Before the
DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE
WASHINGTON, D.C. 20554

In the Matter of:	)	
	)	
"Information Privacy and Innovation in the Internet Economy"	)	**Docket No. 101214614-0614-01**
	)	
	)	
	)	
	)	
	)	

COMMENTS –PUBLIC COMMENT #1

TELCORDIA TECHNOLOGIES

Telcordia Technologies (Telcordia) hereby submits comments to the National Telecommunications and Information Administration (NTIA) on its Public Notice requesting comments on the Department of Commerce's Internet Policy Task Force (IPTF or "Task Force") report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" in the above-captioned proceeding.[1]

BACKGROUND

Telcordia is a software and engineering and consulting company with a vested interest in expanding the deployment of broadband. Telcordia, formerly known as Bell Communications Research (Bellcore), was created in 1984 at the time of the AT&T divestiture as a unique entity with a mission to provide common R&D as well as technology generic requirements and seamless operational capabilities across all the new service provider boundaries. We have the depth and breadth of telecommunications

[1] Public Notice, Information Privacy and Innovation in the Internet Economy, 75 FR 80042, Released December 21 2010.

experience to handle the full spectrum of communications and information networking engineering and design issues. We offer the following comments on the issues raised by the Task Force.

EXECUTIVE SUMMARY

Adequately addressing privacy and security is necessary to create vibrant marketplaces for context-aware personalized information services. Marketplace members benefit if a trusted third-party manages the complex privacy and security requirements associated with accessing end-user's personal and confidential information. A reliable, robust policy-based privacy clearinghouse system that acts as trusted gateway between service providers and sensitive information can foster an expanded information services marketplaces for end-users, personal and confidential information database owners, and value-added Application Service Providers (ASPs). The privacy clearinghouse system would ensure that only authorized and reputable service providers are given access to sensitive information, only to such information required by their services, only for users that have validly opted-in to such services, and with necessary tracking and trace-back capabilities.

We present our comments on and responses to questions in the Task Force report in the context of a policy-based privacy clearinghouse for protecting consumer privacy based on two primary recommendations:

1. A central privacy clearinghouse/gateway for protecting consumer privacy, built upon the techniques of policy-based management, should be considered as part of the solution as it:

- Promotes transparency by enabling automated processing and translation of privacy policies and specifications into easily understood descriptions;
- Allows easier access to and comprehension of privacy policies by consumers;
- Enables strict enforcement of privacy policies and regulations as well as complete logging and audit capabilities to demonstrate compliance;
- Provides multiple benefits to all stakeholders, include fostering innovation in the information services marketplace via new services, applications and "mash-ups," which translate into incentives for adopting the approach; and,
- Enables a consolidated/simplified approach for managing privacy policies, regulations, and specifications.

2. A multi-stakeholder process for specifying the gateway solution architecture and functionality, including the technology aspects, is the best way to ensure that all stakeholder needs are represented and to get better "buy-in" for the resulting solution.[2] Specific privacy solution aspects that should be done through a multi-stakeholder process include:
    - Architecture and protocol specification for the required technical infrastructure such as a policy-based privacy clearinghouse; and
    - Formats and standards for machine-readable versions of Purpose Specifications, Use Limitations, and Privacy Impact Assessments (PIA).

[2] A similar approach (i.e., using a multi-stakeholder process) has been successful in the case of OpenID. See "Open Trust Frameworks for Open Government: Enabling Citizen Involvement through Open Identity Technologies," at http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf, 10 August 2009.

