Comments of the World Privacy Forum

Regarding the Request for Information for the National Privacy Research Strategy

From the National Science Foundation
(Federal Networking and Information Technology Research and Development Program)

Sent via Email: nprs@nitrd.gov

National Science Foundation RFI
Attn: National Privacy Research Strategy.
NCO, Suite II–405,
4201 Wilson Blvd., Arlington, VA
22230

October 17, 2014

The World Privacy Forum is pleased to have this opportunity to respond to the request for information from the agencies of the Federal Networking and Information Technology Research and Development Program regarding a joint National Privacy Research Strategy published in the Federal Register 79 FR 56091.

The World Privacy Forum is a non-profit public interest research and consumer education group. We have published many research papers and policy comments focused on privacy and security issues. Much of our work explores technology and health-related privacy issues, biometrics, consent, data analytics, and many other rapidly evolving areas of privacy. You can see our publications and more information at www.worldprivacyforum.org.

I. Foundational Principles: Privacy Rights, not Harms

We were pleased to see this statement in the RFI:

> Respect for privacy is a cornerstone principle of our democracy. A variety of laws and policies guide collection and use of data by the government, corporations, and organizations. However, because technology advances can outpace law, respect for privacy must be a guiding principle in the technological domain and our information systems must be designed to provide the means for protecting privacy.

The paragraph that followed this which focused on privacy harms to individuals as a way to evaluate privacy was much less pleasing. An evaluation of privacy harms can be appropriate in a privacy discussion. However, the principal focus in those discussions should be on **privacy rights and interests**. Individuals have rights to privacy and interests in how their personal information may be processed (collected, maintained, used, and disclosed) that exist whether or not the processing results in harms.

Processing of personal information must always take into account the rights and interests of individuals. We note that some data processors prefer to focus privacy discussions exclusively on harms so that they may process personal information as they please unless and until a data subject can prove tangible harm in a court of law. We reject that approach to privacy, and we urge that any National Privacy Research Strategy start with the focus on rights and interests.

As individuals live in a world of connected cars, biometric controls, most daily financial transactions recorded via debit or credit cards, and other digital collection spots. There are legitimate research uses for much of this data. However, it is essential that individuals have rights to shape their digital exhausts. Otherwise, individuals lose much personal choice, and this can ultimately be limiting in a democracy, and much worse in non-democratic states. Researchers have a stake in privacy as well. Without suitable privacy rules, the public will not support research.

II. Scenarios that Illustrate Critical Issues in Privacy: Statistical parity, scoring/modeling, and granular consent / electronic consent

The first request in the RFI is to "Describe one or more scenarios that illustrate a critical issue concerning privacy…." We read this question as an attempt to understand what privacy concerns are arising and not being (adequately) addressed. Given that this is our interpretation of the question, here are our key responses.

As a baseline of understanding, we want to reiterate the necessity of analysis and work based on the foundation of Fair Information Practices (FIPs). Whenever someone processes personal information, that processing creates raises critical privacy issues. FIPs are the basis for privacy regulation throughout the world. All eight principles are critical. We recognize that not all implementations of FIPs should be the same, and that some implementations may place more emphasis on one or more of the FIPs than on others. However, all implementations should address the same principles.

We view FIPs as a process-oriented set of protections. We understand that additional protections may be necessary. However, to be clear, we see modern privacy as a series of overlapping protections built with FIPs as a base, and the additional protections layering over the top of FIPs. We will discuss this idea much more through these comments. One important aspect of what is missing is something we call "statistical parity," which we will discuss at length next, among other critical issues we see that are not being addressed.

"Statistical parity" and its implementation

There is an urgent need to discover the most important aspects of **statistical parity**, and what

that looks like and how that can best operate to enhance consumer privacy. Statistical parity is a term we coined at the FTC's *Big Data, Tool For Inclusion or Exclusion*? workshop in September 2014. Here is our definition of the term:

Statistical parity means ensuring that all parts of the consumer data analytics process are fair: data collection, which data factors chosen and used for analytics, accuracy of the factors and how well the algorithm works for its intended purpose, and then how the final results are vetted and used, and for how long. Statistical parity means finding ways to ensure privacy and fairness in the analytics process from beginning to end, and to ensure that decisions about consumers are accurate and used fairly and in a non-discriminatory way.

