The remarks of General Counsel Cameron F. Kerry
As prepared for delivery at the OECD 30th Annual Privacy Guidelines Conference
Jerusalem, Israel
October 26, 2010

It's a pleasure join friends and colleagues from all over the world to recognize the OECD's contribution to privacy and Israel's addition to the OECD.

The topics of this conference recognize that there have been tectonic shifts in the way the world uses information technology, the amount of information we all entrust to third parties, and the ability to store and manage all this information.

The conference is timely because, in light of these changes the time has come to adapt the legal and policy framework and avoid fragmented, inconsistent, and unpredictable rules that frustrate innovation and undermine essential consumer trust.

In the United States, the current privacy framework is the product of diverse legal, political and cultural forces, as well as decades of exchange with foreign and international systems. Fair Information Privacy Practices first promulgated by our Department of Health, Education & Welfare as a response to mainframe computing in 1970 and expanded by the OECD's farsighted work are deeply embedded in American law, values, and practices.

Our approach is rooted in the Fourth Amendment to the U.S. Constitution, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." American jurists linked this protection — traditionally limited to protecting physical property and space from government searches — to a broader freedom that extends to interests in individual autonomy and privacy.

These same interests are protected by a robust common law system that protects the basic norms of individual personality and democratic participation.

Within the broad context of constitutional and tort and property rights systems common law privacy protections, an array narrowly-tailored commercial data privacy rules applies to specific sectors with different rules applying to the financial, medical, and telecommunications industries, among others sectors, and numerous states adopting data breach laws and other forms of privacy protection.

Buttressing these laws and legal remedies is a robust system of industry self-regulation, combined with informal agency guidance and enforcement by the Federal Trade Commission and state attorneys general.

Taken together, these strands weave a fabric of privacy protection as strong in practice as any omnibus system. The protections they provide against unlawful use of

information online — whether by businesses, by malicious actors, or by government — enabled Internet commerce to take root and grow rapidly in the mid-1990s, and flourish since then. In 2009, online retail sales accounted for over $140 billion in sales in the U.S. alone. This measures just a portion of the economic impact and none of the social, cultural, and political impact in the U.S. and around the world.

As U.S. policymakers set out to improve on this multifaceted system, we have two simultaneous goals: to shore up privacy protection, and to preserve the unique online environment that has allowed for sustained commercial growth on a global scale.

Properly implemented, our work can strengthen and clarify privacy protection practices, encourage innovative technologies that offer consumers meaningful protection, harmonize laws domestically and internationally, and facilitate new technologies and applications that benefit consumers as well as spur economic growth.

In recent days, the White House announced formation of a Privacy and Internet Policy Subcommittee of the National Science and Technology Council. This subcommittee – which I co-chair along with Assistant Attorney General Chris Schroeder – is working to coordinate federal agencies in an effort to promote a broad, visible, forward-looking commitment to a consistent set of Internet policy principles. These core principles include facilitating transparency, promoting cooperation, strengthening multi-stakeholder governance models, and building trust in online environments.

Our subcommittee is working closely with the Commerce Department's Internet Policy Task Force. Our Task Force leverage the expertise of the National Telecommunications and Information Administration, the US Patent and Trademark Office, the National Institute of Standards and Technology, and the International Trade Administration. At the Department of Commerce, we have taken steps to make sure our own house is in order by appointing as a fulltime Chief Privacy Officer a capable privacy professional known to many of you Jonathan Cantor.

Through its Task Force, the Department is conducting a broad review of the nexus of privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the digital economy.

Privacy has been our first order of business. The Task Force recently published a Notice of Inquiry asking for comments on current privacy rules in the US. From these comments and other discussions, the Department is laying out a path to a unified and dynamic privacy framework.

Some of the key themes of this framework include:

- Reinvigoration of Fair Information Privacy Practices that would provide a baseline level of privacy protection across the various contexts in which recorded data is being used.

- A multistakeholder process that would augment the protections of the FIPPs so new self-regulated privacy protections can emerge alongside technological innovation.
- The possibility of a federal privacy policy office to coordinate unified federal privacy policy.
- A renewed commitment to global interoperability by redoubling our collaboration with multilateral organizations engaged with global privacy standards and principles.

Each of these elements would facilitate our ability to design and implement innovative privacy-enhancing technology:

- New FIPPs would guide industry in enabling users to make smarter choices about online information.
- A stronger self-regulatory framework could guide industry to offer privacy-protecting technology and best practices to their consumers.
- A federal privacy office would help our efforts to bolster the role of privacy policy and urge greater privacy by design. Such an office would work closely with the FTC, while respecting its status as an independent enforcement authority.
- A focus on global interoperability and international standard-setting would help create a predictable environment in which consumers could trust their data is being safeguarded and businesses would have consistent rules across international boundaries.

We are finalizing a discussion paper that will present these proposals and others for public feedback. This process will inform the work of our interagency policy discussions and our views on the several bills that taking shape in Congress.

The United States has embarked on active discussion of an enhanced privacy framework. There is broad recognition that privacy protections are crucial to maintaining the consumer trust that is essential to nurturing the Internet as a political, educational, cultural, social, and business medium.

Our challenge is to create a global and interoperable Internet landscape that enlarges prosperity and democratic values while providing meaningful tools to empower individuals to make informed and intelligent choices for protecting their privacy.

I can promise you the United States will be engaged in this effort with our international partners. I hope that our country's efforts toward a more unified and adaptable privacy framework can contribute to the work of this organization and our international partners as we continues to shape principles that balance privacy with the free flow of information in an interconnected world.

Thank you.