DISCUSSION

I. The Role of Technology for Ensuring Information Privacy and Innovation in the Internet Economy

Telcordia has been conducting research in the area of Internet and Mobile Services privacy for the past couple of years. The major focus of the research was a proof-of-concept policy-based clearinghouse system for ensuring privacy of sensitive and confidential end-user information that also serves as an enabler for (mobile and Internet) services and applications as shown in Figure 1.[3]

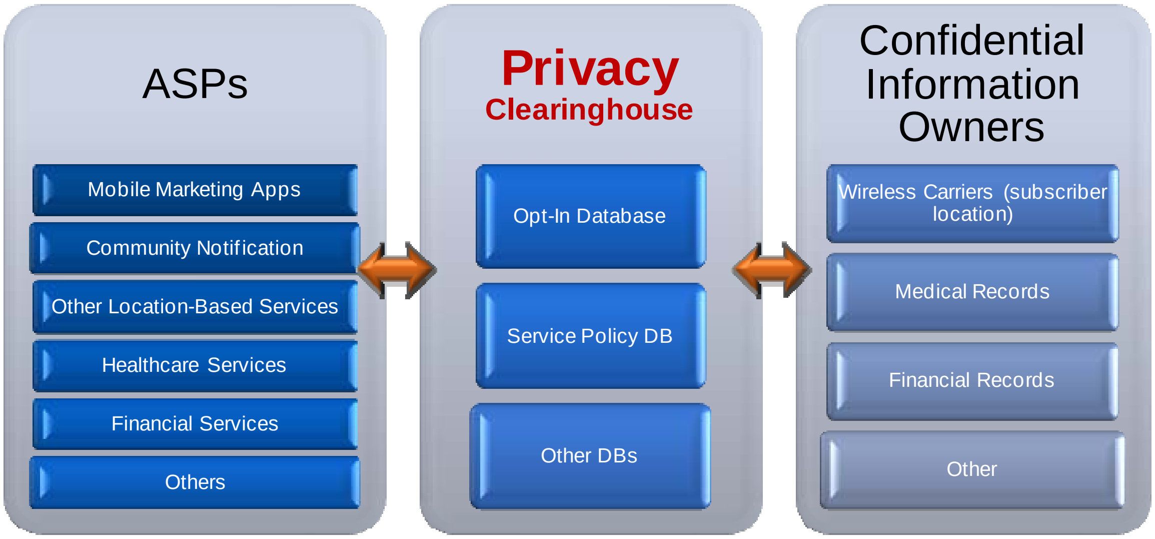

Figure 1. High-Level Architecture of a Privacy Clearinghouse

The policy-based privacy clearinghouse system acts as a trusted entity which manages complex privacy and access control policies and customer preferences to enable secure authorized information exchanges between information sources/providers and application service providers. In addition, the system acts as an access control layer to protect

[3] See "Scalable Infrastructure for Enforcing Privacy and Security of Personal Information" by Ashish Jain, Shoshana Loeb, Stan Moyer, and Euthimios Panagos that was published in the *Proceedings from the International Conference on Internet Multimedia Systems Architecture and Application*, Bangalore, India, December 2010 and "Trusted Access to Sensitive Information in a Diverse Services Environment" by Stan Moyer, Shoshi Loeb, and Thimios Panagos from the *Proceedings of IEEE CCNC 2010*, January 2010. This policy-based privacy clearinghouse system was created to successfully demonstrate the feasibility of a scalable policy-based solution to the complex privacy issue.

confidential and sensitive information residing in information sources as depicted in Figure 2.[4] The main innovation of this system is the application of policy-based management techniques for the management of consumer privacy preferences and privacy policy specifications for end-user data – leveraging many of the advantages that policy-based techniques enjoy in related communications and information networking areas.[5]

