answer to question 10 above, data sensitivity per se is not a direct factor in determining equity. It makes perfect sense for a charitable organization fighting for AIDS prevention to target current correspondents based on their sexual preference and drug use. It still makes sense for Amazon to target users who have bought books concerning religion on the basis of their religious practice, inferred or acknowledged.
However sending targeted mail should be considered outside of "first-party" marketing as it involves another business purpose beyond addressing generic mail to a consumer and requires retaining a profile whose depth can be considerable. This should be explicitly approved by the consumer within an appropriate "personal data contract".

20- Should first-party marketing be limited to the context in which the data is collected from the consumer?

No, in the sense that the address collected from the consumer can be reused outside of the context in which it was collected, subject to the restriction noted in the answer to question 21-b.
Yes, in the sense that the organization who is responsible for the collection context, e.g. a specific website, is determined by this context.

21a- For instance, in the online behavioral advertising context, Commission staff has stated that where a website provides recommendations or offers to a consumer based on his or her prior purchases at that website, such practice constitutes firstparty marketing.

I recommend the FTC revise this definition of first party marketing and restrict it to sending generic marketing solicitations. Without this restriction, an organization would have the power to keep a consumer profile, potentially much richer than a simple address and significantly beyond the time of fulfillment of the transaction which prompted the consumer consent. Such power should not be granted without the explicit consent of the consumer to a detailed "personal data contract" as explained in section IV-a above.

21b- Is there a distinction, however, if the owner of the website or the offline retailer sends offers to the consumer in another context - for example, via postal mail, email, or text message? Should consumers have an opportunity to decline solicitations delivered through such means, as provided by existing sectoral laws?

I recommend the FTC base its decision on the cost to the consumer. Marketing sollications whose reception may increase the communication bill of a consumer, such as with cellular phone or with fax, should be considered as outside "first party marketing".
The same should apply to marketing solicitations whose reception has the potential to forcefully interrupt a consumer, such as with any type of phone calls, holding such an interruption to be a significant personal cost to the consumer.
Such restrictions should be also made general so as to stay independent of technical and business innovation. For example, sending an Internet cable subscriber a marketing solicitation may carry a cost in the future, assuming such solicitations include a sizable video and the cable company starts metering or limiting consumer bandwidth consumption.

22- Should marketing to consumers by commonly-branded affiliates be considered first-party marketing?

No. In the same spirit as the answer to question 21a above, to allow affiliate communications would significantly increase the power granted by the consumer to the organization and decrease the transparency of the process as some companies may have hundreds of affiliates. Better to require the explicit consent of the consumer to a detailed "personal data contract" as explained in section IV-a above and the answer to question 24 below.

23- How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choice about this practice?

By definition "data enhancements" are not necessary for any of the "common practices" which do not require a full, unbundled "personal data contract" as detailed in section IV-a above. Therefore organizations wanting to use such enhancements should provide choice to consumers by convincing them to enter into an appropriate "personal data contract". One should mention that such sources, whose purpose serve no consumer directly, should all be required to strike their own "personal data contracts" with the consumers listed in their databases. Presumably this should be done through intermediaries who interact with consumers and can act as their retailers or agents, as for instance in the insurance industry. This requirement would also bring much needed transparency to the complex world of consumer data collection, storage and processing.

The case of credit reporting agencies merits a special mention. Their purpose is to provide consumers with a credit reference and they should have absolutely no difficulty to "sell" them the benefit of the corresponding "personal data contract", although genuine competition in what is today an oligopolistic market may require to give them free access to their credit history, again a boost to transparency. Their data furnishers should also have no difficulty in getting approval for their own "personal data contract". Reporting delinquent payments should be considered a part of the "fulfillment" of the transaction on which the consumer defaulted. As for regular payments, consumers should be eager to sign a "personal data contract" authorizing data furnishers to report them to the credit reporting agencies with the obvious compensation of an enhanced credit. However dubious current practices such as reporting a consumer for merely engaging in comparative shopping, e.g. for a student or a car loan, would stop as neither part of any commercial transaction nor to the advantage of the consumer.

Practices that require meaningful choice: General

24- What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?

