Kaliya Hamlin
Mary Hodder
Personal Data Ecosystem

February 18, 2011

The Honorable Jonathan D. “Jon” Leibowitz,
Chairman Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

RE: Public Comments on December 2010 FTC White Paper: Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Business and Policy Framework

Dear Mr. Leibowitz:

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 our world view, and then we will comment on how this future-oriented view informs our response to the White Paper and answer your 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 nor is it benefiting the media/advertising/data aggregating complex.

On the other end of the spectrum is the mode where we leave “Business as usual” in place as it has developed over the last few years. The door is wide open for ever more “innovative” pervasive and intrusive data collection, tracking and cross referencing for behavioral targeting in 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 increasingly made from such data, and they are not aware of it, though the consequences can be quite severe. 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 modality with greater choice and control to the individual over their data AND offer greater economic value to the business community, with huge innovation and market opportunities. This market, we believe, will be much larger than the current one based upon surreptitious stalking, and be based upon an ethical model involving the user in the transactions the might occur with their data, where choice, transparency, access and control are central features for users. But it will only be based upon an ethical model *IF* there is some regulatory help to cause it to succeed.

As envisioned, Personal Data Storage Services (PDS) 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, transparency, access and the ability to correct, as well more relevant search results and commercial offers, resulting in increased value for the user from their data.

Over the last year, activity in this space has grown tremendously. In this emerging field of innovation, we have identified over thirteen startups (some of them with significant venture capital funding), at least three open source projects, several technical standards efforts in recognized international standards organizations along with companies in the web, mobile, entertainment and banking industries working on 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, the PDS 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 of 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 (Co-present and Interacted-with People in the World and on the Web)
* Objects (Co-present 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)

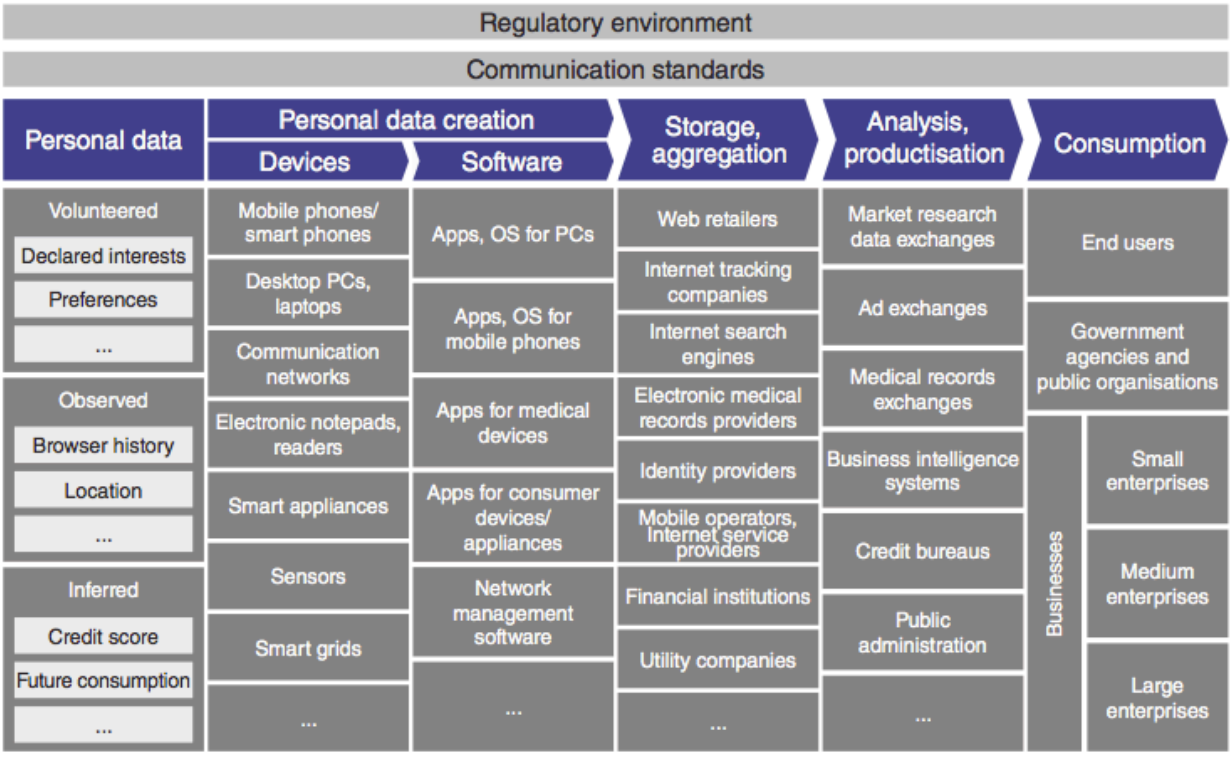
* Health Insurance Data (Claims, Payments, Coverage)

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. There is travel data including miles, trips and future plans.

The diagram below (by Bain & Co) shows how the data listed above gets used across the data systems today. As you can see, user's are not aware of much of where their data goes. They just know they don't like that they are not asked about or informed about where their data goes.

FIGURE 4: THE PERSONAL DATA ECOSYSTEM: A COMPLEX WEB FROM DATA CREATION TO DATA CONSUMPTION



Source: Bain & Company

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 service providers in the Personal Data Ecosystem are working on the user's behalf. Given the sensitivity of the data, and the complexity of running their 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 Consortium has a Value Network Mapping and Analysis project to outline this model and is raising money to support and foster the model.

Lastly, and what we'd really like to see FTC address, is a regulatory model that would significantly help the already emerging companies with user-centric data models.