Nowhere is the need for additional work in the area of statistical parity clearer than in the context of consumer scoring and predictive analytics. Consumer scores are simply the outgrowth of a robust and growing market and use of predictive analytics. But as modern statistical shorthand, scores are important. We published a substantial report about this issue in 2014, *The Scoring of America* <http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/>. In this report, we outline in depth the policy issues around a lack of privacy protections and fairness in analytics, consumer segmentation, and predictive consumer analytics.

We define a consumer score as follows:

> A consumer score describes an individual or sometimes a group of individuals (like a household), and predicts a consumer's behavior, habit, or predilection. Consumer scores use information about consumer characteristics, past behaviors, and other attributes in statistical models that produce a numeric score, a range of scores, or a yes/no. Consumer scores rate, rank, or segment consumers. Businesses and governments use scores to make decisions about individual consumers and groups of consumers. The consequences can range from innocuous to important. Businesses and others use consumer scores for everything from predicting fraud to predicting the health care costs of an individual to eligibility decisions to almost anything. Dixon/Gellman, *Scoring of America,* p. 8.

Many thousands of scores exist, yet consumers have scant rights to find out what their non-Fair Credit Reporting Act scores are, how the scores apply to them and with what impact, what information goes into a score, or how fair, valid, or accurate the score is. Even if the input to a score is accurate, consumers do not know or have any way to learn how information derived from their lifestyle, health status, and/or demographic patterns is used to infer patterns of behavior and make decisions that affect their lives. Those who create unregulated scores have no legal obligation to provide Fair Information Practices or due process to consumers. This in totality is what we mean when we talk about ensuring statistical parity.

We would like to flesh out this concept of statistic parity here with a few specific examples/scenarios. We think that those who are making decisions about research strategies and research agendas need to know what is happening is the real world *today*.

Scenario 1: Data segmentation / categorization and privacy and fairness challenges

When individuals are placed in a category, the very act of categorizing that individual automatically triggers privacy and fairness concerns. Categorizing or segmenting data may bring **helpful or non-helpful consequences** to the individuals in the data. This is a much-studied and well-known issue, for example, see Cynthia Dwork's work on fairness in categorization, *Fairness Through Awareness*, Dwork, Hardt, et al., arXiv:1104.3913v2 [cs.CC] Nov. 2011.

The categorization may be based on marketing data, and as such may be highly inaccurate. The categorization may be based on information typically protected in other statutes, such as race, age, and gender, or on proxies for that information. The categorization or segmentation could be offensive in many additional ways. For example, a categorization of someone as mentally ill, or as a compulsive spender could put an individual into a category that is socially stigmatized. If inaccurate, that is problematic in and of itself. And whether inaccurate or accurate, that categorization could result in positive and negative consequences for that individual. We give you a specific scenario for this occurring in the real world.

A major US health insurer worked with an analytics company to determine whether or not publicly available consumer data could enhance the quality and effectiveness of their predictive risk models. They tested approximately 1,500 factors at the household level and found that the consumer information that showed the most value in predicting individual level risk included:

- Age of the Individual
- Gender
- Frequency of purchase of general apparel
- Total amount from inpatient claims
- Consumer prominence indicator
- Primetime television usage
- Smoking
- Propensity to buy general merchandise
- Ethnicity
- Geography – district and region
- Mail order buyer - female apparel
- Mail order buyer - sports goods

Those unfamiliar with predictive models can find it surprising to learn that information about purchasing sporting goods can become a part of a predictive risk score for a health insurer. Yet it is not unusual to find the factors used in this example are in a modern predictive consumer score model. This is actually a fairly short list compared to some models with thousands of factors. This example comes from Satish Garla, Albert Hopping, Rick Monaco,& Sarah Rittman,*What Do Your Consumer Habits Say About Your Health? Using Third-Party Data to Predict Individual Health Risk and Costs. Proceedings*, SAS Global Forum 2013. <http://support.sas.com/resources/papers/proceedings13/170-2013.pdf>.

In today's world, it is unlikely that consumers know or have the ability to know which of their activities, purchases, interests, or inherent qualities has categorized them. It is also unlikely for consumers to be able to know all of the entities that have categorized them. It is further unlikely for consumers to be able to determine what marketplace and life impact such categorization

might be having.