As detailed in section IV-a, a "personal data contract" should specifies the legal terms and conditions of the market exchange including:
- what pertains to consumer personal data, such as but not limited to,
    - specific and limitative description of data collected,
    - retention duration,
    - explicit and limitative statement of purpose,
    - potential exclusivity relative to that purpose
    - list of partners and subcontractors to whom the data may be transferred for such purpose
    - security measures taken to protect confidentiality, including by partners and subcontractors
    - access given to the consumer to his or her own profile
    - notice given to the consumer to any change in the list of partners and subcontractors
    - audit of the above clauses by independent third parties
- the exact nature of the compensation offered to the consumer including
    - cash payments
    - goods and services in kind
    - what, if any, is offered in case of a data breach beyond the mandatory compensation
- common contractual conditions, such as but not limited to,
    - duration of the contract
    - manner in which the consumer can break the contract
    - non transferability to a third party without prior consent of the consumer

Informed by the terms of such a contract, the consent of the consumer must further be obtained in a free and explicit way, without bundling it with another transaction for which the execution of the contract is unnecessary, including, in the case of a barter, a compensation in kind when the alternative of getting the same compensation in kind, free of any unnecessary transfer of data rights, is not explicitly made available even for a price.

As an example of bartering, a social network service could be offered for free by a company within a "personal data contract" specifying the type of targeted advertising the company could sell, based on the profile filled in by the consumer. In this case the consent of the consumer would not be deemed free if this consumer did not have the choice to subscribe to the same social service for some set price but without giving out any rights to the company to his or her own data besides what is necessary to execute the social networking functionality.

The social network service would of course be free to start up as a free service without bothering about "personal data contracts" as long as it did not repurpose any user data. It would also be free to later experiment with multiple forms of barters and, in due course, find out what forms are the most attractive in terms of user acceptance and profitability. This is exactly what is being done by Facebook except that, in the absence of "personal data contracts", there is no transparency nor any attempt to win user consent except under the threat of user-led rebellions, a situation which undermines consumer rights and consumer trust, and ultimately limits innovation and industry competition.

25- Should the method of consent be different for different contexts?

No. The use and approval of a "personal data contract" is universal in principle. It is the content of the contract which will depend on the context.

26- For example, what are effective ways to seek informed consent in the mobile context, given the multiple parties involved in data collection and the challenges presented by the small screen?
This question is twofold.
From a technical perspective, the nature of the interface is a challenge for the presentation of complex information. However consumer profiles can be displayed even on small screens, especially when using the technology mentioned in the answer to question 6, whereby a confidential environment running on the device acts as unique data aggregator and profile manager, no matter how many parties are involved. As for the business details of a "personal data contract", it is not necessary to deal with them on the same device on which the consumer will register his or her final approval to the deal.
From a business perspective, the number of parties involved may multiply the "personal data contracts" to negotiate. However it is likely that one party within what is otherwise a complex value chain will take the initiative to impose standards contracts on the other participants and act as a retailer or an agent on behalf of them, greatly simplifying the decision process of the consumer. See the answer to question 40 on content providers for an example.
In any case it is advisable to let technical and business innovation solve these issues under a free market competition.

27- Would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts?

It would be inequitable to use such an icon as an opt-out mechanism or a similar warning that a consent is assumed unless withdrawn, especially in a way which would effectively bundle the equivalent of a "personal data contract" with some other desirable offer.
The only equitable manner to use such an icon is as a way to obtain the confirmation of a consumer to the final step of expressing consent to an explicit "personal data contract" which had been previously discussed with him or her. On online commerce sites, this "confirmation" button is typically presented after three or more interactive pages solely devoted to defining a transaction step by step. An example of how this could be efficiently implemented is discussed in the answer to question 40 below in "the case of content providers".

28- Is there market research or are there academic studies focusing on the effectiveness of different choice mechanisms in different contexts that could assist FTC staff as it continues to explore this issue?

The author has no information of academic import on this subject. However his streetwise experience shows that the most effective choice mechanisms always answer two questions:

- what do you want?
- what's in it for me?

A contract is the only way to satisfy these two questions with clarity and the possibility of legal redress.

29- Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?

This question is twofold.
As far as collecting and using personal data for the fulfillment of the offer, whatever it is, that the choice to the implied data exchange is a "take it or leave it" proposition is logical.
In any other situation, this would constitute unnecessary and, as recommended in section IV-a above, inequitable bundling, to be ruled out by the FTC as a deceptive practice and an obstacle to trade on a free market.
However when the offer actually intends to compensate the consumer for some unnecessary transfer of data rights, the "take it or leave it" of such a barter is allowable subject to the condition presented in the answer to question 30 below.