With regulatory help, users would be protected, and advertisers would only pay for leads that directly related to their and users' interests. And a much larger ecosystem could emerge than the existing one where:
1. users run from the stalking and obfuscate their tracking data,
2. advertisers pay for 50% more (at least) than is necessary (partly because 35-50% of most user data they pay for is out of date, and partly because users with no interest are not detectable in the current system and therefore are "annoyed by the system" or "spammed with advertising" they don't want), and
3. because we would not be allowing a system that is "pre-market" (much like the 2007 "pre-market" sub-prime lending environment) to run away with itself, unregulated.

That new marketplace would allow for:
1. users to offer data in exchange for things of value (think mileage programs as an example)
2. advertisers would pay for leads that were valuable
3. users get ads they wanted, and would be free of stalking, where they controlled their own data within and outside of first party relationships

Frankly, a critical mass of users are mad, and they are completely justified because the system is all about stalking, and not at all about their ability to control their involvement in the system.

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 and for user's to be properly protected, it is essential that users have easy access to their data from the providers with whom they do business. 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 you a copy of your complete data.

1. Data must be available to users 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, as a few services offer, is not the answer.

2. Users must have the ability to see and correct their own data, and delete within certain bounds, at sites with which they interact. These tools are not yet created in many cases but we believe with government support, they could be developed and sites that collect data on users could then share that data with users.

2. Simple Internet Open Standards like OAuth allow for personal data stores to link to accounts without the dangerous practice of giving one's username and password to various service providers. Instead, an OAuth token is issued, with username and PW 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 managing data across providers where businesses fail. People need to be able to move their data to an alternate and hopefully more viable provider in these instances, as well as if they just prefer another provider due to different features and services available. 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.

4. Personal data stores and systems must have 4th Amendment protections that require judicial oversight in order for users to feel trust when putting all their data into a single or a few PDSs.

Data transparency, persistence and portability is critical so that as services disappear, user

data and digital assets will persist. (For example, the social bookmarking site Del.icio.us makes personal data available to users, and this capability was utilized a lot recently after Yahoo! was reported to be shopping the website). 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 FTC should recommend that Congress legislate basic data portability, together with a framework for prohibiting cross-site aggregation of data 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 users' explicit permission.

Why is 'Do Not Track' Not a Great Option?

Users want to keep their own data for various reasons, historical, self-assessment, the ability to see what others are looking at, and the ability to trade and share data as they see fit. But they want it to be private and under their control. A Do Not Track model means that it's all or nothing. Users are either tracked, or not. There is no opportunity to see, hold, correct or delete the data. There is no opportunity for users to participate directly in commercial trading or offers concerning the data. There is no opportunity to shut down tracking on other platforms than websites and give that control to users. There is no opportunity for the amazing applications and services that could be built into an enormous market for advertisers and marketers. And there is no opportunity for the market to get better than 50-65% correct data.

Why would users want to trade their own data?

They already do. For high value. For example, there are mileage programs at airlines, car rental companies, via affiliate credit cards and through hotels. 40 years ago, if the FTC had said: Do Not Track, mileage programs would have been shut down. No free plane tickets. No hotel upgrades. No fun for users.

Instead, users can aggregate their miles, from various sources, a credit card, airline trips, purchases at affiliated merchants, and turn them in for hotel upgrades, free plane tickets or upgrades, membership in various airline clubs that have private waiting rooms. These are all things that travelers value enormously. And the mileage score is kept with the mileage program, and the past history detail, after one year, is no longer available. While it is uncertain whether our mileage programs delete the data, it would be great to know that we could have a copy and then have it deleted for privacy reasons after a reasonable amount of time. But regardless of that, we have the ability to trade our scores, or mileage count, for things of great value. And the same will be true of other data scores for other things we engage in, if a PDE model is adopted.

Additionally, various businesses are using personal data to make decisions about us, and barring cross-site tracking won't stop that. Sites that have public data, such as Twitter, are available to create a score, via services like Klout.com. These scores are used by Hotels and

Life and Health Insurance companies (what we know of to date) to rate users and figure pricing and upgradability for services. Users need to be able to see how they appear to others, and a Personal Data Service would allow this picture about all our activities, much like a Mileage Score tells you what you can get in the way of free travel, etc.

So the answer is not Do Not Track. The answer is that users need to own and control their data, have easy ways to correct and aggregate their own worth via data, see it themselves, and share it when they want to. It may be that users aggregate their book purchase records across many sites. That data could then be shared with an app that helps with book recommendations and discounts on book purchases, all without having to be tracked across the web in unseemly ways. Only those interested would use the app, and work directly with marketers on offers, book stores on purchases, and in book clubs for social interaction.

What we need is to "'Create a Level Playing Field"' around Data Aggregation and Services so that users get protection, and are in control of their own data, and firms are incentivized to give us something for what we own, in a trade just as mileage scores are traded. And those trades are not about the travel detail, and the PDE marketplace doesn't have to be either. Users could choose whether to trade the detail. With a competitive market, just like there are many mileage programs and competition in the travel industry, users would have options about where to trade and what they want to do. Or they could not engage at all, as many don't with mileage programs.

How do we manage the companies managing our 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 (i.e. HIPAA data or financial data or educational data which are specifically regulated versus other personal data which is not very regulated).