Among the questions we think are crucial to ask and study with rigor, we include the following:

- How to segment in a fair and accurate way, including removing discriminatory factors used in analysis that are protected in law or factors that serve as proxies for discriminatory practices?
- How to sift segmentation for *hidden* categorization effects and hidden discriminatory effects? (This is often due to mirroring of factors in data sets.)
- How to account for accuracy in each segment, and ensure correct usage of the data according to its accuracy level?
- How to deal with liability issues for someone who acts on incomplete data and gets an outcome undesirable by the individual?
- How to allow for consumer participation and access to categorization results, including removal?
- How to ensure the individual's right to shape their digital exhaust and have control over how they are being analyzed for meaningful decisions that have an impact on their lives or livelihood? (See also Scenario 2 and 3 regarding scoring and granular consent.)

Scenario 2: Modeling / Scoring of individual consumers

Another important scenario to discuss involves the scoring or modeling of individual consumers who are sliced, diced, and analyzed routinely without their knowledge or consent. If one never knows how or when the record will be used, and in what kind of context it will be used, the fairness and privacy concerns should be readily apparent. The trails of our digital exhaust have many potential uses, some beneficial, some not. We understand the lure of research into large data sets; but the data sets with the most impact on privacy are those that can be tied back to an individual. It is research about scores attached to individuals or even households that we see as having long-term impacts.

Among American adults, each individual with a credit or debit card or a bank account is likely to be the subject of one or more scores or predictive models. Many individuals signed up under the Affordable Care Act have a score. Individuals who buy airline tickets have a score. Individuals who make non-cash purchases at large retail stores likely have a score. Scores such as the medication adherence score, the health risk score, the consumer profitability score, the job security score, collection and recovery scores, frailty scores, energy people meter scores, modeled credit scores, youth delinquency score, fraud scores, casino gaming propensity score, and brand name medicine propensity scores are among the consumer scores that score, rank, describe, and predict the actions of consumers.

To create a consumer score, the score modeler feeds raw information (factors about consumers) into an algorithm designed to trawl through reams of data to detect consumer behavior patterns and to eventually sift consumers into a ranking by their scores. Each score generally has a name and predictive or descriptive function.

Today scoring models are easily built from data that is **extrinsic** to the final score. No nexus may exist between the **input** to a score and the **output**. In the financial scoring area, companies can now build financial scores from social media, demographic, geographic, retail purchase history, and other non-traditional information that may not be included in the formal credit file. In the health arena, analysts can now build health risk scores from mere wisps of demographic data, without any actual patient records.

In this new world of scoring, where analysts use factors extrinsic to the purpose of the score to build scores, that a person has red hair can be used as a factor. And the more factors, the better. Instead of using 30 factors, why not 3,000?

How to specifically bring fairness and privacy protection into each step and aspect of this process is an important research area. It is not feasible to have human review of each algorithm creating modeling or consumer scores – there are too many scores, too many models, and it happens too quickly. What, then, is the answer to bring statistical parity to individual consumers?

Scenario 3: Granular consent in the EHR context

Granular consent, or consent with many detailed choices for the consumer to exercise about how their data is used or shared, remains an important concern. Granular consent deserves much more research attention. It can be controversial in many respects, and fact-based discussions are much more helpful than conjecture in shaping policy.

We offer a generic comment about the role of consent. Consent should not be required on an all-or-nothing basis as a means to protect privacy. There can be and there should be considerable variation in the nature of data subject consent. Too often, data subjects are presented with a single choice: agree to preset terms that unfairly favor the person who presented the choice, or go away. In many circumstances, consent should offer data subjects more choices, and the choices should be presented in a meaningful way. Consent should be unbundled to the extent practicable. We need to know more about how to make consent more meaningful.

In the specific scenario we would like to discuss here, granular consent has been a hotly debated issue in the electronic health records space for over a decade. The development of electronic health records (EHRs) gives health care providers, insurers, and other data users expanded ability to transfer patient records for lawful activities.

With In electronic health records collecting so much information in one place (or available through one system), the need for granular consent expands. For example, patients often do not want their dentist or eye doctor seeing or having access to their psychological records, but they nevertheless may want to share some records with some doctors.

