STATEMENT OF NANCY L. HURST
NOMINEE FOR SECRETARY OF INFORMATION
May 1, 2014

Thank you, Mr. Chairman, Senator Grassley, and members of the Senate Judiciary Committee, for your invitation to appear before you today. It is an honor to be nominated for this newly created Cabinet post under the direction of President Obama.

Why was this new Cabinet position created? Twenty-five years ago, a computer scientist named Tim Berners-Lee proposed the development of a distributed information system, the World Wide Web, for the CERN laboratory in Geneva. Conceived as an alternative to closed communications systems; this was the invention of the Internet. By 1993, this website's source code and the first popular web browser software, Mosaic, had become publicly available, making the Internet free and available to all. Since then, we have seen the explosive growth of a digital/technology revolution that profoundly affects almost every aspect of our lives.

Most of us here today began our adult lives before these inventions and opportunities. Most of us would be considered "digital immigrants," that is, we have had to learn and adapt to this new digital technology, much like learning to speak a new language as immigrant adults. These innovations and inventions have come at us as if we are drinking from a fire hose. However, we know that our founding fathers had no idea of the changes ahead that would affect us all as stakeholders in our national government, world governments, public and private institutions. It is bewildering, overwhelming, and difficult to know where to begin.

What is the relationship between technology and information? You may wonder why I keep referring to technology when the position name is "Secretary of *Information*." Over a period of hundreds of years, we moved from an agricultural to an industrial economy, but it only took two decades to become an information economy. Technology is simply the new tool used to

generate, communicate, collaborate, and store the new product - information. It used to originate from a centralized source, such as paper, books, speech, and broadcasts; all had physical limitations that allowed for control of content and dissemination; it now originates through the decentralized Internet. Communication used to be private and controllable, now, any type of written or verbal communication/information can be easily disseminated, even without any of the parties' approval or knowledge.

The control of information has the power to influence almost all economic, social, economic, and political decisions; therefore, information control profoundly affects who controls power. Information is too valuable to be free, and has become a commodity, a valuable asset. Thus, we must develop comprehensive policies that will balance the rights of individual users against the needs of institutions and governments. We cannot continue to enforce our current outdated policies and laws. The framework for using technology for the exchange of information must be constructed in such a way that it is efficient, secure, productive, legal, and ethical, using new sets of rules and institutions, and based on our needs and values.

What are our needs and values? Among and between the different groups consisting of individuals, governments, public and private institutions, the needs and values will often conflict. For example, the individual wants privacy and security, but the corporation wants to know as much as possible about the individual to sell advertising or increase its market share. The government wants information about foreign nationals and governments, as well as its own citizens, to maintain national security. As the information state continues to grow, we have seen governments deliberately increase their control over information creation, communication, and use it to wield power. We also know that there has been a huge growth in criminal activities

where personal credit card numbers, information, and identities are stolen, sold, or used for other illegal purposes.

But, who owns and controls the Internet? Who owns, and thereby controls and benefits from using your personal information: your email, your address, your shopping preferences, and your Internet searches? Who has the ability to control content, and the prices for obtaining content? Who ensures that the rights and duties of users, corporations, and governments are balanced while maintaining an open and neutral system?

I believe that it would be helpful here to examine some recent events so that we may gain a better understanding about why change is needed.

We are all aware of the National Security Agency's demands to Internet and telecommunications companies, such as Verizon and Google, to provide the NSA, on an ongoing basis, with information about any calls made between the United States and abroad. These non-governmental institutions were required to provide this information under FISA subpoenas. The US FISA court, established by Congress under the Foreign Intelligence Surveillance Act in 1978, had its secretive powers strengthened by Section 215 of The USA PATRIOT ACT, and again under the FISA Amendments Act of 2008. These warrantless searches need only be justified by the government's "reasonable belief that a target is outside the United States," and come with an all-encompassing gag order. Many feel that these searches violate the First and Fourth Amendments. "Defendants" are not informed, may not discuss their involvement, nor are they allowed legal counsel, and the court's legal determinations are secret. NSA analysts have vast discretion about what they may collect, and are not required to justify searches to the FISA court. Of the tens of thousands of FISA warrants requested, almost all are granted. In addition to the original warrant, the FISA court also allows two collection "hops." This means that the initial

target's email, calls, and correspondence are collected, and it collects the same information from everyone in the target's address book, and then again from everyone in those address books. Encrypted files or messages can be stored forever, at the NSA's discretion.

The USA PATRIOT ACT of 2001 was enacted because of events occurring September 11, 2001, when nineteen terrorists hijacked and crashed four US airliners. Fearing more attacks, President George W. Bush and Congress acted swiftly by creating new legislation; the USA PATRIOT Act. The final bill was 342 pages long and changed more than fifteen existing laws. Cleverly titled to promote immediate passage, the acronym stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." Claiming that more attacks were imminent, President Bush and Attorney General John Ashcroft urged Congress to pass the bill immediately, without change, deliberation, or debate typical of most legislation. It was enacted forty-five days after the attacks. The vote was taken under a suspension of the rules to cut off debate early to quickly pass the bill. Those of you who were sitting Senators or Representatives at that time voted for The USA PATRIOT ACT in 2001, and, with the exception of Chairman Leahy, voted for the ACT again in 2006. The original Senate vote was nearly unanimous at 98-1, and 357-66 in the House.

