Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket Nos. 09-47, 09-51, 09-137
Comments –NBP Public Notice #21	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commission's NBP Public Notice #21, regarding the relationship between a national broadband plan for the United States and data portability for civic engagement. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet.

I. Introduction

The National Broadband Plan can play a vital role in enabling and encouraging the use of new digital technologies to foster greater government data transparency, increased citizen participation in government, and collaborative civic engagement of all types.

II. Government Data Transparency

One key to ensuring an informed citizenry is making government information available online and making online access ubiquitous. The Open Government Directive recently released by the Administration has the potential to change the culture of caution and secrecy that has previously prevailed in some government agencies. However, much work remains to alter regulations, policies and practices that have historically limited access to data in the hands of the government. Even agencies that do want to put their information online have been blocked by resource shortages, outmoded regulations or inadequate technology.

Moreover, merely opening access to government servers will not be sufficient if the data are not usable by the public. To truly achieve digital democracy, government data must be made available in formats that allow the data to be reused and enhanced by programmers in the private sector, who can provide innovative applications that make the information even more readily available to the public.

Creating government transparency by leveraging private sector innovation

Achieving digital democracy will require a clear vision of the many benefits and cost savings that will be realized by engaging the private sector in leveraging government data by creating innovative applications and tools.

There are already good illustrations of the innovative uses that can be made of portable government data made available online. For example, many localities that release crime statistics and reports now have online, third-party “mashups” transposing this data on top of a map so that citizens can see which areas are safest and which have the greatest problems. Other mashups show the most dangerous traffic intersections or bike paths. There is no way that these applications would have become available without a local government proactively making its crime data available in a reusable format. It is not feasible for a citizen to recode the data. Making it available in a portable format was key to making the data useful to the public.

The format that the data are released in can importantly affect the ability of private parties to make it more readily accessible to and useful for the public. A non-manipulable file may be needed for some purposes, for example where proving the authenticity of the data is critical, but raw data should also be made available to enable programmers to create new mashups and innovative applications.

Ultimately, government data is useful to the public only if users can search and navigate the data. Private sector innovation will supply many innovative approaches to the solution of this “ease of use” problem – if potentially useful data are provided in appropriate formats.

Ensuring that data is released in useful formats

When federal datasets were released on Data.gov, the Apps for America 2 contest[1] resulted in many online applications that made the data more useful to the public. Formatting issues can prevent programmers making use of government data that is theoretically available online. For example, releasing sets of statistics in the PDF format does not allow citizens to manipulate the data to generate new conclusions and innovative interfaces. Presentation of complex data in visual formats chosen by the government on government websites like Recovery.gov is important and useful, but the release of the raw data, in flexible formats, serves an equally important purpose by enabling private sector innovation.

To allow for innovative uses, programmers must be able to access data, download it, and track changes over time, when applicable. This allows them to incorporate the data into useful systems and reused in innovative ways.

In some cases, making information available to the public in usable formats also makes it more readily available to other government agencies. For example, the TARP database would inform both the public and the government – enabling oversight from both private sector watchdogs and journalists and from other government agencies and would permit reuse of relevant information for both public and private purposes. Currently, such reuse is difficult insofar as the data is locked inside many smaller sources or released in non-computable formats.

Identifying dataset that will be useful to the public

Agencies should proactively identify and release the types of data sets that are most useful to the public. These high value data sets will ensure that the data is used in useful ways. CDT has released a series of reports on the Ten Most Wanted sets of information and data that are not available from the government, and these serve as a starting point for the kinds of information that would be seen as immediately useful to

[1] Apps for America 2: The Data.gov Challenge, <http://www.sunlightlabs.com/blog/2009/apps-america-2-datagov-challenge/>

the public[2]. However, they are not the only kinds of data that should be made portable – innovative new uses of information will occur as data is released.

Different kinds of information are useful to different people. The government possesses three main kinds of data: information about how the government itself operates (often sought by advocates and watchdogs), statistics gathered in the course of government missions, and scientific data generated by federal agencies. Each of these kinds of information is useful to the public. It is important to proactively make all three kinds of information available to the public.