In an important and well-researched study, the study results were unambiguous. (*Patients want granular privacy control over health information in electronic medical records,* National Institutes of Health, Journal of the American Medical Information Association, Kelly Caine and Rima Hanania. J Am Med Inform Assoc 2013;20:7–15. doi:10.1136/amiajnl-2012-001023 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555326/pdf/amiajnl-2012-001023.pdf>

No patients reported that they would prefer to share all information stored in an electronic medical record (EMR) with all potential recipients. The study found that patients' sharing preferences varied by type of information and by recipient (eg, primary care provider versus dentist). Further, overall sharing preferences varied by participant. Patients with and without sensitive records preferred less sharing of sensitive versus less-sensitive information. The authors wrote:

> Patients expressed sharing preferences consistent with a desire for granular privacy control over which health information should be shared with whom and expressed differences in sharing preferences for sensitive versus less-sensitive EMR data. The pattern of results may be used by designers to generate privacy-preserving EMR systems including interfaces for patients to express privacy and sharing preferences.
>
> To maintain the level of privacy afforded by medical records and to achieve alignment with patients' preferences, patients should have granular privacy control over information contained in their EMR. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555326/.

A study of Indiana patients on this issue found similar results:

> In a study of the granularity of individual preferences among 30 Indiana patients, not one agreed to share all of their information with all providers on a list of provider types. Primary-care physicians were trusted most and fared best, but still only about 75% of patients surveyed agreed to share all their records, even with them. <http://www.modernhealthcare.com/article/20140916/BLOG/309169995

By furthering research on granular consent, there are many important privacy advancements that could be made and applicable to, for example, data brokers. We recognize that giving people too many choices can be overwhelming and may not produce the best range of outcomes. That consideration should be a factor in designing consent protocols. The needs for more granular consent cuts across many types of data and many technologies. Again, a better technical architecture will allow the implementation of more nuanced and more appropriate outcomes. We observe that researchers, as data users, have a stake in this debate too.

Some specific questions that need to be answered about granular consent include the following:

- How to do data segmentation that is meaningful to patients?
- How to create granular controls that are flexible through time and can be revoked without causing problems throughout complex systems?
- How to ensure data preferences that are expressed stay with the data as it travels?
- How to design granular consent so that it is not overly burdensome for patients or healthcare providers and can take place at the time when it is salient and meaningful for patients?

Scenario 4: Electronic Consent for Health Research in EHRs

New technology should give individuals new capabilities to express their preferences with respect to the processing of their own information. We have already discussed this in the context

of granular consent in EHRs. We specifically want to raise the issue for use of patient records in health research. We support the use of patient records for health research. While we think that there are serious flaws in the current system using Institutional Review Boards to review research protocols and to waive the need for individual consent, we are not prepared to say that patient consent should be required for all research disclosures.

The role of patient consent in health research requires a broader national conversation that goes beyond the scope of the current RFI. However, we think that there should be some role for patient consent for research disclosures at least some of the time. We are not prepared at this time to draw a line. We first want to listen to and participate in the debate over how our society wants to support health research. However, there are things that can be done now in advance of any societal decisions.

EHRs should be built to support a greater role for patient consent. This would be a fruitful area for research. One of the features that supposedly makes EHRs attractive is the ability for patients to play a greater role in their health care, supported in part by greater access to their own records. That same ability to involve patients creates an opportunity to ask the patients for their approval of research projects in which they want to participate. In those circumstances when patient consent is possible and appropriate, the patients who access their own records are easily found and can be asked for their consent. A well-designed EHR will allow patients a variety of choices regarding research disclosures.

Some patients will make their records available for research under all circumstances. Some will approve in advance some types of research, will reject other types, and will want to be asked for permission in other cases. Some patients may be willing to allow use of their records if a designated organization (e.g., a disease advocacy organization, a church, or the ACLU) approved the research. Patients should be able to decide to participate or not participate in projects that have a specific purpose, e.g., to determine whether a drug they are taking has undesirable effects on different populations. They may even give their consent for multiple similar projects, e.g., I want to participate in all drug studies that involve *X drug* or *Y category* of drugs.

An efficient and flexible system of patient consent for research will only work if it is built into EHRs. We recognize that we have not decided as a nation exactly where to draw the line between research that needs consent and research that can rely on a substitute for consent. Nevertheless, we can still establish a system that will support whatever decision is ultimately reached. In the absence of a national determination on the broad question of consent, an EHR that supports patient consent for research could allow different approaches by individual record keepers. Today, the decision to cooperate with researchers is largely left to health care providers. A well-designed EHR will allow each provider to decide what role it wants patient consent to play.