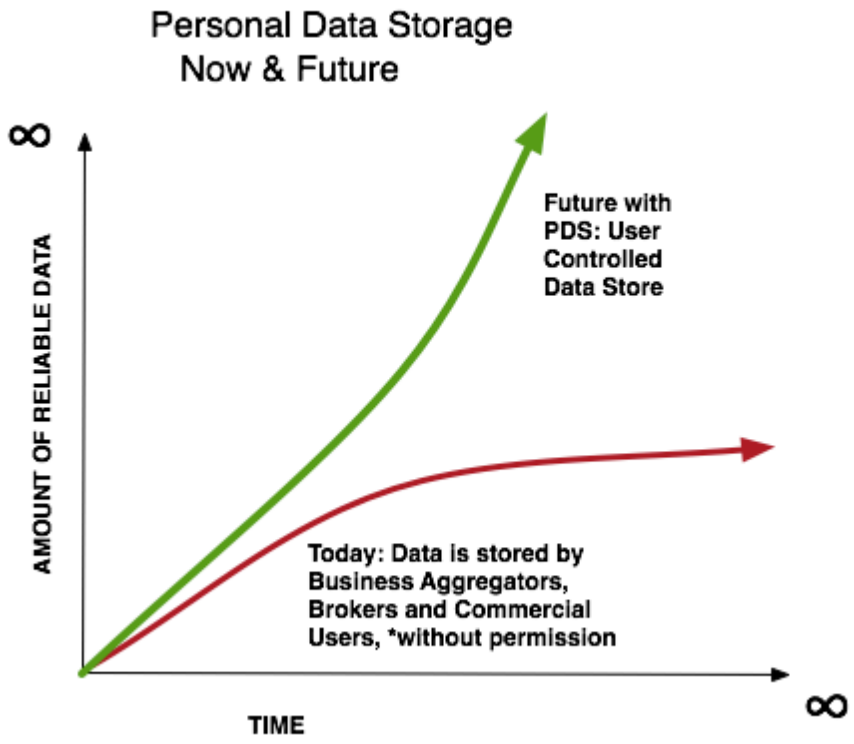
For example, Google and Facebook have vast collections of data about individuals, resulting from their activities on Google's and Facebook's sites and systems: what users click on, who they know, what they search for, where they go, etc. Sites analyze these data sets and then provide "relevant" ads based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

Today with mobile devices connected to the web, mobile carriers collect a very similar set of data - where an individual goes, whom 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 do so.
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, or not at all, 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. 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 ecosystem is personal data storage services that are totally under the control of the individual. But a user-centric identity system needs to function in partnership 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 when 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). Identity 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 (PDE) where individuals are in control of their own data, aligns with the interests of all the stakeholders that we are seeking to balance. Only the data stalkers lose.

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 geo-location data, for example). And innovation for the PDS and applications 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, Executive Director, Personal Data Ecosystem Collaborative Consortium
director@personaldataecosystem.org
@identitywoman
Mobile: 510-472-9069

Mary Hodder, Chairman, Personal Data Ecosystem Collaborative Consortium
User Advocate, Founder and Entrepreneur
mary@hodder.org
@maryhodder
Mobile: 510-701-1975

Co-Signers:

Sarah Allen, CEO Blazing Coud, Inc.
Stacy Banks, Citizen
Joseph 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 FOR COMMENT ON PROPOSED FRAMEWORK

- 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?

Users doing business with a company with sites of similar name (same domain name example: Gmail and Google search and Google docs) should expect that those sites will maintain data about their customers. This data collection should be governed by law and a site privacy policy. There would then be every reason to expect that sites we do business with, including reading, will understand and track us on their sites alone. 3rd parties should not be allowed to track us, nor should sites expect to track us after we leave their home sites to go to other sites across the web.

We advocate a regime where each company is required to show users everything the company has on the user, allow the user to submit corrections or delete data, take a copy of the data and have it a machine-readable format if the user wishes. And we advocate 4th Amendment protection for these datasets, whether they are held by the site a user does business with, or held in a personal data service (PDS) they have set up for self-tracking purposes.

We believe sites with more than 5000 users or 10,000 readers should be required to follow the

above. These thresholds would still allow for startups and innovation, and the FTC, DOC and others would be able to know when to track a site after launch.

Additionally, some period of time between adoption of the change and enforcement, coupled with contests and offerings for open source that could easily allow users to get their data from sites, would allow sites to manage user requests in an automated fashion.

For example, a Wordpress plugin could allow users to make comments on a blog over time, and the plugin could then allow the user to login and have the user's activity sent to them. Similar plugins could be developed via open source contests for other content systems that are commonly used on the web such as Ruby on Rails, Joomla, Movable Type, PHP, etc.

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

YES, we believe it's fair to address user information which can be linked to the user from a site they do business with, based upon the business conducted, in the PDE framework.

If a user visits a site, a cookie and possible login might be all that connects the user to the site; or the user should be able to state they do not want a cookie maintained.

If a user engages with a site more than just in browsing mode, for example by, purchasing something, creating a profile, or creating content, the user would then have reasonable links to the site and again, could either maintain a cookie to facilitate easy login upon each subsequent visit, or opt out of the cookie.

Users could easily understand and expect this level of interaction and tracking just within the site's purview.

However, under a PDE framework as well as a Do Not Track framework, sites would be barred from tracking the user outside of the bounds of the site the user does business with, and under the PDS framework, users would have access to their own data, the right to a copy and updates, and rights to delete and correct their data. Data that exists on other websites and platforms would not be allowed to be collected from originating site, not only through tracking, but through services like Rapleaf, which for example, have matched email address lists from companies like Facebook, to find everything about a Facebook user across the web, in order to report it back to Facebook. Other forms of collection and correlation should be prohibited as well.

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

Having a standard that applies to Personally Identifiable Information means that as companies determine that something is linkable (i.e. we take this to mean relatable back to a single person

or device) it will fall under the PDE and DNT standards. However, if we have a PDE standard as we've described above in our letter, it will mean that attributes will be selectable in an advertising system for say, an advertiser to buy, but the advertiser will never see any specific data of users who receive their ads.

Facebook today operates this sort of "attribute" sale for advertising and is an excellent model for a PDE environment. Under a PDE regime as described above, if *only I can track myself*, then I'm deciding what to share. Companies may not share data outside their own company. But if I say in effect "yes, share certain attributes with brands and sites I like", then some information about me will be available to those I share it with, and others will not be able to trade or share in my data at all.

When a website or mobile company wants to use an advertising system, they will not pass user data to the advertiser under a PDE model, but rather would have the advertiser pass the site ads with matching codes into the site or company displaying the ads. Then the site owner would use software to match the coded ads to their users. The advertiser would never see any user's data.