Privacy concerns for releasing government data

While making useful government information available to the public online has great potential, there are some important privacy issues associated with data disclosure. Readying data sets will require, prior to release, checking that they do not contain personally identifiable information, sensitive information, or other information that could be used to link the released data to individuals. CDT has released a whitepaper on the challenge of data de-identification that may be useful in this context.[3]

III. Identity Management and Government Services Delivery

The extension of broadband across the nation has the potential to enable access to services for citizens who simply cannot reach an appropriate government office in person. In addition, it will enable e-government tools and services on federal Web sites that allow personalization for users. Such government services may involve the collection and use of personal or confidential information, and it may be necessary to confirm or authenticate the identity of a user before providing access to government data. Therefore, achieving digital democracy requires addressing the question of identity management.

---

[2] Show Us the Data: Most Wanted Federal Documents, a joint report by the Center for Democracy & Technology and OpenTheGovernment.org, <http://cdt.org/righttoknow/20090320_TopTenReport.pdf>

[3] Data.gov and De-Identification Considerations for the Open Government Directive, <http://www.cdt.org/policy/government-information-datagov-and-privacy-implications>

In order for online transactions with government to become richer and more complex, individuals will need to be asked to identify themselves. Sometimes, this will be a simple self-asserted identity or pseudonym, perhaps verifying access to a personalized news feed or customized web page. Other times, individuals will need to provide more information about themselves to the government, necessitating more robust authentication of this information. The National Broadband Plan should address the privacy implications of identity management systems used to provide personalized services online.

If the privacy and data security concerns are adequately addressed, there is great potential for creating more valuable trust-based citizen to government relationships online. Moreover, thoughtful government-enabled solutions to identity management systems can enable the creation of valuable, innovative transactions in the private sector as well. If the privacy issues associated with identity are not adequately addressed, the goals of digital democracy could be seriously undermined.

Current state of identity management

Identity management is a broad term, encompassing all manner of systems that serve to identify individuals, prove identity, authenticate attributes and control access to online systems and particular information. This field is developing quickly, and many different parties are bringing new solutions to the marketplace.

New models for identity management separate the “identity service provider” from the “relying party” that needs some information about the user, allowing users to log in to thousands of websites using a single set of credentials. Such “user centric identity” systems, if carefully designed and implemented, can give the user greater privacy protections and greater control over what information is provided in connection with any given transaction. They can also provide the relying party with greater assurance that the identity information is accurate, while lowering costs for systems that no longer have to implement their own identity management systems. A trust framework often connects the user, the identity provider, and the relying party, laying out a set of conditions that each party should adhere to in order to maintain a trusted system.

Currently, the federal government is beginning to work on ways to make use of these improved identity authentication technologies. The Federal CIO Council has an Identity, Credential, and Access Management subgroup (ICAM) that has recently released a set of requirements and processes for the adoption of third party identity management systems by government agency relying parties[4]. Other subgroups of the CIO Council's Information Security and Identity group are working on identity issues related to cybersecurity.

The responsible use of new identity management technologies in government is an important complement to the deployment of broadband. These technologies and policies could enable federal agencies to provide citizens with greater access to government services. And government can take steps to encourage private sector uses of identity management systems that increase the potential for trusted transactions online while also protecting privacy.

Spectrum of credentialing

When individuals are asked to identify themselves, there are many ways to do so. For example, a users can identify themselves as "anonymous", "someone with a specific fictitious name who has visited this site before," "someone who lives in California," or "the Jane Smith that was born in California 35 years ago and has a specific taxpayer identification number." These identity "claims" lie on a spectrum of identity credentialing ranging from lower to higher "assurance" and lower or higher risks to privacy and/or risks from data insecurity.