We emphasize that we are not suggesting that IRBs should not have a role in overseeing health research protocols. For example, IRBs should have sufficient technical expertise to make sure that the projects, even done with consent, produce meaningful and scientifically valid results. A greater capability of supporting patient consent can be baked into health information technology and can support the role of IRBs by including patients' views in decisions about health research.

This is a fruitful area for attention and research. The proper architecture will allow for the implementation of a variety of policy outcomes. We urge a focus of research on consent in this context.

III. Concepts, methods, and constructs needed to assess privacy.

FIPs must make up the baseline for conceptual assessments of privacy. Statistical parity must also be included. Much work remains to be done on what precisely statistical parity methods and constructs would be able to be used to assess privacy in a consistent way.

A request for information about "assessment capabilities" seems like an attempt to find a measurement mechanism for privacy-related outcomes. FIPs are process-focused. One of the criticisms of the HIPAA Privacy Rule and the EU privacy regulations has always been that you can get the process right--all the right notices, provision of access, etc.--and still not get privacy right. The market-based response to this criticism is "if people use a product/service they must be happy with the privacy protection included in the product or service." This is not always the case, particularly in cases where consumers face limited choices between market offerings.

We are interested in finding way(s) of assessing end results and, therefore, ways of designing systems and products so that the end results can be achieved. We observe the increasing processing of personal information by government and private entities. Much of the increased processing is the result of technological advances. The same technologies and advancements should be employed to protect privacy and to support data subject rights and interests.

We have several broad suggestions as to some of the promising candidates.

A. Data Provenance and MetaTagging

In some circumstances, it will be appropriate to tag data so that **the source** of the data is transferred whenever **the data** is transferred. In other words, we suggest that metadata be employed to show the provenance of the data. This is technically possible and already happens to some extent in Electronic Health Records, and. It has great potential for privacy. We observe in passing that better provenance of data has great value to researchers as well.

Metadata will help individuals determine how their data has been processed, who is responsible for any given data field, when the data was created or added, and how to exercise rights of access and correction. Finding practical and appropriate ways to tag personal data is an architectural issue that needs research and attention.

Another area for research and attention that would go far to ending some of the worst cases of information abuse is how to ensure the meta tagging is kept with the data, and how to allow for audit trails based on the data provenance that consumers could track. Instead of focusing on opt out, which has its own problems and challenges, a focus on how users could manage rights through managing metadata could potentially go far to address challenges with data reselling that is not authorized, desired, or is harmful.

B. EHRs as an example of information tech that supports data subject rights

In addition, information technology can directly support data subject rights. EHRs provide an example. Giving patients robust access to their health records is a feature of EHRs. That same type of access is appropriate for other electronic records. However, access and other data subject rights must be baked into the technology from the beginning. This is yet another architectural issue worthy of research and attention.

C. Ad tech potential

Finally, the same technology already used to deliver advertising to individuals with a particular set of characteristics can be used to deliver notices and requests for consent to individuals under specific circumstances and across platforms. This idea has been discussed by Esther Dyson in a number of settings. See, e.g, her article <http://www.huffingtonpost.com/esther-dyson/release-90-user-managed-p_b_650383.html>. We do not have copious research to share here, but we see this as having good potential and we would like to see ideas developed here.

IV. Big Data

The fourth request in the RFI begins by mentioning the White House Big Data report's recommendation for adoption of a ''responsible use framework'' that would provide greater focus on the use of data and hold entities that utilize data accountable for responsible use of the data. This request seems to place the locus of the decision about what constitutes "responsible use" outside the individual. There are specific instances where this may be necessary, e.g., in law enforcement, but it should not be a universal approach to privacy.

Regarding big data specifically, Big Data has not been shown to provide a reliable enough basis for developing an entirely new approach to privacy solely applicable to big data: buzzwords are not the right way to drive major policy changes nor privacy management.

We observe that the White House report did not include a meaningful definition of Big Data that allows any objective observer to distinguish Big Data from any other compilation of data. We agree that larger compilations of data create greater challenges, but we do not agree that there are always fundamental differences in kind rather than just differences in degree. Sometimes there are, but not always.

We understand that some believe that in a sensor-rich, data-rich analytics environment, that controlling data collection is no longer possible, and that controlling use is the last bastion of privacy. We disagree. We would support research that challenges this hypothesis rigorously. We are not persuaded that responsible use frameworks will be successful. We have, in our research, discovered that in trying to build frameworks that protect use of data are extraordinarily challenging on many fronts.