The only senator to vote against was Senator Russ Feingold of Wisconsin. Some of the reasons that he felt that the bill "did not strike the right balance between empowering law enforcement and protecting constitutional freedoms…" were that the NSA would be able to:

- Execute warrantless searches based simply on "reasonable cause" if the NSA believes that intelligence gathering is a "significant purpose," rather than the higher "probable cause" required under the Fourth Amendment,
- Monitor computers without probable cause, for as long as they wish,
- Collect any and all business records of anyone who might they might wish to investigate under the guise of investigating terrorism,

- Implement fishing expeditions without judicial oversight.

Does The PATRIOT ACT affect go too far in restricting our citizens' rights under the First and Fourth Amendments? Do you know whether you or your family members, friends, or colleagues have experienced any of the invasions of privacy that have been described as possibilities by Senator Feingold? How effective has this program been in thwarting terrorism? Only the NSA, with virtually no external oversight, knows this information. Based upon what we all now know about the NSA vacuuming up data supplied by Google, Apple, Verizon and other providers, and the nature of your positions as leaders in the US government, it is quite possible that that emails, phone calls, or any electronic communication about you, your spouse, your family members and your friends may have been collected by the NSA. You could ask them; they will not tell you. The US government's worldwide reputation has suffered, as NSA's surveillance of other world leaders, including German Chancellor Angela Merkel and Brazilian President Dilma Rouseff, became public knowledge.

We know much more about this and other US government surveillance programs due to the disclosure of classified documents approximately one year ago by a then 29-year-old high school dropout and government contractor named Edward Snowden. Some view him as a heroic whistle-blower, whose stated motive was "to inform the public as to that which is done in their name and that which is done against them." What does this say about our government's ability to secure classified information? How safe is our collected personal information if one individual is able to obtain access to thousands of classified documents? How should the US government address its charges of espionage against Snowden as he receives temporary asylum in Russia, while 2014 Pulitzer Prizes were awarded to the very publications that published the leaked documents? Why weren't these publications also charged with espionage?

The President states that he is now working with lawmakers to revise the means by which the data obtained by private enterprise is stored, that is, the data would not become automatically available to the NSA upon their request. Is this too little, too late?

If the Internet content is free, then how does Google make money? We don't pay Google to use its browser to access content. Any discussion about technology and information must include an acknowledgement of the company called Google and how its growth has contributed to information accessibility. It began in the 1990s with founders Sergey Brin and Larry Page following their aspirations to "organize the world's information." Initially, they were against using an "advertising funded search engines" model, believing that this would cause a bias toward advertisers and away from consumers. They believed that their revenue sources would be earned from licensing their search engine technology to other companies. In a 1999 press release, Google included the statement that they want to "organize the world's information and make it universally accessible *and useful*." In 2000, they decided to introduce a very restricted ad format as an experiment, and subsequently changed their minds about selling ads when they "accidentally" discovered that plain text advertisements produced in enormous profits.

Today, Google, as well as many other websites we visit, are regularly collecting information about us as users. Online and retail shopping establishments collect information as well. This can include your name, address, email, credit card information, services that you use, how you interact with their ads, search queries, phone numbers, what you purchase, and location information. They are also likely to install "cookies" on your computer that they tell you are used to improve their services and to offer more personalized and relevant search results and ads, and are usually a condition of using their services. This information is often shared with or sold to other companies, organizations, and individuals. These days, almost any site that you visit will

want to install “cookies,” which allow websites to collect certain information about how you use the site and provide information to be used for advertising. However, cookies can be used for malicious purposes such as spyware. You should expect that most of your Internet activity will be tracked by various organizations unless you know what specific actions you could take to prevent it. This information may be contained in your user agreement or privacy policy; did you read it thoroughly?

How safe is your collected information? Credit card information has been stolen when retailers Target, Neiman Marcus, and others have recently been hacked using malicious software developed by a seventeen-year-old Russian, who then sold it to other cybercriminals. Skimmers can be placed on ATMs and credit card machines to record your information. Identities are stolen from credit card applications, employer files, medical records, or directly from your own devices by the use of malware.

Governments, business institutions, and criminals all collect information about individuals through legal and/or illegal means. Governments collect without your knowledge, businesses collect by requiring you supply personal information as a condition of doing business as well as requiring your acceptance of multi-page contracts full of legal jargon meant to protect the business from the individual. The criminals collect through aggressive “phishing” tactics, malware, and invasive software. How can users protect themselves?