While some of this technology may be new to many website and mobile companies, matching technologies exist for coding types for matching. Right now many of those technologies reside with advertisers, but there is no reason a site could not buy the matching software directly and do the actual matching of a user to the ad themselves. It would require a change in how site owners manage ads with advertisers, but it would be a way to protect user data from leaving the original site. In other words, when a user is at a site, they are doing business with that site, however lightly. And the site would in turn, keep the user's data within the site, for the ad matching process using the matching tool internally against a user's data. The user would be far more protected than today, as advertising and data mining companies work to track users everywhere with technical stalking methods.

- If it is not feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device," what alternatives exist?

We believe it is feasible for user data to be protected within a single site. American companies do it for European customers now. Why can't these same companies exist in a PDE or DNT regime?

If companies were forced to give users a copy of their data, allow users to correct, delete and see what companies knew about them, and those companies weren't allowed to sell or track us across sites, we would then only have to worry about bad actors tracking and collecting data on us. At that point, bad actor behaviors could be addressed by proper security methods, the "1000 eyes" or crowd-sourcing, and other techniques to manage services and technologies acting outside the law.

- Are there reliable methods for determining whether a particular data set is "linkable" or

may become “linkable”?

In some ways, this is like obscenity: you know it when you see it. How can we systematize how a method with limited data sets can produce unlinkability to machines or people?

We do know that the more attributes about a person are exposed, the more likely they are to be identified. And we know that each person has their more unusual characteristics, so depending on which few attributes are selected, a few people will always be highly identifiable based upon the answers to those attributes.

For example: gender, age and ethnicity could be answered by these characteristics: female, 44 and white. However, a female, 73 and Inuit would likely be highly identifiable.

Every combination of attributes will produce some uniquely identifiable people.

Many in the online tracking industry as well as search firms have claimed that data such as zip code, age and gender are not linkable, and yet we know from privacy researchers’ work that in most cases, these three data points can lead to a single person. And there are other examples of claims of un-identifiability that didn't pan out.

When search firms have allowed researchers to look at search data, hiding the user’s identifying information (where the user is in the logged-in state, or via IP address, the data identifiers are replaced with a random ID number string) and claimed that the users’ identities were obscured, the few users reporters attempted to track down were easily findable and quite shocked to be found (see the AOL search data case).

The problem with attempting to make formulaic some method for determining when and how linkable people are by a few attributes or behaviors, is that some will always be specifically identifiable and so the formula will fail.

Instead, we strongly recommend the PDE regime defined above. That regime would allow only users to aggregate their own data, and then to control to whom and when to release data about themselves when they want to... only users can judge which sets of personal attributes will lead back to themselves every time. And those unique attributes can then be kept private. The PDE regime would allow users to mimic what we've done in real space for eons: keep private what we want to and release what we feel comfortable releasing when we feel comfortable about it.

Under the PDE regime where users are the *only* ones who can track themselves from site to site, and release their data as they wish, we would be far less concerned about the linkability of data back to users because users would be in control of it, and sites would not be able to share it offsite.

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

Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Obviously, "designing for privacy" is a key component so that these protections are built in early, but without the regulatory help around the edges (prohibiting anything but self-tracking, and sharing only with permission). There are various measures used within companies to keep identities from being passed around and employees knowing user identities, but these are created and maintained on a case by case basis. There is no open source code that we know of that is specifically designed to anonymize users within a system under all circumstances.

Incorporating substantive privacy protections, such as a policy that says "only I can track myself across sites" in a PDE framework would go a long way toward incentivizing the development of technologies that would work to anonymize users in real ways. Additionally, we advocate contests and incentive programs to get engineers to create open source code for use in systems that will help "privacy by design" from the beginning.

- 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?

Yes. Companies should be forced to share all data the company has on a user, when asked for by that users, and continually after that, if requested. Companies should be required to allow users to see all the data collected on them, and to make that data available for collection or deletion (with the exception of recent information, or information such as account name and profile data in order to keep the account open). Data should be able to be kept for longer than a default retention period, if the user asks, if only in score form; think of mileage accounts where the user has a mileage score that can relate mileage that is several years old, but where the details of where the mileage originate from disappear after 13 months.

It seems reasonable, regarding Section V(B)(1), that data on users should be collapsed after a prescribed period, so GPS data could be kept for 6 months, search history 9 months, social media trails for 9 months, etc. But those kinds of details need to be thought out carefully, and likely with people in industry and in *user* roundtables to get it right. Then, collapsing the data (as the mileage example shows) would mean that a user could, for example, have numbers of visits to places shown, but not when or how; and would then be able to delete, say, visits to a therapist, or visits to home, if they wanted a home address kept out of their records. Social media data with specificity might be kept in a Personal Data Store that was older than a retention period would otherwise specify, but the service might only show the number of entries a person had made (Facebook status updates, as an example) prior to the retention period specified. So if a person had 4,000 status updates prior to the last year, that score could be shown to the user, but the actual status updates would be deleted, as well as fed into the user's Personal Data Store if that user desired it. Then the user could decide whether to make those status updates public, or keep them, or later to delete them. But ultimately, the user would have complete control over their own entries.

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

Yes.. some definitions should be clarified and businesses should be required to post the reason they are collecting and storing data, and share that with users when they share all the data they have with each user.

Purpose Binding should be enacted, so that individuals can find out whether data stored about them has a purpose, and whether it was collected and maintained properly. If it was not, 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 a company lists - 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.

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

Users should be able to choose this within certain limits. Most businesses would likely want to keep 6 months to a year of detailed data, however, if a user wants to get all their data and move it, they may want to ask for anything a business has, even collapsed data, from as far back as can be found. After users have had a chance to get their data, then it would make sense for businesses to keep data for that shorter period.

- Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?

