Kaliya Hamlin
Mary Hodder
Personal Data Ecosystem
Collaborative Consortium

Submitted by email: privacynoi2010@ntia.doc.gov

January 28, 2011
Gary Locke, Secretary of Commerce
Lawrence E. Strickling, Asst Sec for Communication and Information
Francisco J. Sánchez, Under Sec of Commerce, Intl Trade
Patrick Gallagher, NIST
U.S. Department of Commerce
1401 Constitution Avenue, NW., Room 4725
Washington, DC 20230

Re: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

Dear Secretary Locke, Mr Strickling, Mr. Sánchez and Mr. Gallagher:

We are submitting these comments in response to the December 2010 Commerce Department Privacy Green Paper.

We represent a community of end-user advocates and technology innovators focused on individual rights and access to individuals' own personal data, and the business and innovation opportunity that this new user-management and control offers (our full list of names are noted at the end of this letter).

First, we want to outline where we are coming from, and then we will comment on how this future-oriented view informs our response to the Green Paper and questions for further comment.

Personal Data Storage and Services

A Middle Way between Do Not Track and Business as Usual Stalking

There is a way to deal with users' personal data that most have not yet explored. This alternative approach sits between the two extremes of a familiar spectrum: either Do Not Track, or Business as Usual Stalking.

On one end of the spectrum is the “Do not track” view, which relies on using technology and a legal mandate to prevent any data collection (as per the FTC Proposal). In this scenario, cross site behavioral targeting is suppressed because users signal they do not want any information to be collected on them as they move about the web. In this approach the economic value advertisers have been getting through higher click-through rates by providing more targeted ads is eliminated and sites that receive revenue from serving targeted ads is reduced if not eliminated. The economic value of the data is not captured by the end-user or the media/advertising/data aggregating complex.

And on the other end of the spectrum is the mode where we leave “Business as usual” in place as it's developed in the last few years. The door is wide open for ever more “innovative” pervasive and intrusive data collection and cross referencing for behavioral targeting, developing profiles - digital dossiers created on billions of people, without their knowledge or consent, based on IP address, device identification, e-mail address etc. The status quo is highly invasive of people’s privacy, linking their activities across contexts they wish to keep separate or private if they chose to do so. In addition, decisions about people's lives are beginning to be made from such data, and they are not aware of it. Economic value is derived, but at the expense of the basic dignity and privacy rights (ie personal control) of the individual.

Personal data storage services are emerging, representing a middle way through, to provide an opt-in mode with greater choice and control to the individual of their data AND offer greater economic value to the business community with huge innovation opportunities.

As envisioned, Personal Data Storage Services allow individuals to aggregate their personal data, to manage it and then give permissioned access to businesses and services they choose -- businesses they trust to provide better customization, more relevant search results, resulting in increased value for the user with their data.

Over the last year, activity in this space has grown tremendously. In this emerging field of innovation, we have identified over ten startups, at least three open source projects, several technical standards efforts in recognized ISO’s along with companies in the web, mobile, entertainment and banking industries considering this model.

One of the most important things about this emerging space is that it has engendered active business development both in the United States and across Europe. In other words, this model is viable across North American and European privacy regimes. Furthermore, this model offers the possibility of achieving global interoperability, one of the key goals articulated by the Commerce Department for this forthcoming set of policies and regulations.

People are the Only Ethical Integration Point for Disparate Data Sets

Today there is a personal data ecosystem emerging in which almost everyone unknowingly participates but without the personal individual controls to afford user centric privacy. People unwittingly emit information about themselves, their activities and intentions, in various digital forms. It is collected by a wide range of institutions and businesses with which people interact directly; then it is assembled by data brokers and sold to data users (ie businesses that exploit our data without including us in the transaction). This chain of activity happens with almost no participation or awareness on the part of the data subject: the individual.

We believe that the individual is the only ethical integration point for this comprehensive and vast range disparate personal data. For example, the list of data types below was put together by Marc Davis for the World Economic Forum talk: Re-Thinking Personal Data event in June of 2010. It highlights the vast range of datasets about an individual that might be in some digital form in some database somewhere.

Identity and Relationships
* Identity (IDs, User Names, Email Addresses, Phone Numbers, Nicknames, Passwords, Personas)
* Demographic Data (Age, Sex, Addresses, Education, Work History, Resume)
* Interests (Declared Interests, Likes, Favorites, Tags, Preferences, Settings)
* Personal Devices (Device IDs, IP Addresses, Bluetooth IDs, SSIDs, SIMs, IMEIs, etc.)
* Relationships (Address Book Contacts, Communications Contacts, Social Network Relationships, Family Relationships and Genealogy, Group Memberships, Call Logs, Messaging Logs)

Context
* Location (Current Location, Past Locations, Planned Future Locations)
* People (Copresent and Interacted-with People in the World and on the Web)
* Objects (Copresent and Interacted-with Real World Objects)
* Events (Calendar Data, Event Data from Web Services)

Activity
* Browser Activity (Clicks, Keystrokes, Sites Visited, Queries, Bookmarks)
* Client Applications and OS Activity (Clicks, Keystrokes, Applications, OS Functions)
* Real World Activity (Eating, Drinking, Driving, Shopping, Sleeping, etc.)