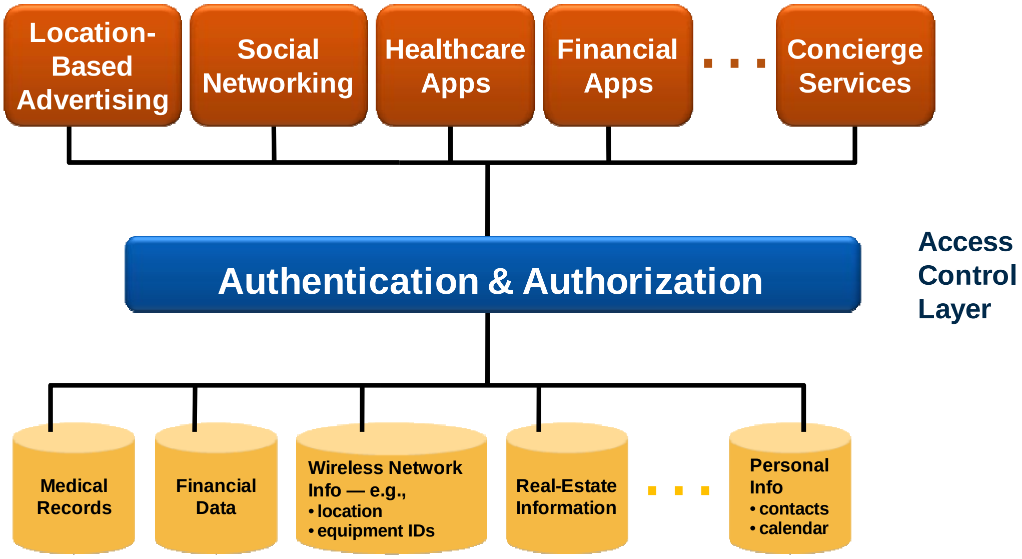

Figure 2. The Access Control Layer provides authentication and authorization functionality to protect access of sensitive and confidential consumer information sources.

The use of policy-based management (PBM) techniques provides many advantages over traditional management techniques – some of these advantages are:

[4] This type of architecture is similar to that of the Rule Holder in the Geopriv Requirements architecture as described in "Geopriv Requirements," IETF RFC 3693, February 2004.

[5] Telcordia has many projects and prototypes that apply policy-based management techniques to network and configuration management. For example, Telcordia employees wrote one of the first books on Policy-Based Management for mobile ad-hoc networks – *Policy-Driven Mobile Ad hoc Network Management* by Ritu Chadha and Latha Kant, Wiley-IEEE Press, 2007.

- The automation of privacy use and access decisions facilitates all administrative and processing functions (even with growth) for streamlined management and “lights out” operation.
- Easy management of personal privacy profiles for end-users is made possible by enabling specification of privacy preferences through high-level or general policies and automatic translation to laymen’s English;
- The system is easily adaptable/evolvable to future changes in privacy specifications as the privacy rules are not hard-coded into the system, but are rather programmed through privacy policy specifications.
- PBM combined with a hierarchical approach (such as groups and categories) has the ability to scale to large numbers of (differing) privacy policies and end-users. The scalability advantage is especially important in the complex world of consumer data privacy as the number of different types of policy specifications is very large and is expected to grow even more.

Note that while Figures 1 and 2 depict the application service provider and information owners as separate entities, we do realize that in some occasions those functions are provided by the same organization (e.g., a credit card company that utilizes end-user transaction data on its own credit cards to offer a service). In these cases, the organization will still find value by using one centralized repository for all privacy policies of several variants of the clearinghouse architecture – e.g., deploying a local instance of a distributed version of the clearinghouse[6] or by separating the different

[6] As described in “Scalable Infrastructure for Enforcing Privacy and Security of Personal Information” byAshish Jain, Shoshana Loeb, Stan Moyer, and Euthimios Panagos which was published in the

organizational functions. The distributed version of the policy-based privacy clearinghouse retains the same benefits as the centralized version due to the same use of policy-management techniques and a logically centralized repository for all privacy policies.

In the remainder of this comment, we focus on using a policy-based privacy clearinghouse system to achieve the dual goals of "commercial data privacy and innovation in the Internet economy." In addition to the consumer protections and advantages discussed above, the proposed policy-based privacy clearinghouse system also has many potential benefits for stakeholders in the information industry including:

- By automating the privacy approval and verification process, the system allows service providers to offer services sooner, thus enabling information providers (and all others in the value-chain) to get to market (and see revenues) sooner.
- By handling the privacy approval and verification process, the system enables information sources and application providers/developers aggregators to focus on their core competency.
- By acting as a gateway to multiple information sources, the number of business relationships that an application service provider/developer must establish is reduced and the ability to easily create "mash-ups" from multiple information sources is enabled.
- By attracting a variety of application service providers and developers, a marketplace for consumers of sensitive and confidential information is

created, enabling the owners of the repositories of that information to monetize that data.

