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 #29	)	

JOINT COMMENTS OF PUBLIC INTEREST GROUPS

We the undersigned respectfully submit these joint comments in response to the Commission's NBP Public Notice #29 regarding privacy concerns and expectations with respect to broadband applications in the context of the development of the Commission's National Broadband Plan.[1] We commend the Commission for its commitment to carefully considering the privacy issues inherent in this topic.

There are a number of powerful online applications on the horizon that can provide great societal benefit, including e-Government, smart grid technologies, and electronic health records. These applications both depend for their success on the widespread availability and affordability of broadband and at the same time could drive demand for broadband services. In a virtuous cycle, they both depend on broadband and could help spur further broadband growth.

However, these applications also pose risks to consumer privacy because they involve the collection and exchange of sensitive personal information and in some implementations will require the development of more robust identification and authentication services. Therefore, their acceptance – and hence to some extent the future of broadband development – depend on the degree to which consumer privacy is protected. To increase consumer trust and truly achieve broadband's potential, these applications require a robust and comprehensive privacy protection framework.

Currently, the United States does not have such a comprehensive privacy protection law. Debate has occurred in Congress on the issue and the Federal Trade Commission (FTC) is taking a fresh look at privacy. The National Broadband Plan offers an excellent opportunity to give impetus to the development of a comprehensive privacy law. In its report to Congress, the Commission can contribute to the development of privacy policy in the US by highlighting the role of trust in promoting adoption of broadband-based applications and

[1] While this statement presents our common Vision and Principles, please note that the individual signers may also separately file more detailed comments to address the Commission's specific questions.

the risk if privacy is not protected. We call upon the Commission to address in its vision the role of privacy in promoting broadband adoption.

In assessing consumer expectations of privacy, the Commission need look no farther than the comprehensive privacy principles known as the Fair Information Practices (FIPs). The FIPs, first developed by the Department of HEW in the 1970s, are now universally recognized. These principles have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and the other "sectoral" federal privacy laws that govern commercial uses of information online and offline in the US. We strongly believe that the FIPs remain relevant for the digital age and now need to be re-emphasized and codified to address the dramatic advancements in information technology that are underway.

More recently, a comprehensive set of FIPs was endorsed by the Department of Homeland Security (DHS). DHS's formulation of the FIPs offers a robust set of modernized principles that should serve as the foundation for any discussion of legislation, regulation or self-regulation in the online sector.[2] These principles, as articulated by DHS, are as follows:[3]

- **Transparency.** *Entities should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of information.*
- **Individual Participation.** *Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.*
- **Purpose Specification.** *Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.*
- **Data Minimization.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as is necessary to fulfill a specified purpose.*
- **Use Limitation.** *Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.*
- **Data Quality and Integrity.** *Entities should, to the extent practicable, ensure that data is accurate, relevant, timely and complete.*
- **Security.** *Entities should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*
- **Accountability and Auditing.** *Entities should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

---

[2] *See* U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[3] However, here we apply the DHS principles more broadly to data collecting entities in general.

We urge the Commission to endorse the FIPs and to recommend them to policymakers as the best available basis for policy guidelines of all types.

Despite the unprecedented challenges to privacy in the modern environment, the United States still has no comprehensive law protecting consumer privacy rights. Adoption of such a framework should be one of the essential components of the National Broadband Plan. While many of the policies that can help ensure online privacy are outside the Commission's jurisdiction, the National Broadband Plan offers a valuable opportunity to highlight the need for privacy protection, to endorse the FIPs as a detailed framework for privacy protection, and to recommend that Congress and other regulatory entities take appropriate action.

Respectfully submitted,

Ari Schwartz
Vice President & Chief Operating Officer
Center for Democracy & Technology
1634 I Street, N.W., Suite 1100
Washington, DC 20006
(202) 637-9800

Lewis Maltby
President
National Workrights Institute
166 Wall Street
Princeton, NJ 08540
(609) 683-0313

Linda Sherry
Director, National Priorities
Consumer Action
PO Box 70037
Washington, DC 20004
(202) 544-3088

Robert Ellis Smith
Publisher
PRIVACY JOURNAL
PO Box 28577
Providence, RI 02908
(410) 274-7861

Susan Grant
Director of Consumer Protection
Consumer Federation of America
1620 I Street N.W., Suite 200
Washington, DC 20006
(202) 387-6121

Frank A. Pasquale
Loftus Professor of Law,
Seton Hall Law School
Associate Director, Center for Health & Pharmaceutical Law & Policy,
Seton Hall University
One Newark Center
Newark, NJ 07102
(973) 642-8485

The CryptoRights Foundation, Inc.
(415) 333-3003

January 22, 2010