Communications
* Text (SMS, IM, Email, Attachments, Direct Messages, Status Text, Shared Bookmarks, Shared Links Comments, Blog Posts, Documents)
* Speech (Voice Calls, Voice Mail)
* Social Media (Photos, Videos, Streamed Video, Podcasts, Produced Music, Software)
* Presence (Communication Availability and Channels)

Content
* Private Documents (Word Processing Documents, Spreadsheets, Project Plans, Presentations, etc.)
* Consumed Media (Books, Photos, Videos, Music, Podcasts, Audiobooks, Games, Software)
* Financial Data (Income, Expenses, Transactions, Accounts, Assets, Liabilities, Insurance, Corporations, Taxes, Credit Rating)
* Digital Records of Physical Goods (Real Estate, Vehicles, Personal Effects)
* Virtual Goods (Objects, Gifts, Currencies)

Health Data
* Health Care Data (Prescriptions, Medical Records, Genetic Code, Medical Device Data Logs)
* Health Insurance Data (Claims, Payments, Coverage)

Other Institutional Data
* Governmental Data (Legal Names, Records of Birth, Marriage, Divorce, Death, Law Enforcement Records, Military Service)
* Academic Data (Exams, Student Projects, Transcripts, Degrees)
* Employer Data (Reviews, Actions, Promotions)

In addition to this list, there is also the emerging wellness, or "quantified self," data that some users are beginning to collect about themselves through life-tracking companies including daily or more granular statistics about their bodies and wellness activities.

Service Providers Must Work For the End-User
Most people do not host their own e-mail servers or websites on servers in their basements. Similarly, most individuals will not have the technical skill or desire to actually manage the collection, integration, analysis, permission management and other services needed to derive value from their data. However, the fact that a few users can host their own email means the open standards for email and http are available top to bottom. We what to see Personal Data Services available through open standards, open source code and an ecosystem that will interact with people who host their own PDS.

But mostly, individuals need to be able to trust that the service providers in Personal Data Ecosystem are working on user's behalf. Given the sensitivity of the data, and the complexity of running your own servers, most users will rely on Personal Data Service providers. In addition, market models need to emerge that support the Personal Data Store Service Provider making money while working on the users' behalf. The Personal Data Ecosystem Collaborative Consortium has a Value Network Mapping and Analysis project to outline this model and is raising money to support and foster the model.

Personal Data should be treated like Personal Money.
Individuals must be able to move data between service providers, as they can move money between banks, retaining its value. However, with user's data, it's the user that is the provider, but there must still be many takers because of open data formats, activity streaming, and clear identity models that are also portable and separate from the data bank.

End-user choice and the right to transfer data from one service provider to another is key to this model. Just as our money does not become worthless when we move it from one bank to another, the same needs to hold true for individuals' data.

Consumers need to be able to to Collect and Aggregate Their Data from Product and Service Providers
For this Personal Data Ecosystem and Economy to emerge, it is essential that consumers have easy access to their data from the providers they do business with. The steps involved in getting data out of services are tedious and onerous, and often multi-step because we don't have clear "patterns" and open standards for getting data, nor do we require companies to give a copy of your complete data.

1. Data must be available in machine readable ways using open standards such as microformats and activity streams that are driven by many developers and users, not just a single company. Where data export is available, it is often not machine readable. Manually exporting repeated monthly statements as they are issued is not the answer as a few services offer.

2. Simple Internet Open Standards like OAuth allow for account linking without the dangerous practice of giving a username and password to various service providers. Instead, an OAuth token is issued, and username and PW are passed only to the issuing party. This keeps users from sharing login information with unscrupulous services and means the OAuth provider doesn't have to "police" a service just to manage login credibility.

3. Portability of data is critical for many reasons, including in managing a business failure. People need to be able to move their data to an alternate

and hopefully more viable provider in these instances. Additionally, to create competition and innovation for Personal Data Services, data must be portable to prevent "lock-in" -- which is currently what many businesses use to prevent users from going elsewhere.

Data persistence and portability is critical so that as services disappear, user data and digital assets (for example, the social bookmarking site Del.icio.us makes personal data available to users and it's been used a lot recently after Yahoo! was reportedly shopping the website) will persist. Users create content and generate data during site usage and those users should be able to easily export their work product from those sites. Business models should not rest on "locked-in" data from users.

The Commerce Department should recommend that Congress legislate basic data portability together with a framework for prohibiting cross-site aggregation about a user unless the user agrees to have their data aggregated. Then, the FTC would enforce data portability and the prohibition of cross-site aggregation of personal data without user's explicit permission.

Create a Level Playing Field around Data Aggregation and Services
Which companies can do what with what kinds of data?