30- What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?

In such a bartering situation, the disclosure recommended in section IV-a above is to compel the organization which makes the offer to propose an alternative with the same service and no need for a "personal data contract". This puts a monetary value on the trade-off and informs the choice of the consumer between the two.
Free market competition will also provide the consumer with means of comparing this monetary value with other offers.

31- In particular, how should companies communicate the “take it or leave it” nature of a transaction to consumers?

As recommended in section IV-a above, this practice may be implicit as part of
- a "product and service fulfillment" case
- or a barter case with the disclosure of an unbundled alternative

or it must be ruled out as a deceptive practice and an obstacle to trade on a free market.

32- Are there any circumstances in which a "take it or leave it" proposition would be inappropriate?

As recommended in section IV-a above, this proposition is always inappropriate as being a deceptive practice and an obstacle to trade on a free market, except as part of:
- a "product and service fulfillment" case
- or a barter case with the disclosure of an unbundled alternative

33- How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?

As recommended in the answer to question 24 above, the scope of sensitive information should be part of the "personal data contract" whenever one is necessary.
However it must be remembered that, in the healthcare and health insurance industry for instance, such sensitive information may be naturally collected and use to fulfill ordinary transactions, a fact which is often made explicit as an opt-in cell which it is necessary to check on the forms and procedures used by these industries. This "take it or leave it" reminder is perfectly admissible.

34- What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection?

Deep packet inspection is a purely technical process and, as such, should not be ruled out as inequitable.
The type of data collection it enables is not however tied to any transaction fulfillment and, as any other unnecessary data collection by whatever means, should always require the informed consent of the consumer to an appropriate "personal data contract", free from any bundling entanglement, as recommended in section IV-a.

Consumers aside, deep packet inspection is technically at odds with the purity and hence the sustainability of the current Internet architecture as defended by Professor Tim Berners-Lee from MIT and the W3C. This technique further enables the relative competitive advantages of incumbents in the communication, content publishing and advertising industries to be redrawn. The best solution would be for the FTC to avoid any technical judgment which interferes with market competition among businesses.

Like all other intrusive techniques or business practices developed over the years to harvest consumer data, deep packet inspection may be rendered moot if innovative solutions like the one developed by the author and mentioned in the answers to questions 6 and 40 are adopted, as they enable the consumer to have total control over his or her data while reaping all the benefits of personalized interactions, such as targeted advertising, in cooperation with the organizations which propose them. This rebalancing of innovation away from privacy invading techniques is a major benefit of a free market and shows how consumer protection and industry welfare are not necessarily antagonistic.

35- What (if any) special issues does the collection or the use of information about teens raise?

Assuming "personal data contracts" are the consent mechanism adopted as recommended in section IV-a above, the case of teens is not a special issue. It should be governed by the existing body of laws, which imposes a minor to be represented either by a parent or a legally appointed tutor when executing a contract.

36- Are teens sensitive users, warranting enhanced consent procedures?

Yes in the sense of the answer to question 35 above.

37- Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone." What are the benefits and drawbacks of such an approach?

The "personal data contract" mechanism recommended in section IV-a above is focused on consumer data right transfers which are not necessary to the fulfillment of a transaction.
From this perspective social networks, which enable their members to share information with other members, may present special challenges to privacy protection outside of the "notice-and-choice" model and even of the "harm-based" model in the sense that harm is self-inflicted by the consumer during the fulfillment of the desired transaction.
It might be both appropriate to disjoin such a special and sensitive topic from the current framework and rejoin it as the separate and important question of protecting minors from self-chosen irresponsible behaviors. The toy industry for instance is held responsible for manufacturing safe toys. In computer-mediated services, social media services may not be the only source of such worries. What to make for instance of computer games, including massively multiplayer online role-playing games?

38- What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?

As detailed in section IV-a and the answers to questions 23 an 26 above, it is recommended companies which do not directly interact with consumers and yet need to enter into a "personal data contract" either use those companies which do, either as clients or suppliers of consumer data, as retailers or agents or invest in other sales channels as they see fit.
The case of advertising networks engaged in targeted advertising is examined in the answer to question 40 below.

39- Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?