The value of behavioral data does decrease over time, but data submitted by users in many cases would likely remain effective in a profile. Geo-location data also would decrease in value. There are many kinds of data, and the user should be given the choice about how long to keep data, when feasible.

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

All parties need to support open source data deletion and retention software, so that legacy data systems can be cleaned out. Additionally, open source data deletion and retention systems need to be created for current and future data management. These open source software programs could be made through contests, much like the $25m contest system the Obama Administration just announced on 2/17/11 for other software development they know are needed for various reasons.

- 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?

There are situations where systems are not able to update, collapse into non-identifiable data, etc. Companies should then be required to delete old data, when feasible. If they are found to be selling old data that falls under this category that should have been deleted, there should be penalties depending.

- Can companies minimize or otherwise modify the data maintained in legacy data systems to protect consumer privacy interests?
Maintain comprehensive data management procedures

It depends. Depending on the types of data collected, the types of backups and legacy systems, the kinds of staffing resources (think startups that remain in a zombie state, and that cannot pay staff to delete only data or to write the code to delete, for example), companies may not be able to delete old data. However, what they can easily do is destroy old data and be penalized for selling it or doing anything with it other than destroy it. The key is to figure out what is reasonable, and then penalize the selling of old data.

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

Contests, open source challenges, education, workshops held by private entities for learning about building for privacy including old data management, etc.

- 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?

Rather than trying to control an arms race with browser controls for the suppression of data, relying on website operators and advertisers doing the “right thing” because they are “self regulating,” we need to face facts that entities will collect and sell data if it’s legal. Those that operate outside the bounds of the law can be dealt with via enforcement, but most players will, given strict prohibitions and penalties, follow the rules.

We need government regulation to defend user rights, so that companies and other entities play fair with user data and put users back in a position that considers their needs and wants with their own data.

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

The list is reasonable, but considering that new technologies are developed all the time, it

seems that defining data as “commonly accepted” from users compared to data that isn’t a commonly accepted practice is short sighted.

Rather, we recommend that you require that sites share all data they collect from users, with the ability to correct, delete and have their own copy. If you did that, sites would find that sunshine and user attention would cause they to either make a good case for whatever data collection they are doing, or shut it down.

Let’s get users interacting with their data and let them decide what is fair. If it’s outside the bounds of 1st party interactions, or the policy of having users receiving, correcting and deleting their data, data collectors would then be subject to FTC rules and penalties.

- Are there practices that should be considered “commonly accepted” in some business contexts but not in others?

The practice around users’ data that should be commonly accepted is one where users’ data only stays within the 1st party business. And that users get to see, hold, touch, delete and correct their own data.

- What types of first-party marketing should be considered “commonly accepted practices”?

Any data collection that occurs on a single site in the short term (within the time frames where data collection is agreed to be reasonable as addressed in another part of this letter) would be reasonable, as long as the business is required to turn over all data collected to the user. This would include tracking the user, collecting data from interactions on and with the site, and that the user has the ability to delete, correct and hold the data.

With that in mind, if a site then used data they had collected as a 1st party to a user, to apply some kind of advertising matching to the user, within their own company bounds, that would be reasonable.

The key element of a scenario like this is that the 1st party to the user would have to maintain all data, share it with the user, and do the matching themselves internally with tools, instead of allowing the user data outside the bounds of the company, and the user would have notice and the ability to correct any data about themselves.

- 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?

Yes. If companies are required to share any data they collect about a user, and the user is allowed to correct and delete data (deletion should probably be constrained so that fairness is preserved for the company in terms of their ability to manage the situation reasonably), then users would have choice about how sensitive data is used for marketing.

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

For sites with multiple platforms (web and mobile and in person, for example) using data only in one context seems onerous for the business and not great for the user. Users expect that when for example, they purchase something at Apple.com, then receive it in the mail, set up services and buy apps on their Apple device, and then go into the Apple store, that Apple has the user's records and purchases together and is ready to provide service. Limiting that would be ridiculous. As would limiting a mobile and website carrier from advertising based upon their interactions with a user. For example, if a user checks in at a location via mobile device on Foursquare, and uses the Foursquare website later offers the user a deal based upon the mobile check-in, that too is completely reasonable. Where it gets creepy is if the location company were to sell that data to an advertiser, and later a location-matched advertisement were to show up say, in a web search on Google. Not good. However, if user data collection is limited within a 1st party business, then we are fine with multiple contexts.

We would recommend that as long as the user has access to their data, the ability to delete and hold it, all the data collected from a 1st party should be allowable to use for advertising purposes within the bounds of the 1st party's platforms in all contexts where that user deals with that business.

- 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 first-party marketing. An analogous offline example would include a retailer offering a coupon to a consumer at the cash register based upon the consumer's prior purchases in the store. 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?

No.. all first party interactions are okay as long as they are based upon a first party relationship with users.

As stated before, we believe that if users have rights to see all data collected about them, to hold it, correct it and delete it, easily, that problem businesses will be strongly incentivized to fix their practices or risk losing customers.

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

If Google markets GMail, I don't think users would have a problem with it -- it's all a part of the same business. But if the business isn't owned by their "affiliates" even if they make a marketing deal to share a brand, we believe first party data on users shouldn't be shared.

However, if users are asked to have their data shared with an “affiliate” and a user agrees, then it would be okay to share the data, because the user had given permission.

- 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?

This practice should be strictly prohibited. If a user wants to share more about themselves than they have already with a business, that business might ask the user if they can have additional data, and may even offer the user something for the shared data.

What, for example, Facebook does now, as they share our email addresses with Rapleaf, a data collection company, and Rapleaf then matches those email addresses using the apis of other companies to “find” the user in other places so the user can be matched, is unethical and not what the user expects when they go to a site and provide an email address for login to the site.

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

Sites could “ping” a user (contact them in some form as the user has indicated they want to be contacted) at his or her data bank, where the user may decline to answer such requests, decline that particular request, or accept the request for information.