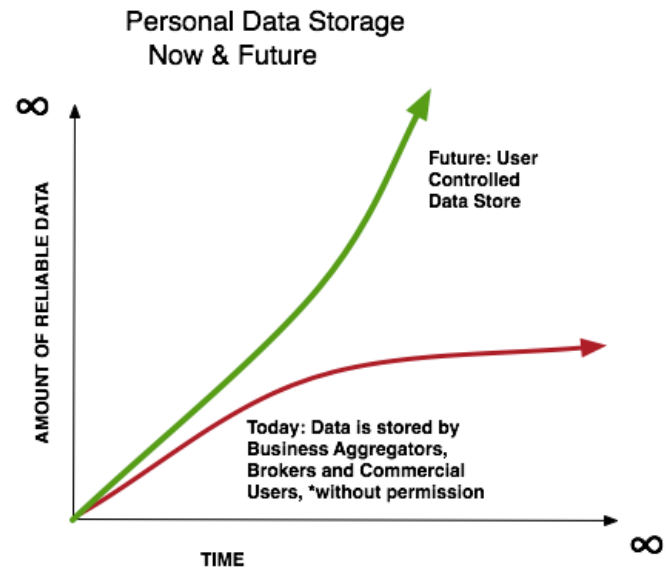
Today the regulatory patchwork associated with data protection means that different types of data are subject to different protections affecting how different industry sectors use and compete in relation to personal data (ie Hipaa data or financial data or educational data which are regulated verses other personal data which is not very regulated).

For example, Google and Facebook have vast collections of data about individuals -- resulting from their activities on Google's and Facebook's sites/ systems: what user's click on, who they know, what they search for, where they go etc. Sites analyze these data sets and then provide "relevant" ads based on the site's best guess as to the user's their activities.

Today with mobile devices connected to the web, mobile carriers collect a very similar set of data - where an individual goes, who they call and text, where they go to on the web. Yet mobile carriers are subject to very different (and more strict) regulatory regimes which prohibit them from using this data as freely as Google and Facebook.

A model where 1. individuals choose a data service provider where each individual collects and aggregates their data in a "data bank" and 2. can freely consent to providing access to it to 3rd and 4th party service providers, will result in greater individual data control while providing businesses with more accurate and comprehensive personal (at whatever level people choose: anonymous, pseudonymous or named) profiles, creating enormous market and business opportunities because the businesses that want these interactions can count on the data quality and the desire to interact. Right now, advertisers have imperfect data and are forced to "buy" far more reach than is necessary in order to get to those who are interested.

Keeping our Data for a Lifetime, If We Want to
What if the individual could choose to retain all or a subset of the information about themselves for as long as they wanted? This is a graph that shows today's current data environment and a future where people are in control of their own data, and the opportunities around opt-in, more reliable data than stalking users surreptitiously currently permits.



The red line shows us what's happening today: some data aggregators are necessarily self-regulating by limiting the amount of time they keep data, and governments are limiting data retention and anonymization practices. And much data that is collected is without explicit permission, other than through onerous privacy policy the user agrees to once (usually) and

The green line shows us what WOULD happen if people were given the capacity to store and manage their own data – if they could keep as much data as they wanted for as long as they wanted, in their own data banks. Digital footprints reflecting a lifetime could be shared with future generations, people could self assess, and applications through a marketplace would emerge to create new businesses and data uses we haven't yet thought of to date. In this user-centric model, the individual can aggregate information about themselves, where new classes of services -– more specific to the individual, based on data accessed with user permission, can emerge.

The foundation of this eco-system is personal data storage services that are totally under the control of the individual. But a user-centric identity system needs to function in partnerships with it (separate from a PDS) and we will need a regulatory regime that supports both of these technology solutions in user-centric form, where users own and control their own data.

These new data and identity service providers will be more viable if individuals can have simple ways to link their accounts and data together if the user desires, even if multifaceted identity systems reflect a complex personal outlook to the world. One thing to note is that in systems that offer multiple faceted identities under one login, that men reportedly maintain two identity facets, but women are averaging six (this statistic was reported to us personally from individuals at Diaspora, the open source social network). Indentity systems need to be flexible to accommodate user needs with a variety of requirements. And of course, simplifying the login and password problem people face online is something we support heartily.

The model presented above, a Personal Data Ecosystem where individuals are in control of their own data, aligns with the interests of all the stakeholders the Commerce Department is seeking to balance.

Companies who collect personal data win: by sharing and synchronizing with people's personal data stores, companies get far more accurate information. New services can be offered on data sets, including data not previously permitted to be used or accessed for providing services (telephone log records or mobile geolocation data, for example). And innovation for the PDS and apps marketplace would be a huge new area of development for startups and large companies alike.

People win: by collecting, managing, and authorizing access to their own personal data, users will increase their trust and use of digital realms. This empowers people to work together in communities and groups more efficiently and effectively. Users will be able to see themselves reflected, and participate in transactions more directly with vendors.

Regulators, advocates, and legislators win: by protecting people with new frameworks that also encourage innovation and new business opportunities, government can give people useful tools to interact with agencies because user's identities are trusted.

Thank you for the opportunity to share our world view on personal data. Attached below please find our specific answers to the Green Paper questions.

Kaliya Hamlin, Personal Data Ecosystem Collaborative Consortium
director@personaldataecosystem.org
@identitywoman
Mobile: 510-472-9069

Mary Hodder, Citizen, User Advocate, Founder and Entrepreneur
mary@hodder.org
@maryhodder
Mobile: 510-701-1975

Co-Signers:
Sarah Allen, CEO Blazing Coud, Inc.
Stacy Banks, Citizen
Joe Boyle, Developer
Judith Bush, Citizen
Aldo Castenada, Personal Data Ecosystem Podcast and Citizen
Jennelle Crothers, Citizen
Iain Henderson, Mydex
Emily Howe, Citizen
Dwight Irving, Ph.D.
Joe Johnston, Respect Network
Liana Leahy, Citizen
Kevin Marks, Microformats.org
Drummond Reed, Respect Network

Appendix: Questions and Answers from the Green Paper

Section A. Bolstering Consumer Trust Online Through 21st Century Fair Information Practice Principles

Recommendation #1: The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

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

Yes. However without the data and privacy framework in place, it's hard to know what the FIPPs and enforcement should be.