It is only natural that data brokers standardize on an appropriate "personal data contracts", for example according to a "Fair Personal Data Contract Model" approved by the FTC under a safe harbor mechanism as detailed in section IV-a above. However such standardization should not be such that it be contrary to antitrust laws. A parallel can be found in the homeowner insurance industry. While its contracts are actually fairly standard, they are also modular, the pricing of each module is free and special riders can always be introduced so that competition remains lively.
Ultimately the benefit of the mechanism is to bring down the cost of the associated "data transactions" while enabling innovation and competition to thrive to the direct benefit of the consumer.

Take for instance innovative solutions like the one developed by the author and mentioned in the answers to questions 6 and 40. They enable the consumer to have total control over his or her data while reaping all the benefits of personalized interactions, such as targeted advertising, in cooperation with the organizations which propose them. With such an approach, a data broker could get rid of the actual storing and processing of consumer data and act more like a cooperative, selling to its clients the service of downloading their external agents to the consumers who have signed its novel "personal data contract".

Practices that require meaningful choice: Special choice for online behavioral advertising: Do Not Track

40- How should a universal choice mechanism be designed for consumers to control online behavioral advertising?

the "Do Display" approach

As detailed in section IV above, online behavioral advertising is a very important example of a data transaction requiring the free and informed consent of consumers to some appropriate "personal data contracts". This represents a contrarian approach to the legitimate effort of the FTC to protect consumer privacy against the dangers of targeted advertising while preserving the vitality of this recent phenomenon. Instead of asking consumers who do not want to be tracked to register with some site, this approach asks consumers who are willing to be tracked to register with the organizations engaged in the tracking value chain which feeds the display of targeted ads.

This "Do Display" approach is thought to be more robust in view of the difficulty to police a "Do Not Track" mechanism. Contrary to what happens with the "Do Not Call" registry, an individual consumer cannot easily tell a violation has occurred and the FTC does not have the resources necessary to investigate on its own. It is true that initial ramp up problems have led current targeted advertising networks to deliver the same ad to consumers who see it following them from site to site. While highly visible, this tracking ad phenomenon is a temporary artifact independent of the much more serious and invisible issue of behavior tracking.

The "Do Display" approach is predicated on the responsibility of the site on whose pages the targeted ad is displayed. The reason is twofold:

- as an ad space seller, it is the main beneficiary of the income stream generated by targeted advertising
- as a content provider, its reputation is the most at risk as the consumer knows about and voluntarily patronizes its site

It is further recommended to make this actor responsible for giving its "Do Display" consumer access to his or her profile each time a targeted ad is displayed.
Finally sites which are found in violation of their contracts or without the necessary contract would risk civil penalties but also, whenever they do it knowingly, in a systematic or reckless manner, federal criminal offenses, as recommended in section IV-d above.

The most powerful of such sites will likely police the rich pool of actors participating in the value chain to insure they do not run afoul of the law. Actors they come to recommend will gain the confidence of less powerful sites, which lack the resources necessary to control the rest of the chain by themselves.
Once one of these same powerful sites has signed a "personal data contract" with a consumer, it might also be of its own interest to prevent competitors to draw the same benefits without the constraint of a contract and thus not only recommend ethical actors but also investigate unethical ones, either directly or via an industry association and denounce them in the same way or via the consumer concerned. Similarly, while a patent licensee usually expects its licensor to protect the rights of the patent concerned, it is always possible for a powerful licensee to attack a competing infringer directly as the harm is shared between licensor and licensee alike.
A "Do Display" approach of course cannot directly prevent unethical actors from tracking consumers against their will no more than a "Do Not Track" registry. But by enabling an effective control over sites which display targeted ads, it should cut off the income stream of the rogue sites engaged in illegal tracking, which do so under the hope of being paid for the display of ads they help target.

The "Do Display" approach brings a further benefit as it compels consumers to identify themselves as they sign the corresponding "personal data contract", resolving the conundrum of how to give access to one's profile based on a simple Internet Protocol (IP) address when there is a risk, however small, of an identity error. The execution of the "personal data contract" would provide a secure login procedure.

the case of content providers

Content providers merit a special mention as many business models have been supported by advertising in the past and it is highly likely content providers will want to make full use of opportunities promised by targeted advertising in the future.
As long as advertising is not targeted, there is no need for "consumer data contracts".
If a content provider wishes to introduce targeted advertising, it may draw as many bartering deals as needed, as long as each deal specifies:

- its associated "personal data contract", whereby
  the consumer compensation is some form of free access to content, with perhaps some extra cash compensation
- its alternative, whereby
  the consumer has access, likely for a subscription fee, to the same content without transferring any data rights