An OMB memo[i] in 2004 defined distinct "levels of assurance." Each level of assurance (LOA) is based on the principle of proportionality – that is, collecting no more data than necessary in order to successfully implement a particular type of government service. Specifically, GSA and OMB set out four levels of assurance:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity

[4] Identity, Credential and Access Management (ICAM), <http://www.idmanagement.gov/drilldown.cfm?action=icam>

- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

Each of these levels offers a range in which agencies can work to determine the proper authentication tool (if any) to provide the needed level of assurance. Level 1 offers a particularly large range of possibilities. Under Level 1, an agency could choose to use a limited authentication system verifying that a user has established a self-asserted pseudonymous relationship with the website, or use no authentication at all. For the purposes of simply visiting a Federal government Web site containing general information available to the public, the lowest iteration of Level 1 - no authentication necessary - is clearly the most appropriate assurance level. While this would maintain user anonymity as far as the agency is involved, it is important to note that this would not impact the ability of law enforcement to collect information about the user when there is probable cause to do so.

As government websites offer more personalized services to the public, a non-anonymous Level 1 assurance becomes necessary. For example, maintaining a set of log-in credentials with a particular agency to enable attributed comments on their blog should be kept at a pseudonymous level 1, as comments can be moderated and commenting is not generally risky to the agency or the user. As government websites provide users with services that require the website to locate the user or require financial information, then it is appropriate to require the user to provide the website with personal information at level of assurance 2 or 3 in order to authenticate the user and mitigate potential risks such as fraud and identity theft. When dealing with particularly sensitive information, such as intelligence data, level 4 assurance becomes appropriate.

This spectrum of authentication credential options, ranging from anonymity to full identity, with pseudonymity as a key intermediate option, is important for both protection of privacy and security. Without the options provided by such a full spectrum of authentication solutions, it is likely that more information would be collected than is necessary and both privacy risks and data security risks would increase.

Federal ID pilot programs

As noted, the U.S. government is launching a series of pilot programs that will use third party user credentials to authenticate users to federal Web sites in order to provide a better user experience. Using third parties to authenticate users makes sense in many ways, allowing users to use credentials they already have (rather than yet another set of user name and password) and allowing agencies to free up development resources for other tools, instead of maintaining their own sign-on system for all users. In addition, a third-party authentication system with multiple identity providers allows the federal government to avoid creating a national identity database.

In order to work with the government, third party identity providers are creating identity schemes that are trusted by the government – these schemes are part of trust frameworks that outline the ways that identity providers will ensure that users are properly credentialed to government websites. The creation of robust trust frameworks for government use, as well as for general use, requires that identity providers and trust framework providers work together to answer a set of questions around the provision of identity and services online. CDT has published a whitepaper that identifies important issues that must be resolved as these types of identity management programs are established[5].

The development of trust frameworks for user centric identity provides a unique opportunity to design truly user-centric and privacy protective identity management regimes. Determining the obligations of each party interacting within the auspices of a trust framework will be the key aspect of creating such “trust frameworks.” Creating appropriate relationships between each of the parties in a user-centric federated identity system will in turn create stronger, more trusted relationships online.

Any such trust framework should:

- impose and enforce some set of rules that increase trust in associated identification services, thereby enabling productive transactions between

[5] CDT Discusses Key Policies Issues Surrounding User-Centric Identity Management, <http://www.cdt.org/policy/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management>

strangers;

- allow flexible evolution of the relevant services and support an adequate business model for participants;
- be robust against fraud or manipulation, protect the privacy and security of user data, and provide appropriate avenues for dispute resolution, redress, and/or liability in the event of performance failure; and
- be adequately open to new participants without eliminating minimum qualifications and rules.

One reason that CDT supports government use of third party identity providers is to avoid the creation of a centralized national ID database or system of linked databases. Developing a single database for all would create a massive and potentially vulnerable centralized repository of highly sensitive personal information on almost every American. There is no legal or technical framework robust enough to ensure the security and privacy of personal information stored in such a centralized, privatized, ID system. Such a centralized ID system would be a "one stop shop" and treasure trove of valuable information for identity thieves, terrorists, and unscrupulous government employees.

The use of identity management by government will allow citizens to access services online that require personal or confidential information. It is important to ensure that the identity systems used by government will create trusted relationships online and allow users to control the information that is passed to the government. In addition, it is important to ensure that a centralized national database of identity information is not created and held by the government.

Respectfully submitted,

Heather West
Center for Democracy and Technology
1634 I Street, NW
Suite 1100
Washington, DC 20006
202-637-9800

December 9, 2009