One key aspect that makes FIPPs effective include Purpose Binding the legal framework that makes it illegal to store data without the purpose for which it was collected to be maintained with the data. Purpose Binding would make storage reasons clear for auditing purposes as well.

People need disclosure of the purpose for which the information is to be gathered so that they can agree or stop the information gathering.

Individuals should have the right to have a copy of their data in machine readable form so that it's easily accessible and portable to Personal Data Services and applications.

Companies who collect data and wish to use it for a purpose different from that stated could "return" the data to the individual and then be re-granted or license the right to access/use the data.

Question A. 2) (appendix 1b) How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in

addition to being the basis for FTC enforcement actions?

Until the data and privacy framework is agreed upon, it's difficult to answer this question. However, speculatively, we would like to see a vibrant market of auditors who are measuring compliance fostered as part of the Personal Data Ecosystem. Companies with a good reputation/audit would attract more business and users.

Auditing should not be done by the FTC on a day to day basis, but enforcement against companies that are out of compliance would be appropriate. We believe a commercial marketplace that values compliance and allows consumers can make informed choices is best.

Question A. 3) (appendix 1c) As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?

Yes. The FTC should be granted authority to issue more detailed rules about how data portability and non-collection of cross-site data is handled once the framework is agreed upon. FIPPs that protect users and give them reasonable notice should be encouraged, as well as favoring data maintained in open standards instead of single company standards. As an example, finding simple ways to communicate privacy and data portability controls to users needs to be created with public domain icons matched with simple controls for privacy data actions. The FTC could suggest a standard in their FIPPs but allow innovators to create these icons, definitions and controls for users in a common, shared, open source manner for the public domain and use by any site or entity online.

Question A. 4) (appendix 1d) Should baseline commercial data privacy legislation include a private right of action?

Yes - if Purpose Binding is enacted and individuals find data about them that is stored without the purposes for which it was collected maintained they should have the private right of action.

Subjects should also have a right to access the data stored about them.

We are on the cusp of tools being able to support individuals who wish to keep track of all the information they share digitally (via web forms, applications and via mobile devices) - with which company and under which conditions. If a consumer's record of their own behavior and actions does not match those of a company - that is, they have a purpose binding and date of collection but the consumer does not have a record of the transaction. This could be grounds for a private right of action.

Section B. Advancing Consumer Privacy Through a Focus on Transparency, Purpose Specification, Use Limitation, and Auditing

Recommendation #2. To meet the unique challenges of information-intensive environments, FIPPs regarding enhancing transparency; encouraging greater detail in purpose specifications and use limitations; and fostering the development of verifiable evaluation and accountability should receive high priority.

1. Enhancing Transparency to Better Inform Choices

Question B. 1. 1) (appendix 2a) What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.

We believe that by leveling the playing field regarding personal data collection about individuals across multiple sites (ie, regulating that multi-site data collection only be done with user permission and control) and encouraging innovation around the Personal Data Ecosystem (an ecosystem of technologies and companies that work within the proposed bounds of user controls over their own data, user knowledge and choice, use limitations and audits), that many technologies, companies, applications, open data systems and formats will be created.

The market power and size will be far greater than it currently is in the data collection industry because users will feel safe about sharing very personal data through personal assertion with 2nd party authentication. Then, businesses will be certain they are getting correct data, advertisers will only pay for qualified leads (though brand advertisers will still be able to promote their brands with no affect to their activities), and the surreptitious stalking methods now used by data collection entities such as Rapleaf, Facebook and Intellius which produce imperfect data for marketing purposes will yield to methods that are ethical and far more profitable than the ones in place today. In fact, we believe these companies are uniquely qualified, though certainly not without competition, to work in highly competitive and innovative ways within a Personal Data Ecosystem framework where data collection companies, or Personal Data Banks, emerge to help us manage our personal data.

People have a fundamental right to know what information is out there about them, to control and correct it, and to make it available when a business entity or other service offers something. Fostering the emergence and innovation of these new tools and norms that support individuals being able to see and evaluate their own data -- to have a record of informational transactions -- as they conduct their own digital business is now possible.

Since entities all over the web and offline are now evaluating ways they can collect and use data they find about users, we users have a great need to see what we are being evaluated by, and a Personal Data Service would allow for this self assessment as well.

And since a majority of Americans now are using the internet and we will approach ubiquity in the next 10 years, fostering innovation for Personal

Data Services with user control and business and marketplace benefits makes sense. This emerging norm of PDSs allows for forward thinking approach on how to solve the problem of user protection and better data to businesses.

Individuals will be able to, in the very near future, collect and manage their own digital foot print - thus having a comprehensive picture of their digital selves.