In this manner the consumers will be free to judge for themselves what are exactly the benefits of targeted advertising that the content provider offers.
As consumers of the content will be clearly identified either as clients paying for the content or as registered data suppliers paid in kind, it is likely that digital piracy will decrease and trust will increase.
The content provider may act as a "personal data contract" retailer for the advertising network, which has no normal direct contact with the consumer. It is likely that the advertising network will in turn act as an agent for the information sources which engage in tracking the consumers, for the sake of standardizing their "personal data contracts". In this regard the advertising network could obtain the informed consent of the consumer to a common "personal data tracker contract" represented by a specific icon but with the name of the tracker left blank. Later each information source affiliated to the advertising network could obtain the informed consent of the consumer by displaying this icon for the consumer to opt-in in one click as suggested by question 27.

potential results of free market competition

Competition will drive different advertising networks to offer different income streams to a given content provider and content providers to pass on different fractions of these streams to a given consumer. It will be even possible for advertising networks to bypass content providers and sell their own "personal data contract" directly to consumers to be used on participating content providers. This is especially feasible and attractive if targeted advertising uses the innovative technology mentioned in the answer to question 6. Developed by the author and detailed in US Patent Application no 2009/0076914, this implementation of targeted advertising is one use of the personal confidential interactive environment described in US Patent no 6,092,197 and the profile targeting mechanism described in US Patent application no 2006/0053279.

The principle of the solution is to let the confidential environment of a consumer 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 and the source of each profile item is recorded, 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.

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 on the page of a participating content provider acting as a space seller.

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 five 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
- ad personalization, with no liability relative to holding consumer personal data
- ad display, governed by the personalized ad service
- service auditing, performed on the local journal maintained by the environment

Thus, in its capacity as ad space seller, a content provider has no access to the consumer data used for targeting and, while receiving higher fees for its space, can continue to operate as before with no need for "personal data contracts" nor fee-based alternatives. Besides information furnishers, the only "personal data contract" needed is from the advertising network providing the service personalization and, as no one other than the consumer, including third parties, has access to the aggregated profile used for targeting, this contract is very simple and attractive, with the possibility to offer cash to the consumer or perhaps a discount on digital content sold by an independent online content store.

Offering cash for watching ads presumably attractive to the viewer has been pioneered by MyPoints.com, a United Airlines subsidiary, based on the Cybergold US patents 5,855,008 and 5,794,210. This is not the only possible way to give cash or cash equivalent rewards to consumers who voluntarily participate in targeted advertising. Instead of depending on their viewing the ads, their compensation could also be based on the use of their profile, in a manner similar to how the author's invention proposes to reward profile information sources.

On such a free market and as explained in section IV-a above, consumers will be able to pick the most effective advertising networks, either directly or indirectly, while independently patronizing the best content providers. By dissociating privacy protection from business model considerations, this privacy-enhancing technical innovation has the potential to unleash business innovations for which the key factor would be the ability to develop cooperating networks of information trackers, advertisers, content providers and consumers.

41- How can such a mechanism be offered to consumers and publicized?

According to the detailed answer to question 40 above, the contractual mechanism described would be most likely driven by:

- either the sites displaying targeted ads, which are in natural contact with their own visitors
- or the advertising networks, reaching out to consumers through direct advertising or other indirect channels

42- How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?

Consumers would have no difficulty in understanding the contractual approach detailed in the answer to question 40 above.
As explained in the answer to question 28, such an approach addresses their two major concerns:

- what do you want?
- what's in it for me?

assuming the FTC follows the recommendation of section IV-a above, rules out bundling as inequitable and thus provides a positive answer to their third major concern:

- do I have a choice?

Most consumers have a common experience in dealing with complex contracts such as an auto insurance or an extended warranty on kitchen appliances. At the very least "personal data contracts" recommended in section IV-a above will appear to be a model of clarity and conciseness, compared to obfuscatory Privacy Policies "designed more to limit companies' liability than to inform consumers about how their information will be used".
Actually competition will soon ensure these contracts are sold with great efficiency by focusing the attention of the consumers on simple, key differentiators, e.g. the level of privacy protection and the compensation offered.
Consumer Reports and other sites will develop comparative charts.
While vigorously prosecuting all deceptive practices, the FTC can offer a safe harbor approval to "Fair Personal Data Contract Models" developed by the industry.