- By providing a single user interface for the management of personal privacy data use and the automated translation of privacy specifications and policies into layperson’s text, consumers will be able to more easily identify and comprehend their personal privacy implications.

The above stakeholder benefits are important in providing incentives for both organizations and consumers to participate in such a system.

The recommendation to use policy-based management technology to address many of the privacy issues is aligned with some of the commenters on the first NOI[7] as pointed out in the Task Force report that states “Similarly, a number of commenters noted that privacy-by-design and technological approaches, such as icons on advertisements or profile management dashboards, could be used to implement industry standards.”[8] In fact, the clearinghouse system that we described has the concept of a “profile management dashboard” for end-users to utilize for managing the use of their information.

We will use the remainder of this paper to make specific comments on portions of the Task Force report and to respond to selected questions from the report. Most of the comments and responses will assume the existence of a clearinghouse/gateway system. The order of the comments and responses is based on the order the text and questions appeared in the report and does not reflect our opinion on their relative importance.

[7] Department of Commerce, Notice of Inquiry on “Information Privacy and Innovation in the Internet Economy,” issued April 23, 2010, Docket No. 100402174–0175–01.

[8] “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework” by the Internet Policy Task Force, p. 45. The quote references comments on the original NOI by AT&T, CDT, and Google.

II. Comments on Bolstering Consumer Trust Online through Fair Information Practice Principles (FIPP)

In this section, the Task Force report notes that "Others stopped short of explicitly embracing the current notice-and-choice framework but urged caution with respect to changing it."[9] While we believe that "notice and choice" is a useful concept, we do believe that some changes are required. One valuable change would be to make the notices easier to parse by computer systems (i.e., make them standardized and/or machine-readable). With the privacy policy notices readable by computer systems, it is possible to perform automated translations of the notices into language that a layman can easily comprehend, greatly improving the ease of use for consumers. With the delivery of these notices incorporated into a policy-based privacy clearinghouse system, adding the automated translation capability becomes a relatively simple function as the notices are translated into privacy policies in the system and then presented to end-users as part of their privacy preference profile.[10] To facilitate the development of machine-readable notices, "standard" families of privacy policies within a privacy policy taxonomy should be defined. The standard policy family would evolve over time as needs required and exceptions to these standard policies would also be allowed.

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

As discussed in the previous section and as pointed out in the Task Force report, under the "current notice-and-choice model, consumers' privacy rights depend on their

[9] Ibid. p. 27.

[10] For example, the Creative Commons has "wrapped" some free software/open source licenses with a human-readable "Commons Deed" and machine-readable metadata with goal of making software licenses more easily understandable by end-users. http://wiki.creativecommons.org/FFAQ.

ability to understand and act on each individual company's privacy policy."[11] This point is relevant to another statement in the report that says "information must be accessible, clear, meaningful, salient, and comprehensible to its intended audience."[12] As discussed in item II above, this goal can be achieved by ensuring that policies are readable and translatable by computer systems; the computer systems can then present the information to the end-user in a simple, comprehensible, and meaningful way. This allows end-users to make better informed decisions about how (and why) their information will be used.

The Task Force asks "*What is the best way of promoting transparency so as to promote informed choices?*"[13] We believe that the privacy clearinghouse described earlier is an ideal way to promote transparency because:

- It automates the information choice process and presents the choices in a uniform (and agreed upon) manner.
- Through automation and translation, the privacy implications can be presented clearly (to the average end-user).[14]
- Regular notification of privacy choices can be issued as a reminder to the end-user of their privacy choices.
- A centralized location for examining (and comparing) privacy choices can be provided so that end-users can easily locate all their choices.
- An auditable log is created that can be examined later by end-users of an independent third-party on behalf of end-users.

[11] Task Force report, p. 31.
[12] Ibid. p. 31.
[13] Ibid. p. 37, question 1, which is also question #5 from the Federal Register supplementary information.
[14] Similar to the advantages of notice translation and automation described in section II.