These are just a few of the issues requiring our attention as the information age progresses. Where do we begin?

We need an Internet Bill of Rights. As Secretary of Information, I hope to enlist the acknowledged inventor of the Internet, Tim Berners-Lee, as one of my advisors. When he introduced the World Wide Web technology in 1989, it was meant to be free and available for

anyone to use. He now believes that an Internet Bill of Rights is needed to protect the "open, neutral" system necessary to provide equal access and to protect the privacy of its users. Our Internet Bill of Rights must balance the responsibilities and rights of individual digital users, public and private institutions, and government, while maintaining an open and decentralized network by:

- Requiring net neutrality – All Internet data must be treated equally, without allowing Internet Service Providers the ability to decide content speed or limitations,
- Regulating government surveillance - limit the gathering and use of metadata on our citizens,
- Establishing that service providers will not be liable for user-published content,
- Placing limits on the amount of information that business can collect about individuals,
- Requiring reports be made available for individuals, similar to a credit report, that include all data collected about them by government and businesses,
- Promoting the Internet as a Commons to ensure equitable access to Internet resources for all citizens, and reach out to those who currently do not have the means. We must acknowledge that digital communication provides education and access to services that are key to our healthcare and economic growth as a nation.

What other legal, ethical, and practical issues need to be addressed to reflect the realities of new technology?

- We must revise the format of contracts that users are required to accept so that they do not have to divulge unnecessary personal information. Contracts should be written understandable language instead of typical legal jargon, length should be minimized, and restrictions on vendors and users should be balanced.
- Institutions must be financially accountable to their customers for the consequences of security breaches; a "year's worth of credit reports" is an inadequate deterrent. They must be required to report breaches immediately to both law enforcement and to their customers.
- Vendors should not be able to limit their own liability to a minimal amount typically stated in their user contracts, nor should they be able to eliminate customer rights normally available under the law.

- Numerous laws and regulations currently exist requiring compliance from companies that use the Internet to do business. These laws should be clarified and revised into a simpler, limited format to enable reasonable compliance from the business owner.

- Intellectual property laws need to be revisited to ensure that innovation is encouraged and to reflect the reality of sharing and distribution afforded by digital technologies. These issues are especially challenging as they pertain to software development, trademarks, patents, medical research and development, and artistic creativity, requiring a balance between rewarding innovation and restricting dissemination.

- We must revise the National Archives and Records Administration retention policies to ensure that consistent guidelines for all federal agencies are followed, including the executive branch. These policies should be free from political decisions and fall under the purview of the Secretary of Information.

- We must explore how individuals can control their personal information, rather than having to provide it, free, to other organizations so that others may commoditize it.

- The US government must require industry best practices for its own security systems and collaborate among its own agencies in sharing common-use data.

- We need watchdogs and accountability for government actions and for the protection of our citizens.

- We must provide a safe resource for government whistle-blowers so that they do not undertake the type of drastic revelations as Edward Snowden in order to force accountability of our own government.

- We must protect our children from predators. Phone companies should educate parents about the laws governing "sexting"; that if a photo is of a minor, it is a felony and is considered child pornography. Even minors can be criminally prosecuted and placed on a registered sex offender list. Children should also be explicitly warned that NOTHING is private on the Internet!

- Employers must inform employees that if they wish to maintain digital privacy, they should not use their employer's devices for personal communication or search activity.

The role of the Secretary of Information should be to develop a team of advisors and staff that originate from corporate, government, public institutions, academia, and the legal community to develop national information policies and laws regarding the creation, communication, use, and storage of information. We must explicitly incorporate an ethical framework for the development and use of information technology. These policies must reflect

contemporary issues, be comprehensive, productive, efficient, secure, legal, ethical, and anticipate future developments.

How do we implement new information policies? You, as lawmakers, must take responsibility for educating yourself about these issues so that you are prepared to introduce new legislation. You must understand how new technology works; to change the laws that may criminalize unsuspecting innovators or users, but protect outdated entertainment institutions; or that protect the gigantic business interests and government intrusions at the expense of the individual. You must set aside partisan politics and the interests of the well-funded lobbyists, and respond to the needs of your individual constituents. You must evaluate the effects of the far reaches of the NSA, the FISA court, and The USA PATRIOT ACT; and question whether the rights of our citizens been compromised, and whether these dragnets have accomplished any tangible results in combating terrorism. We must ensure that the original checks and balances among our three branches of government still operate effectively. We cannot allow the Internet to be dominated by government and corporate interests at the expense of its users. It is time for us, in collaboration with other countries, to develop information policies that recognize that access to information on an open, neutral Internet is necessary for economic growth and prosperity.

I acknowledge that much of the work ahead is undefined, unknown, and has little precedent. However, we must not delay in examining our future; we must take back our leadership role in collaborating on the international stage while providing the best guidance for our own citizens.

Thank you, Mr. Chairman and Members of the Senate Committee on the Judiciary, for your time and attention. I would be happy to take your questions.