43- How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of the choice are?

To back the contractual approach detailed in the answer to question 40 above, section 5 of the FTC Act fully empowers the FTC to ensure contracts are free from deceptive practices, including the false "take it or leave it" choice created by bundling "personal data contracts" with other, independent, desirable offers, as indicated in the answers to questions 31 and 32 above.
Meanwhile free market competition pushes marketers to develop easy to grasp presentations of the strengths of their offer.

44- What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?

The danger of too much standardization is to create a latent conflict with antitrust laws or abandoning the benefits of free market competition and the innovation it drives. However carefully introduced standardization decreases so-called free market transaction costs, as illustrated in the answers to questions 39 and 40 above.

45- How many consumers would likely choose to avoid receiving targeted advertising?

The answer obviously depends on the context in which targeted advertising is allowed to develop.
With the free market approach recommended by section IV-a above and further detailed in the answer to question 40 above, very few consumers would deprive themselves of the significant benefits created by targeted advertising, especially if the actors of the value chain compete by:

- sharing more of their financial gains with the consumers
- embracing technical innovations such as the author's to offer total privacy protection to the consumers.

Without a free market approach, policing the many actors of the value chain, which are invisible to the consumers and may be outside the reach of the FTC, will remain difficult, undermining consumer trust in an exploitative system, even though many consumers may decline registering their wishes for better protection as a waste of their time.

47- What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?

With the free market approach recommended by section IV-a above and further detailed in the answer to question 40 above, this is a highly unlikely situation.
Otherwise the likely outcome will be:

- either a repeal under industry pressure of the measure which has enabled consumers to opt-out
- or a shift of targeted advertising to a shady world of difficult to police intermediaries, with
    - data collection practiced by malware
    - data aggregation implemented by foreign entities, already known for spamming and botnet farming
    - advertisers and ad space sellers insulated from these actors by laundering specialists

In both cases consumers will be losers. In the latter case, even the legitimate industry will lose as the economic revenues will be smaller overall and will have to be shared with the underground operators.

48- In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?

It is highly desirable to let free competition express the best business models. Granular choice would give consumers greater choice and there is scope for domain specialization, e.g. targeted advertising for sports, travel, education...
With the free market approach recommended by section IV-a above and further detailed in the answer to question 40 above, this differentiation will be likely as consumers will contract out with the content providers or the advertising networks of their choice. At least some of these counterparts will find domain specialization a natural differentiator, especially given their added value is in part to develop cooperating networks of information trackers, advertisers, content providers and consumers. Indeed content providers today are often specialized by domain.
The author's innovation described in US Patent application no 2006/0053279 shows how easy it can be for consumers to express their control by signalling their wishes to advertisers and pre-filtering their ad flow. It is important to note the difference between a personal profile item, "I hate cats", and a wish, "Is your offer related to cats?". The latter is only weakly correlated to the former, e.g. "I hate cats but my grand-daughter adores them", and does not need the same level of protection.

49- Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?

The free market approach recommended by section IV-a above and further detailed in the answer to question 40 above is a truly universal mechanism which makes no difference about point of contact technologies. As developed in the answer to question 26 above, the practical implementation of the approach will of course depend on technical functionalities.
Any approach which makes a difference in principle between technologies is bound to introduce administrative bias in their development. This would be as detrimental as the current approach by default, biased as it is against privacy as explained in section II above and illustrated in the answer to question 15 above.

50- If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?

It is not in the self-interest of for profit companies to truly endorse a mechanism which promotes competition. It will only implement a uniform choice mechanism voluntarily if the latter fails to protect the consumers from current exploitation or at least create a safe harbor for practices otherwise subject to antitrust law.
As the answer to question 47 shows, individual companies may find it expedient to appear endorsing a mechanism which can be bypassed by illegal means safely kept at arm-length.
However the FTC is already empowered by section 5 of the FTC Act to protect consumers from deceptive practices, which suppresses contractual freedom as illustrated in section IV-a above. This should be reason enough for the FTC to compel the industry to adopt the recommended mechanism detailed in the answer to question 40.
If the FTC feels necessary, it may seek to obtain further legislative backing, for example to more explicitly condemn the practice of bundling "personal data contracts" with an independent, desirable offer.

Companies should increase the transparency of their data practices

Improved privacy notices

51- What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

The issue of standardization relative to antitrust statutes has been addressed in the answer to question 44 above.
From an implementation point of view, a word should be said about the use of formal systems in privacy practices as they create a feasible framework for both defining and enforcing such practices.