Why should companies that aggregate data through surreptitious stalking make money on users? Why should the users not be able to deal directly with the entities that would like to trade data for services? With transparency of the data and permission-only collection, users will be able to make their own transactions directly.

Pervasive web access and mobile technologies give us the ability for individuals to store a copy of their own data sharing/release history. And why should advertisers looking for qualified leads work with 3rd and 4th parties when they could talk directly with those who solicit transactions, without having to share all their data? Obviously there will be bad-actors, but let's build for entities doing the right thing, and then manage the security and enforcement issues that come up.

A mix of legislative, regulatory, and voluntary private sector approaches is the best way to reach to this goal:

1. Regulations requiring user permission, notice and control for cross site data collection for Tracking ONLY with Notice, Permission and Control.

2. FTC enforcement through FIPPs & PPO working with industry and user advocates and privacy entities to control bad actors constructively.

3. Innovation by Industry for a Personal Data Ecosystem with Personal Data Stores, Advertisers for direct lead generation, and an applications marketplace to help users use their data in interesting and new ways we haven't yet though about today.

Question B. 1. 2) (appendix 2b) What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

One of the biggest incentives for technology companies to adopt systems is general community blessing and we support that model. However, we also suggest that a collaboration with regulators be fostered to involve them in developing and understanding the reasons for these systems.

We support a model of **Tracking ONLY with Notice, Permission and Control** for users. Within that framework, notices to users need to include some kind of simple icon and labeling system that simply communicates to users what is happening before they turn over data and some kind of standardized system for communicating user's past experiences with sites also needs development. We believe that if these two systems were made available because they were formulated via community unconferences with full transparency, disclosure and inclusion, and designed to collaboratively develop these systems, icons and the usability around them, and refinements were done through iteration with that community over time, that companies would adopt them.

We expect continual updating of PIA assessments by past users could be promoted as a way for users to evaluate a site before doing businesses with that company.

Question B. 1. 3) (appendix 2c) What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

We need a multi-stakeholder process to define the elements. This could be done through unconferences and online collaborative tools to collect input and collaborate on PIAs.

Question B. 1. 4) (appendix 2d) What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?

PIAs will make sense once we have a framework and standards. Generally, we support audits conducted in an audit marketplace, user feedback reviews and ratings, etc. However, we feel this is premature to figure out enforcement before we figure out what the basic privacy and data policy will be.

Later we would like to answer this question when we know more about what our privacy and data system will be.

Question B. 1. 5) (appendix 2e) Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

Yes.

Question B. 1. 6) (appendix 2f) What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?

Poor. Privacy policies are long and full of legalize and are completely in favor of the companies in order to limit liability. But we know that companies, including our own, can do better to make privacy policies more clear, more simple and more accessible.

Question B. 1. 7) (appendix 2g) What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves multiple sources being presented through a single user interface?

We believe in transparency, but want to work through what the system will be, before we figure out the basic UI to communicate that transparency. This feels premature.

However, user driven review systems that could evaluate and communicate the validity of systems have the advantage of being uncentralized, with the 1000 eyes watching model. The down side is that users can pass along incorrect data or reviews that may make it hard to get people accurate evaluations of companies and systems.

Question B. 1. 8) (appendix 2h) Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?

We would like to have simple tools and data visualization standards (like a red light, green light traffic model) that can support the data and privacy framework under proposal.

Many of the systems that aggregate user data are vulnerable to 'viral attack', where a bad actor provides a superficially attractive game or service, if the user hands over their own data, and then the bad actor service posts the user's information back to the network of friends to draw more 'friends' into the service. This kind of bad acting can be countered by making warnings against such actors visible on the page that asks for permission for user's data (through say, an OAuth page or an equivalent). Seeing warnings from a user's friends, trusted organizations or a weight of strangers acts as a countervailing force to this contagion. This is the 1000 eyes option that can be supported in systems to warn others, instead of creating centralized security.

Here are a couple of references to inform you about user review systems:

1. http://buildingreputation.com/writings/2009/12/the_cake_is_a_lie_reputation_f_1.html

2. http://iiw.idcommons.net/Social_Consent

When you couple these solutions with different devices, the problem becomes exponentially more complicated. We believe that with the development of more simple warning systems and some way to sum up user reviews and ratings, we can overcome the issues with multiple devices and smaller screen sizes.

2. Aligning Consumer Expectations and Information Practices Through Purpose Specification and Use Limitations.
Question B. 2. 1) (appendix 2i) Are purpose specifications a necessary or important method for protecting commercial privacy?

YES! We encourage the use of Purpose Binding when collecting data and would like to see that method used to help users understand what is being done with their data, and make companies more accountable for the reasons they retain data.

Question B. 2. 2) (appendix 2j) Currently, how common are purpose specification clauses in commercial privacy policies?

Purpose specification clauses are very common in Europe. In the US, they are not so common because there is currently no reason to say why a company collects data. But we believe this should change.

Question B. 2. 3) (appendix 2k) Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?

Icons with clear information about how data is used should be developed. Mozilla Foundation is doing work in this area and we encourage you to look to their work to inform Purpose Binding.