Or, a first-party site could make the request through the platform they currently use to interact with the user.

Since personal data stores are currently being developed by sites like Personal.com and Mydex, methodology for such requests is not yet a practice that we can point to, but we expect within 12 months, when the FTC intends to answer these responses, that there will be methodology.

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

Yes.. it would make sense if a first-party site were to use the context and platform where they regularly interact with the user. However, given that personal data stores are in development, it will likely happen that common requests for data will also happen within the context of the PDS.

- 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?

If only first parties are allowed to contact users to ask if an affiliate can have the user's data, it would make sense that using the 1st party's platform would be acceptable. Being contacted directly violates user expectations and if, as we recommend, only 1st parties can contact the user, then using whatever methods the user has interacted with through platforms already used makes sense.

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

A uniform icon or graphic for conveying to the user that a *new* request by an outside or "affiliate" party through a first party for the user's data is being made could make sense and would likely tell the user that this is not a 1st party request for data.

- 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?

There was a survey done by Krux Digital recently which showed that: "... 52% of adult respondents said they already take 'an active role in managing their digital signatures.'"

Mediapost goes on: "The Krux survey found, not surprisingly, that 85% of respondents would use centralized data management tools to control their online profile if they were available. If these numbers are even vaguely accurate, then consumers want something from the industry that it is far from providing: a true one-stop privacy shop that affects their data signature everywhere."

Reference: Media Post, Will Consumers Take Charge of Their Own Privacy, January 21, 2011, https://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=143436

We believe that this indication of user interest in a single stop for privacy and data control is key. And the Personal Data Ecosystem will foster a way for users to manage their data and privacy, through personal data stores.

We encourage you to take a look at the following startups doing work in the Personal Data Ecosystem, as evidence that Personal Data Stores are what is coming. What's needed from the government to help this along is a little regulation around the edges, for user's the own and control their data, be able to correct and delete it, and to prohibit 1st parties from sharing that data. If user's feel confident with 4th amendment protection of these data stores, they'll use them to protect their privacy and data without further intervention from the government.

Here is a list of the companies doing something in the Personal Data Ecosystem:

Data Storage, Collection and Sharing

Personal.com has raised 7 million in venture funding and although it does not yet have any services, their website articulates clearly how personal data will be under the control of the user in a value marketplace.

Mydex is a Community Interest Company (based in the UK) has begun a community prototype that connects individuals' personal data store accounts to local government agencies.

Singly Jeremy Miller's startup to build apps based on data from data stores built using the Locker Project code base -- an open source project for collating, securing and sharing personal data .

Statz is a startup that supports a user pulling in her information from different service providers including mobile phone records, energy and utility records, health and fitness, shopping and payment and transportation records. Statz gives you instructions on how to go into your mobile carrier or electric company and export your statements - often this involves a dozen steps and is very labor intensive - not something easy or that everyone will do.

Greplin does "Personal Cloud Search." When people set up Greplin accounts, they give the service access to a range of accounts - LinkedIn, Gmail, Basecamp, Flickr, etc. Then users use the Greplin engine to search across them.

Backupify is an "all-in-one archiving, search and restore service for the most popular online services including Google Apps, Facebook, Twitter, Picasa and more."

Switchbook helps "manage user-driven searches across multiple search providers and websites, creating a powerful new way to explicitly express search *intent* anywhere on the Internet."

Trust Fabric provides "Vendor Relationship Management (VRM) infrastructure. Businesses use CRM to manage customer relationships, while VRM lets individuals manage their relationships with businesses. TrustFabric writes Open Source software and gives customers a platform to represent their side of the VRM+CRM relationship. TrustFabric is based in Cape Town, South Africa."

Allow helps "you to stop unwanted marketing and to get in control of the way your data is used."

Cloud Inc (Consortium for Local Ownership and Use of Data, Inc.) "A non-profit technology standard consortia started in early 2009 that believes that a new era of ME 1.0 is at hand, an era that looks beyond Web 2.0, while simultaneously looking to the founding principles of the Internet as the solution to many of today's most vexing issues of privacy, security and data."

Data Inherit **"**Data Inherit online safes from Switzerland offer individuals around the world highly secure online storage for passwords and digital documents. You can access your online

safe using any Internet browser or an iPhone from anywhere and at any time. In addition the unique data inheritance functionality will protect your data in emergency situations. Simple and convenient."

PDS Verticals Acting for Particular Areas of Interest

Mint -- "Mint brings all your financial accounts together online, automatically categorizes your transactions, lets you set budgets and helps you achieve your savings goals." Mint was a startup recently purchased by Intuit Inc. for $170m.

Dopplr -- social travel interaction with all a user's travel data from across travel providers.

Trippit -- similar to Dopplr.

Shwowp -- aggreggates all a user's shopping data in order to share it when the user wants to do so.

New Application Building and Design Tools

Kynetx is "developing a new language that looks at data from personal data stores and public datasets and can do real time matching based on rule sets created by the individual to surface relevant content."

Emancipay "EmanciPay is a relationship management and voluntary payment framework in which buyers and sellers can present to each other the requirements and options by which they are willing to engage, or are already engaging. Including choices concerning payment, preference, policies."

Open Source Projects for PDS

The Higgins Project

Project Danube

The Locker Project

The MINE! Project

Project Nori

Industry Initiatives

Persme end-user advocate known as Identity Woman online, and cofounder the Internet

Identity Workshop.

Project VRM at Harvard led by Doc Searls focused on developing Vendor Relationship Management Tool

World Economic Forum Rethinking Personal Information effort - limited links online to this - there is a video from this latest forum. Yesterday the World Economic Forum released their analysis of the Personal Data Ecosystem and called personal data a "new asset class."