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 personal confidential, interactive environment developed by the author and presented in the answer to question 40 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.

In this architecture, each layer enforces more formal constraints on those above it. In particular the middle level allows macros developed by industry associations and approved under a safe harbor as recommended in sections IV-a and b above to be easily used as industry standards as long as more innovative industry members are not obliged to follow them.

52- How can companies present these notices effectively in the offline world or on mobile and similar devices?

One should distinguish implementing a standard from getting the consumer to give his or her approval.
As explained in the answer to question 26 and illustrated in the answer to question 40 for the case of content providers, it is not necessary to deal with the business details of a "personal data contract" on the same device on which the consumer will register his or her final approval to the deal.
On the other hand the formal system developed by the author can be implemented on a mobile or similar device as long as it supports 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 ability to handle so-called trusted Java applets.

53- Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?

Assuming a free market, it would indeed be very efficient for consumers to automatically search and compare "personal data contracts" by feature.
This however is not a current requirement of commerce and the trend, judging what the airline industry is doing and the results of research by Professors Glenn and Sarah Fisher Ellison from MIT, is more toward obfuscating such search and compare tools.

Reasonable access to consumer data

54- Should companies be able to charge a reasonable cost for certain types of access?

On a free market, nothing should oblige organizations to charge at least some consumers for accessing their profile, the way banks charge for printing checks or keeping a checking account. However consumers may be expected to refuse to enter into contracts with such burdensome clauses which, in the case of banks, are really designed to keep less desirable consumers away.
For what happens when the market is not free, see the oligopoly of credit reporting agencies. The latter actually charge all consumers access to their own data and the government has imposed a minimum right to free access.

55- Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?

This point should be a clause of any "personal data contracts" as detailed in the answer to question 24. The inclusion in such a contract of the right to transfer consumer data for a reason which is not necessary to its explicit purpose should furthermore be declared to be a deceptive practice in accordance to section IV-a.

56- Where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?

This special case should be handled in accordance to the practices of schools and healthcare services catering to children. While the parents of a minor would be responsible for executing or not the "personal data contracts" from which their child may want to benefit, this may not give them the rights to accessing their child's personal profile.

57- Should access to data differ for consumer-facing and non-consumer-facing entities?

There should be no difference in principle although implementation would obviously differ. Within the approach recommended in section IV above, a non-consumer facing entity would probably use a consumer-facing entity as a retailer or an agent to avoid the burden of managing consumers directly.

58- For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?

Such non-consumer-facing companies cannot sell their information without at some point involving a consumer-facing entity. By declaring the latter must inform the consumers of any data import or export necessary to the purpose approved by the consumers, as part of the "personal data contract" recommended in section IV-a above, no non-consumer-facing could remain in the shadows. To avoid being accused of deceptive practices, they would seek to draw their own "personal data contract" as required, likely through a consumer-facing entity acting as their retailers or agents.

59- Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?

By forcing non-consumer-facing entities to enter into "personal data contracts" with consumers, the recommendations developed in section IV above would make the question somewhat moot as consumers would become aware of these entities. The advantage is that the author's innovative approach described in the answers to questions 6, 39, 40 and 51 above, would then provide an easy solution as mentioned in the answer to question 39 above. It uses a personal, confidential, interactive environment which hosts external agents sent by authorized organizations, including non-consumer-facing entities, behind what can be thought of to be a privacy one-way valve. This environment further plays the role of standard profile manager, accessible at all times by the consumer whose profile it is and by no one else.

Material changes

62- What is the appropriate level of transparency and consent for prospective changes to data-handling practices?

This point should be a clause of any "personal data contracts" as detailed in the answer to question 24. The right to change at will without prior and explicit consent of the consumer should be declared a deceptive practice according to section IV-a.

Consumer education

63- How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?

The best incentive would be the need for individual businesses to sell "personal data contracts" to consumers as recommended in section IV-a. Market competition will then reward the best communication efforts, with the help of the traditional facilitators of commerce.

64- What role should government and industry associations have in educating businesses?

The safe harbor mechanisms recommended in sections IV-a and b would be efficient tutors, providing positive guidance without infringing on industry freedoms, while the needed negative guidance would come from FTC rules explicitly detailing deceptive practices it forbids as part of its mission per section 5 of the FTC Act.