Question B. 2. 4) (appendix 2l) What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

Educational efforts is a great first step. Many technologist don't understand and have little experience with intellectual property, security and privacy laws and social norms. The hacker ethos is just to stay up all night and code something you need. But this hasn't worked well to protect users, and users are understandably wary. Instead, educating, showing by example working systems from Europe, and working through collaborative efforts will help technologists begin to understand how relate the ways a system works with the statements about how personal information is used and how to state finally in clearer, more practical words what is happening with a user's data.

Question B. 2. 4) (note, DOC has two question 4's so we have two answer 4s)
(appendix 2m) How should purpose specifications be implemented and enforced?

Once we have agreed on a system and standards, we can work through what the purpose specifications and enforcement. We would recommend this be done in community forums, unconferences, and inclusive online collaborative systems, when the time comes. Once we have community design and agreement, we believe that implementation and enforcement can follow.

Question B. 2. 5) (appendix 2n) How can purpose specifications and use limitations be changed to meet changing circumstances?

One method could involve giving data back to consumers at the end of transactions or a defined period. At that point, the company could ask for it again or ask for an extension?

A Personal Data Store model would also support having consumer data stored at the user's data bank, where a commercial entity would gain access

to a limited data set of permissioned by a user. Then the commercial entity would have to comply with the terms of data use that users set. This is a VRM or Vendor Relationship Model that causes the users to have more control over their data. VRM is in sync with the Personal Data Store model.

3. Evaluation and Accountability as Means to Ensure the Effectiveness of Commercial Data Privacy Protections

Question B. 3. 1) (appendix 2o) Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations? What steps should be taken if inconsistencies are found?

CEOs of companies collecting data are ultimately responsible for their company practices, as is already the case with any other regulations and requirements companies must follow.

Personal Data can be incredibly sensitive and is very valuable. Just as the government has mandated in laws governing the integrity of company's financial statements like Sarbanes-Oxley where senior executives take personal responsibility for the accuracy and completeness of corporate financial reports, so should they be personally responsible for the data safety and integrity of their users.

These laws enumerate specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance. We believe that the data and privacy framework should also have these kinds of limits and penalties.

Question B. 3. 2) (appendix 2p) Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?

YES. Technologies are available if not yet widely adopted.

Their are tools for users to capture their own usage data as it is created via computing and mobile devices. A startup in this space is working on an open source tool for this.

Personal Data Services are emerging to aggregate user data from a variety of sources. We have identified more than 8 startups in this space although there are no clear standards yet other than OAuth which supports account linking.

Personal Information Sharing Services - the flip side of Data Storage Services are also emerging they also can as as a canonical copy of particular data (a piece of information) about a person. Mydex based in the UK is doing this now for individuals interacting with local government agencies.

An example might be storing a current phone number, current address for mailing, current bio or photo. To help with the portability of data between data stores - links to data should be persistent across domains. XRI (eXtensible Resource Identifier) is an OASIS standard that links data. It works with HTML but there is a name space for this protocol that is optional - with a global registry for people and organizations.

Permission-based access to a data store is also possible with a still being developed open standard at OASIS XDI (XRI Data Interchange)

We also know that RDF is looking at changing its standards to accommodate development of systems for personal data collection.

Question B. 3. 3) (appendix 2q) Are technologies available to help companies monitor their data use, to support internal accountability mechanisms?

There is a whole set of auditing tools and suites that support companies doing SOX compliance - similar tools will emerge in this new market for data and privacy framework compliance.

Question B. 3. 4) (appendix 2r) How should performance against stated policies and practices be assessed?

Audits through a commercial audit marketplace, with FTC oversight.

Question B. 3. 5) (appendix 2s) What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?

Section C. Maintaining Dynamic Privacy Protections Through Voluntary, Enforceable, FTCApproved Codes of Conduct

1. Promote the Development of Flexible but Enforceable Codes of Conduct

Recommendation #3: Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped up FTC enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

2. Create a Privacy Policy Office Convening Business with Civil Society in Domestic MultiStakeholder Efforts

Recommendation #4: Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration's lead on international outreach on commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO would have any enforcement authority.

Question C. 2. 1) (appendix 4a) Should the FTC be given rulemaking authority triggered by failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period?

If industry is not able to produce a code of conduct that is voluntarily enforceable, the FTC should create one, with the caveat that as soon as industry does create a code of conduct, that will be used.

Question C. 2. 2) (appendix 4b) How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

Do Not Track Technologies are only one kind of technology that should be discussed and developed. Businesses that make money from valuable data need to see a way that they can still get access to data with proper oversight and user control. Technology and business processes that allow for individuals to collect their own data as they generate it in the usage of services must be developed too. These services would work not under Do Not Track, but Tracking ONLY with Permission and Control. If the only technologies developed are ones that end this economy of data, businesses will have no reason to adopt or support these efforts.

We know that pure suppression of data online doesn't work. The music industry knows that iTunes is a better model than suing customers. We can't suppress Wikileaks. The best way to get what we want is to incentivize, not suppress. To create a win-win-win for users, industry and government.

So rather than emphasize suppression as the complete model, we would recommend a model that is: **Tracking ONLY with Notice, Permission and Control**. The resulting data marketplace with Personal Data Services would be offered (there are many startups and businesses already in production, but they compete with surreptitious stalkers, so to put things on a more level playing field, we need regulation to help all parties), where businesses could track with user's permission, as long as they provide notice and control to users over the data.