To cite a simple example: when we make purchases with credit cards, retailers can sell our transaction histories to third party data resellers or data brokers, who can then use the results to build categories and segment that data with ever increasing levels of refinement. Scores such as the Consumer Prominence Score can be the result. This score has been used to help determine

health risks for health plan rates, as we documented in our *Scoring of America* report.

Do such sales of consumer transactions constitute "responsible use," and if so, on what basis? Is there a role for FIPs in a "responsible use" framework? Are consumers notified about uses under such frameworks? Do they have access? Or do fundamental information rights get taken away in this model? In a use-based model, often the FIPs-based rights (or at least some of them) get taken away in preference to back-stopping the privacy challenges at the use point. But at the use point, the damage gets done without oversight or consumer control or recourse. We believe that rigorous research that challenges the assertions of the effectiveness of such a framework need to be conducted. We would also like to see research that looks at layering a "responsible use" framework with FIPs-based frameworks for maximum effectiveness.

Some of the questions around responsible use models include:

- Do sales of consumer transactions constitute "responsible use," and if so, on what basis?
- How are FIPs incorporated in a "responsible use" framework?
- Are consumers notified about data uses under responsible use frameworks? Do they have access? Or do fundamental information rights get taken away in this model?
- How does statistical parity plus FIPs plus use protection work together compared with other single-model approaches? (See discussion of layered protection model below.)
- How can a responsible use framework be designed to mitigate risks to the individual?

A. The layered protection model

We have hypothesized that a layered, overlapping protections approach is going to work best going forward. FIPs plus statistical parity, for example, working together as a model. Perhaps a responsible use framework could be added on top of this, in addition to, **but not replacing** the other frameworks. The days and era of having a single-silver bullet solution to privacy are long gone, and it is much more helpful to find effective ways of layering protections and building in individual consumer choice – meaningful choice – wherever possible. We would like to see a request for scenarios on this point. We emphasize, however, that any model that leaves out FIPs will be incomplete in approach.

B. Digging into responsible use in context

What is "responsible use" in one setting may not be in another setting. Trying to quantify and weigh both benefits of data use and potential risks and harms is a helpful exercise. However, while this approach seems to make sense, it is not clear how it could possibly incorporate all the various and changing perceptions of benefits and harms that individuals might have. Because of the inherent problems here, we urge research on specific scenarios to tease out a variety of underlying patterns – and we also urge an approach that views responsible use from an individual point of view, including choice mechanisms that individuals should have. We also urge a study of privacy risks or harms from the point of view of the individual, not the organization that will be benefiting from the use of the data. Privacy-related risks to a company or a government agency are very different from risks or potential harms as seen by the individual, and it is the risks to the individual that privacy rules should be designed to mitigate.

As an example, we cite the Facebook mood study. Facebook is not subject to the Common Rule,

yet Facebook undertook human subject research which in an academic context would have been subject to the Common Rule and would have required meaningful consent. How would a responsible use guideline impact both Facebook and the individual consumer here? Both considerations are important. It is not enough just to guide corporate behavior; individuals still need rights and need to have meaningful choices. Not all choices are as meaningful as others, this, too, would be useful grounds for research.

C. Consumer (individual) consent as part of all layers of protection

We encourage any research done in the area of use-focused frameworks to include consumer consent as part of the fabric of the framework. This is admittedly challenging. Yet without this rigor, use-focused frameworks just become an excuse to leave the consumer out of the equation. Please also see our discussion of granular consent and consent for health research earlier in these comments.

D. Enforcement of use-focused frameworks

One of the many challenges of use-focused frameworks, as mentioned, is their loci of removal of individual choice in the way information is used. Another key problem is enforcement. This is rich territory for many rigorous studies on how enforcement of use could be enacted. Self-regulation will not be effective here. Without enforcement or transparency of behind-the-scenes actions, any framework that focuses on use becomes a fig leaf and nothing more.

V. Conclusion

We are pleased that this RFI was published, and we support the goal of more research on the challenges to privacy. While we have disagreements with the manner in which the RFI frames some of the challenges to privacy, we hope that our suggestions show that we share your interest in finding better ways to protect privacy rights and interests.

In order to further this conversation, we encourage you to convene a public meeting to encourage dialogue of the stakeholders on this issue. We would be happy to participate in this dialogue.

Respectfully submitted,

Pam Dixon
Executive Director, World Privacy Forum
www.worldprivacyforum.org