Personal Data 2.0 analysis area of STL Partners

Events on Personal Data:

Internet Identity Workshop - May 3-5, 2011 Mountain View

ID Collaboration Day - February 14th, 2011 in San Francisco

New Digital Economics - Personal Data Ecosystem Deep Dive Day - April 7th, San Francisco

Kynetx Impact

- 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?

If first parties were required not to share data, other than with the user in order that the user were able to have a copy with updates, and delete, correct their data, we would find no fault with a "take it or leave it" proposition where users were required to adopt the sharing of their data with the 1st party in order to use the site or service or platform.

However, without the above protections, all sites and services will continue as they do now: requiring users to give away the farm in order to use the site. This IS the status quo now.

Part of the requirements we have outlined where users own their own data and 1st parties can't share it outside of their relationship with the user, or those the user permissions (others on the site such as "friends" or "followers" etc) means that the user cannot "give away" this right in order to use the site or service.

- 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?

If you level the playing field and force all sites, by law, not to share data or obtain data offsite, it would be very clear to users because it would be the law. Then privacy policies would be a

whole lot different and user's wouldn't have to be lawyers to understand them.f

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

If a personal data system with data regulation as we have outlined above existed:

Each site could say, "In exchange for using the site, you consent to give us your data licensed to us while you are here, and we will share with you a copy of this data, for your use, deletion or correction. And we will, by law, not share your data outside of our business."

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

Yes, if we had a law that protected users by giving them rights to their data, where sites had to provide a copy to the user, agree to allow the user to control, delete, and correct it as necessary, and to not share the data outside the business, and to not aggregate other data from outside the business (first party) relationship.

- 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?

Users will know when something is sensitive. Given a law that protected users by giving them rights to their data, where sites had to provide a copy to the user, agree to allow the user to control, delete, and correct it as necessary, and to not share the data outside the business, and to not aggregate other data from outside the business (1st party) relationship, users could decide to delete, protect or otherwise consent to sharing "sensitive data."

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

If sites are not allowed to collect data outside of their 1st party relationships with users, we could expect that deep packet inspection for the purposes of collecting data on users would not be legal.

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

There are special concerns for kids and teens. However if we required that user data stay with a first party unless a user decided to receive her data for use in a Personal Data Store, we believe kids and teen issues would be mitigated.

- Are teens sensitive users, warranting enhanced consent procedures?

Yes.. they are sensitive and in many cases using more of the currently available privacy and data controls on sites than adults. However, with the data protections we are recommending, we believe this issue would not be a problem.

- 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?

We are concerned with sites sharing with other sites, beacons and flash cookies and tracking that is unexpected in the eyes of a user. If a site decides not to allow teens to share their information with “everyone” that is the decision of the site owner and the users, if that site is otherwise following the law.

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

Sites should not be able to collect data if they are not a 1st party site. It should be illegal, because the user does not have a relationship with the company collecting the data. If that company wants to work with the user, the company would need to ask the user for permission to collect data on them.

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

Data brokers in a Personal Data Ecosystem regime as we have proposed would likely become very good Personal Data Stores, with direct relationships with users in order to store their data with permission. Once the user has agreed to storing their data with a Personal Data Store, they will have a 1st party relationship. At that point, users will be able to take their data with them, delete it, correct it, and otherwise share it by choice for their own benefit.

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

Behavioral advertising conducted only with 1st parties a user has a relationship would not be troubling. At that point, the user has already made the choice to do business with the 1st party. If the user chooses to leave and delete their data, the 1st party would be required to go along with the user’s choice about the user’s data.

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

We need to make a wholesale change in the law so that user’s are not stalked as they are today, and their data sold and traded without their permission.

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

We believe that given the regulations we propose, that private companies would standardize on mechanisms that user's could understand.

- 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?

Private companies should be charged with this task, with the government only getting involved in nefarious cases of deceptive practices.

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

It is helpful for users to find standardization in anything, especially digital interfaces. However, we believe this is best left to the marketplace to determine, as companies who want to do the right thing, by following the rules, will work to make standard user interface conventions happen.

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

We believe that users who trade their data in a Personal Data Ecosystem will then happily receive targeted advertising based upon the transactions they sign up for, while in a system without user choice and control over their own data will produce unhappy dissatisfied customers as we currently find in the marketplace.

- How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?

We believe those numbers to be between 30-50% depending on which opt-out tools and surveys you look at.

From Mediapost's recent report on the Krux Digital survey: "A .. sizable number (38%) say they use opt-out tools. Now, those opt-outs could refer to anything from an email unsubscribe button to visits to the NAI ad network opt-out resource. But the basic statistic suggests there is a sizable interest among consumers in having a degree of control over how their identity is used online. The survey also showed that 30% already use the 'private browsing' feature."

Reference: Media Post, Will Consumers Take Charge of Their Own Privacy, January 21, 2011, https://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=143436

- 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?

From the Media Post article referenced above:

“One of the interesting insights the Krux numbers suggest is the value of the first-party publisher relationship in establishing trust in online privacy. The survey found that 86% are fine with the idea of viewing ads in exchange for free content. It is within that context that we need to better understand where users place their trust in this value exchange and the degree of intrusiveness they are willing to accept. For instance, 57% of respondents said they are accepting of data tracking and ad targeting on a specific site. That is, they are most accepting of data tracking when it involves a content brand they already know.”

We believe that users expect data to stay within the site they interact with.. the first party. After that, users will want to opt out. If a site wants to advertise, they will need to purchase tools to use in-house, under the regime we propose where data can only stay with the first party.

Reference: Media Post, Will Consumers Take Charge of Their Own Privacy, January 21, 2011, https://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=143436

Rather than function in an opt-out system where many users will avoid ads and create blocks to tracking that won’t really work long term, we recommend that a personal data ecosystem will solve the problems users face, advertisers face (up to 50% of the data they receive from the data stalkers is bad.. they just don’t know which 50%), and you face in trying to regulate data practices could be solved by it. Yes, many will have to change and it will cost the industry, but ultimately, the changes will bring about a much larger marketplace than currently exists where users run away, obfuscate and lie, and attempt to block via an arms race the tracking and ads they don’t want.