The Task Force asks "*Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?*"[15] PIAs that are in a standardized and machine-readable format, can be easily parsed and utilized by a technical system for protecting consumer privacy. For example, such PIAs can be automatically translated into privacy policies for information sources and/or services and applications that could then be enforced by privacy protection system. As there are many advantages to the use of standardized PIAs in a machine-readable format – such as reduced administrative overhead, faster time to service deployment, and great end-user comprehension – we do believe that standardized, machine-readable PIAs should be required. The specification of PIA standards should be accomplished through a multi-stakeholder process in order to guarantee that all stakeholder needs are addressed.

IV. Comments on Aligning Consumer Expectations and Information Practices through Purpose Specifications and Use Limitations

In this section, the Task Force then asks a couple of questions related to purpose specifications – "*Are purpose specifications a necessary or important method for protecting commercial privacy?*" and "*How should purpose specifications be implemented and enforced?*"[16] We believe that purpose specifications are an important feature for providing transparency to the consumer, as those specifications indicate the reason for needing/using the personal data. Combined with "Use Limitations," the purpose specifications can be used by a policy-based privacy clearinghouse system to derive privacy policies provided the specifications are in a standardized and machine-

[15] Task Force report. p. 37, question 5, which is also question #9 from the Federal Register supplementary information.

[16] Ibid. p. 40, questions 1 and 4, which is also questions #13 and #16 from the Federal Register supplementary information.

readable form. These privacy policies can then be automatically enforced by the system, which provides a strong measure of confidence to the consumer that their personal data is being used only as intended. Complete and comprehensive audit logs generated by the systems can be examined by an independent third-party organization to also verify compliance with the specifications and limitations, both on a periodic basis and in response to specific concerns or new issues.

V. Comments on Evaluation and Accountability as Means to Ensure the Effectiveness of Commercial Data Privacy Protections

In this section, the Task Force states "Before any audit can take place, of course, the data about how information was used must exist."[17] Further, the report goes on to say that "audits depend on some degree of technical infrastructure that can account for how information has been used, and how it should have been used."[18] These statements on the need for a technical infrastructure to generate information that can be audited are similar to some of the requirements that led us to develop a privacy clearinghouse/gateway solution as described in Section I. The creation of auditable logs at various levels and at interfaces of the system is a requirement and a useful capability that we identified for the system.[19] This capability is a strong motivation for incorporating such a system as a technology component in any consumer privacy protection solution.

[17] Ibid. p. 40.

[18] Ibid. p. 40.

[19] For example, the policy-based privacy system can create log entries for actions like:

- End-user privacy profile change (e.g., through an "opt-in" or "opt-out")
- Access to confidential or sensitive personal data (by which service/application and for what purpose)
- Actual uses of personal data in a service or application

The Task Force asks the question "*Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?*"[20] While some technologies are starting to emerge for consumers to verify how their personal information is being used,[21] there is currently no standard or uniform mechanism available so that consumers can verify the use of their personal information in an intuitive manner. Our recommendation is that a "standard" technology consisting of a policy-based privacy clearing house as described in Section I with a personal privacy dashboard will enable consumers to verify use of their personal information.

The Task Force then further asks "*Are technologies available to help companies monitor their data use, to support internal accountability mechanisms?*"[22] Many logging mechanisms exist that companies use to monitor data use. However, in most systems auditing is performed through standardized reports and flags. This means that changes in auditing and detailed inquiries may require manual effort or custom programming, both of which can be relatively slow and costly. We recommend the creation of a standard, auditable log format for the access of personal data[23] – this format should also be developed through an open, multi-stakeholder process. Based upon this format, policy-based management technologies can automatically compare the log data with purpose specifications and use limitations that specify how the data should and should not be used

[20] Task Force Report. p. 41, question 1, which is also question #19 from the Federal Register supplementary information.

[21] e.g., icons in advertisements as described in the Task Force report on p. 46.