Additionally, technologies such as OAuth exist today for users to authenticate without giving away their user-name and password from multiple online sites in order to pull together data. (When users give away their login and PW, it is is called the "password anti-pattern" and is very dangerous and insecure for users.)

The DOC/FTC and PPO should foster open standards development for data portability by supporting multi-stake holder open processes through events that convene key stake holders and foster progress solving key use cases. If these efforts are truly to be multi-stake holder, technical adopters in the nonprofit, startup and open source curators must be at the table along with large companies. End user advocates including those who are experts in accessibility and user experience design must also be involved. Events and industry meetings will be held, but government support will help legitimize these efforts. Government support could come through attendance, convening sessions at multiple events and providing guidance for how the Government will use industry standards, authentication and identity and data systems, in person, and in writing in consistent and open ways.

Getting open standards adopted will be the cost involved for companies who already have existing systems in place that operate in a closed way.

Open source code libraries that implement open standards in various widely used languages (that is, libraries that are free for anyone to pick up and use in their existing systems) could also have incentive prizes offered. And the commercial sector could be prize awards demonstrating interoperability between competing companies and or between different code bases running on different systems.

However, the main way we believe development will happen is if there is a regulatory and oversight change. Private investment will immediately react to fill in the gap in services that provide Personal Data Services in a much larger way than is currently being financed.

Once an open standard has industry blessing for solving a particular problem and has been demonstrated to work, offering bounties for the first 10-100 adopters in various niches of industry makes sense. For example open source social software with more then 10,000 installations on the web could have a $5,000 bounty for getting it into their core code base. A small commercial firms could also get a bounty for using certain kinds of systems to prove models early. These could be offered in different amounts depending on the stage of the company and complexity of use-case.

Though prize and bounty plans could be created as a contingency, we believe it's very likely, given the ways other ecosystems have developed as examples, that a Personal Data Ecosystem would incentivize development by open source and application developers on it's own, through private investment.

Question C. 2. 3) (appendix 4c) Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?

If there is regulation requiring that tracking only occur with user permission and control over the data, then the only new policies needed would be those to manage bad-actors who violate the letter and spirit of the law. At that point the FTC could step in with rules, or Congress could step in with additional code, to manage these bad actors. After the privacy and data system is created, failure models, enforcement and best practices can be created based upon knowing an existing framework, not speculation.

This is just too early to determine.

However, we would caution that full public transparency and involvement, including industry, user advocates and privacy entities, be included in the process determining how to control bad-actors. The PPO should maintain regular open meetings with all entities to discuss these issues resulting in recommendations to the Administration.

Question C. 2. 4) (appendix 4d) How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?

Cooperation needs to be fostered between these kinds of entities - it is essential for a successful market outcome. One way to foster collaboration that has been successful in our communities is conferences with a clear focus but without a pre-set agenda so those gathered can get real work done and exchange ideas about how to make progress.

3. Enforcing FIPPs and Commitments to Follow Voluntary Codes of Conduct

Recommendation 5. The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

Question C. 3. 1) (appendix 5a) Do FIPPs require further regulatory elaboration to enforce, or are they sufficient on their own?

Again, we are Silicon Valley innovators, who care about protecting users and making a new market that's more fair. We want a reasonable system that protects users and allows for an innovation in a business marketplace based upon opt-in participation.

FIPPs and Codes of Conduct are inappropriate to determine now until we know what our system will be. We would like that you ask for comments on this later part of the process when it is appropriate later.

Question C. 3. 2) (appendix 5b) What should be the scope of FTC rulemaking authority?

Until we know what the privacy and data system will be and what the standards will then be, we cannot determine the scope of FTC rulemaking authority.

We want FTC support for Tracking ONLY with Notice, Permission and Control. But what the enforcement and rules will be is TBD because we need to know a lot more to figure this out.

Question C. 3. 3) (appendix 5c) Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under Federal Trade Commission Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?

At this time, we don't see the current FTC enforcement methods to be a problem. FIPPs could be included with the current Section 5 jurisdiction.

Question C. 3. 4) (appendix 5d) Should non-governmental entities supplement FTC enforcement of voluntary codes?

There is a role for non-governmental organizations to provide industry the ability to work collaboratively to share policy frameworks and privacy practices transparently. NGEs can help create a market place for qualified auditors to audit/test against claimed practices. NGEs could also help with oversight of technologies and services for the FTC.

Having a marketplace of policies and auditors would allow for user to understand the level of protection their data is being protected by and having that independently verified is good. It can foster a market based incentive for good privacy practices.

Question C. 3. 5) (appendix 5e) At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval?

Potential options include providing an ex ante "seal of approval," reviewing development but delaying approval until the code has been tested and all groups (industry, user advocate and government users) agree it's workable, and delaying approval until enforcement action is taken against the code.

Question C. 3. 6) (appendix 5f) What steps or conditions are necessary to make a company's commitment to follow a code of conduct enforceable?

We agree with fines for non-compliance, as they have in Europe. We think this is the only real way to enforce statutes and possibly codes of conduct.

D. Encourage Global Interoperability

Recommendation #6: The U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' commercial data privacy frameworks. The United States should also continue to support the APEC Data Privacy Pathfinder project as a model for the kinds of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks.