The system isn’t really serving anyone but the data stalkers. Let’s fix it in favor of advertisers who want better more reliable leads, users who want more relevant ads and to stop the stalking and have more control over their data, and government who needs to protect citizens in useful and real ways.

- 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?

We believe this is unrealistic. If a site needs to make money to provide content, and it does this with advertising, then shutting off all ads will cause the site to fail. Rather, limiting data collection to what they site knows just from a 1st party relationship will be enough to allow an advertising model to work, if they run the advertising tools themselves for matching.

Regarding granular controls for more targeted ads, users would give permission for some datat to be released through their personal data store relationship. The user would consent to share

selected data with the site but at the point where the user wanted to turn this off, they should be allowed to end the relationship, and no longer provide data.

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

Yes, if users' data were theirs to put into their own personal data store, this would a universal mechanism for choice where each user would control what they share, with the understanding that they ultimately own their own data, and share it via licensing with site and services.

At that point, no matter the platform or use, the user is put into a more equal position with the service, and services will be forced to respect the user's wishes and provide services, ads and content that is actually useful for the users they wish to attract.

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

Yes.. data should be regulated as we have described repeatedly above, so that user's own their data, and the marketplace can then react by providing personal data stores, applications and advertising mechanisms that respect the new arrangement, and

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

We believe that if users were in charge of their data and therefore the attendant privacy, all industries would have to change. Changes in technology would accommodate this new paradigm and as new technologies were developed, this new data and privacy regime where *only users can track themselves* and *user's control their own data* would lead to standards around user's sharing data when they wanted to.. and services that were nefarious would then be more noticeable and findable. However, we understand that the change over period would be difficult and would take time in order to establish new norms for this shift in understanding.

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

If we change the rules around data collection and control in users favor, where user's would expect their data would stay within each business and not be shared without permission, and users could expect a copy with updates of their data, and the ability to correct and delete data, then this universal change would mean sites would not be responsible for creating messaging that said anything other than what the law said. At that point, sites would simply explain, through written communication and user interface mechanisms, how the user's data would actually work on their site.

- Should companies increase their use of machine-readable policies to allow consumers

to more easily compare privacy practices across companies?

Yes.. but sites also need to accept incoming “link contracts” that permit data to be shared with rules from user’s data stores. Machine readable policies will become a critical part of the Personal Data Ecosystem.

Reasonable access to consumer data

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

Yes.. reasonable costs for access to goods and services is reasonable. Those costs could be about sharing data from a user’s data store, or be charged in dollars.

- 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?

Yes.. and there should be a log of it turned over to the user’s personal data store, much like those who check credit are listed in a credit report.

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

Yes.. parents and legal guardians should have access to kids information, and some teens depending on age.

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

No.. all entities that collect any data should be subject to the same rules. As open source projects and contest produce code that will work in all common publishing systems (such as Drupal, Joomla, Ruby on Rails, Php on Rails and other frameworks, Wordpress, etc) all collectors of data will easily be able to put in a module that allows users to see what has been collected on them and to take a copy, correct and delete what is there, if the user gives authentication. These tools need to be built, but like any other code, there is no reason they cannot be produced.

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

Companies that do not do business with a customer should not have a user’s data.

We do expect that a change over period would occur and during that period, it would be reasonable for companies that currently collect data surreptitiously on users to ask the user if they would like the company to be their personal data store. If the user does not, the company would have to delete the data.

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

Yes.. companies that have shared data would need to provide a list to users of the data and where it has gone. If that sharing has occurred further back than a short period, and the site no longer knows where the data has been shared, we would expect that a cut off point would need to be utilized so that we would only work on this problem with a short history and then look at the problem going forward.

- Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?

YES! Users should ALWAYS be informed if anything is denied or changed due to a score or evaluation of data that has been provided. This notice should be available at the user's personal data store. Once this log has been developed, these notices should be inexpensive to provide via the Internet to a user's data store.

Material changes

- What types of changes do companies make to their policies and practices and what types of changes do they regard as material?

Companies would have to use advertising matching in-house, would need to establish ways of managing user's data that conformed with the user's wishes as established in the contracts that go along with any shared data and would have to abide by rules about sharing a user's data with them, and allowing the user the ability to correct and delete data if the user wished.

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

Sites should be required to give user's 30 days notice of changes in writing, and users, given the ability to take their data, correct, delete and otherwise manage their own data, would be in the position of deciding whether to continue to use the service.

Consumer education

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

Changing the law to allow user's to hold, correct and delete their own data, and share it in personal data stores that provide them privacy and control would go a lot way to demonstrate to users how to manage their own privacy.

People are pretty good at managing their privacy in real life. The issue has come up because in digital space, users are not aware of the stalking done by companies for advertising and other purposes, until something bad happens or it makes the press. User's are mad. And they have a right to be given what's happened.

The best way we can educate people is to start protecting them and their data, and then let companies offer services that conform to the new laws. Then privacy policies won't matter so much, and user's can understand their rights because they are the same for everyone.

Right now, we are "pre-market" where users are unprotected. We need to get to a point where user's are protected. That will cause digital interfaces and interactions to evolve. In the digital realm, the best way to get someone to understand something is to have them use it.

Using a personal data store, where users' data is regulated by law, coupled with a marketplace the user can trade and interact in, will go a long way toward making it clear what is happening with a user's data, because the user will have control, will see when they make changes or delete data, or turns off access to a company.

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

Government and industry associations should be very involved in educating businesses as well as providing resources.

Government should run contests to create code supporting user's right to their data as has recently been announced by the Obama Administration for coding initiatives.

Industry associations should get involved in the process of training companies to understand and build for privacy all the way along the development process, through workshops, conferences and other information dissemination means already engaged in now.