[22] Task Force Report, p. 41, question 2, which is also question #20 from the Federal Register supplementary information.

[23] The need for standard, auditable logs for consumer privacy protection systems is similar to the need to be able to easily analyze and understand computer security logs as described in the NIST "Guide to Computer Security Log Management, a Recommendation by the National Institute of Standards and Technology," by Karen Kent and Murugiah Souppaya, in Special Publication 800-92, September 2006. See: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

and, more importantly, enforce adherence to the purpose specifications and use limitations.

The Task Force concludes the section with the question "*What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purpose and use limitations?*"[24] The privacy clearinghouse/gateway system described in Section I is a technology that facilitates audits of information use. As previously discussed, the privacy clearinghouse system offers several business benefits that provide incentives to encourage organizations to make use of that system. Therefore, we recommend that, in addition to other incentives, the technologies specified as part of any overall solution be chosen with the to provide the additional incentives to encourage adoption – that is, the system that facilitates audits should also provide other stakeholder benefits so that organizations have an incentive to use it. The policy-based privacy clearinghouse described in section I has these characteristics.

VI. Comments on Maintaining Dynamic Privacy Protections through Voluntary, Enforceable, FTC-Approved Codes of Conduct

In this section, the initial recommendation (#3)[25] is consistent with the two main viewpoints that we are advocating. These points are that legislative (or regulatory) incentives are required to enable the creation of privacy clearinghouse/gateway system and that a multi-stakeholder process (e.g., an open consortium) is necessary to develop the specifications. The policy-based privacy clearinghouse/gateway system described in

[24] Ibid. p. 41, question 5, which is also question #23 from the Federal Register supplementary information.
[25] Ibid, Recommendation #3, p. 41.

Section I is based upon “emerging technologies” as referred to in the recommendation. The use of policy-based management techniques to manage privacy policies and preferences provides many advantages and enables the implementation of a reliable and scalable clearinghouse. The “safe harbor” legislation described in the Task Force report does provide good incentive for companies to participate in the system and, combined with other benefits that the system provides (e.g., rapid time to market, reduced development and operational costs), will motivate organization to utilize such an approach.

The report states that “The Task Force seeks additional input […] on the ‘carrots and sticks’ through which to encourage the development of these industry codes.”[26] Specifically the Task Force asks “*How can the Commerce Department best encourage the discussion and development of technologies such as ‘Do Not Track’?*”[27] The multi-stakeholder process that the report proposes for the development of FIPPs is an excellent approach for fostering discussion and encouraging development of technology components as part of the overall consumer privacy protection solution. By bringing together various stakeholders that represent the entire span of the value-chain, with the Commerce Department acting to facilitate, influence, and direct the discussion, progress on developing the necessary specifications. We also suggest that the Commerce Department sponsor other activities like prototypes, demonstrations and interoperability events to stimulate R&D, gain early determination on approach feasibilities, and obtain stakeholder feedback on various technology solution options. These types of activities

[26] Ibid. pp. 48-49.

[27] Ibid. p. 51, question 2, which is also question #25 from the Federal Register supplementary information.

will both encourage development of these technologies and facilitate interaction of the various stakeholders.

CONCLUSION

For the foregoing reasons, Telcordia urges the Department of Commerce to consider our comments and recommendations. This is a topic we strongly believe must be addressed by both the federal government and by all stakeholders involved in order to come up with and deploy a viable solution. We would be happy to engage in further dialog and discussion on this topic in general and our recommendations in particular.

We believe it is possible to create a vibrant information services marketplaces consisting of end-users, personal and confidential information owners, and value-added application service providers and developers to provide end-users with access to a wealth of personalized information services without the fear of compromised privacy. By utilizing policy-based management techniques to create a gateway system many advantages are realized for consumers as well as market incentives

Respectfully submitted,

TELCORDIA

By: C Greene

Brenton C. Greene, President,
Advanced Technology Solutions
TELCORDIA
One Telcordia Drive
Piscataway, New Jersey
(732) 699-2100
bgreene@telcordia.com

January 28, 2011