The internet is global and entities, companies, individuals and other entities engaging in global interactions. Alignment and cooperation with international privacy frameworks is good for American businesses and facilitates global trade, trust and collaboration. We encourage the normalization of US privacy frameworks with other systems.

E. National Requirements for Security Breach Notification

Recommendation # 7: Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies.

Question E. 1) (appendix 7) What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?

One of the challenges with the current breach notification is that there is often no direct link between the individuals whose data was leaked and the company who experienced leaking. Those leaking entities are often data aggregators or brokers and must then do research to locate and notify by mail the data leaks. It is conceivable that in the coming next years, most individuals will have a direct data link to the companies who have information about them stored and it will be easy to notify them of this kind of breach, hopefully electronically. Data breaches of massive data sets would be reduced if companies were not actually storing massive amounts of peoples' data together but instead accessing data as needed with permission from individual's Personal Data Stores.

If *all* the data about a user only resided in one location, instead of in hundreds or thousands of locations, users would then have one "bank" to worry about, and those "banks" primary responsibility would be storage, permission and security. Innovation for PDS security would also be greatly incentivized by guidelines and

F. Relationship Between a FIPPsBased Commercial Data Privacy Framework and Existing SectorSpecific Privacy Regulation

Recommendation #8: A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather should act in concert with these protections.

(NOTE: no number given for this question.) (appendix 8) Are there lessons from sector-specific commercial data privacy laws—their development, their contents, or their enforcement—that could inform general U.S. commercial data privacy policy?

G. Preemption of Other State Laws

Recommendation 9. Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

Question G. 1) (appendix 9a) Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

National Laws for **Tracking ONLY with Notice, Permission and Control** should be broad enough to deal with any major new technology developments. A simple mandate around providing end users their data, allowing them to control the aggregation of it, or prohibit aggregation across sites, IS scalable for new emerging technologies and existing one's alike.

The data types should be defined broadly so they will be relevant to known data, user generated content (short comments, blog posts, photos, videos and any new emerging form that might be yet to developed), usage data and meta-data (data about the data - tags of photos, when they were taken etc as well as the implicit data users create when using websites).

Additionally, these rules for **Tracking ONLY with Notice, Permission and Control** should apply to mobile and other internet connected devices.

Question G. 2) (appendix 9b) How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?

Question G. 3) (appendix 9c) To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?

Again, without a data and privacy framework in place, we should not make FIPPS, and without FIPPs, we can't really talk about appropriate enforcement.

Question G. 4) (appendix 9d) Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

Unknown, until we can evaluate the data and privacy framework.

H. Electronic Surveillance and Commercial Information Privacy

Recommendation #10: The Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

Question H. 1) (appendix 10a) The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that link any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.

There are examples, like the Del.icio.us situation where Yahoo! is reportedly stopping the service, and user's are able to download a simple HTML text document of their bookmarked links, titles and notes. However, all the user's tags were missing from this document as well as the social commenting users had engaged in, when we tested the download process. Tags are a critical part of the reason users use Delicious and this removal of tags demonstrated their desire to retain the value of some of the user's work product without sharing it with users.

Another example of a data privacy problem in the cloud involved FlyClear, a company that went under in 2009. Not only were user's not returned their data, the company attempted to sell user data after the bankruptcy began. This was in direct violation of the terms FlyClear agreed to when users signed up, so a judge disagreed with the company and barred the sales. http://www.wired.com/epicenter/tag/clear/

The most concerning examples include what Facebook has done with user data, where the implement something (Beacon for example) and users blow up, after which Facebook implement changes to give users some controls or an opt-out option. We think Facebook self regulation falls short of what is ethical in dealing with users, and believe that if a basic data privacy protection framework were in place, Facebook would treat users much more fairly. For example, their recent hiring of a German Privacy Group (http://www.nytimes.com/2011/01/25/technology/25facebook.html?) shows they are willing and able to comply with good data privacy policies that are user-centric.

Facebook is also an example of an early Personal Data Store, where users can assert things, those assertions can be relied upon because users tend to perform "honestly" in front of their friends, and then those assertions are sold to advertisers in the form of characteristics that can be selected for ad presentation. However, because they don't show users what is begin presented to advertisers and partners, and do not give users control over this data, the inclusion of the data, they are not even a true Alpha of what a Personal Data Store might entail. We are concerned about the lack of

transparency, full access, opt-in norms for features especially regarding the aggregating of data from outside Facebook that Facebook aggregates with a user's profile, and the lack of ability to correct data the user didn't explicitly list with Facebook in their forms.

Question H. 2) (appendix 10b) The Task Force also seeks input on whether the current legal protections for transactional information and location information raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law. The Task Force also invites comments that discuss whether privacy protections for access to location information need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services.

We would like to see geolocation data collected from users shared with users from any and all mobile sources, and believe that this data should also be restricted from commercial use without transparency, notice, access and control. However, without a general data and privacy framework discussed early in this response, regulating (and the enforcement systems that would go with those regulations) specific types of data feels premature.

Question H. 3) (appendix 10c) The Task Force seeks information from the law enforcement community regarding the use of ECPA today and how investigations might be affected by proposed amendments to ECPA's provisions.

NA