Statement of Susan Grant, Director of Consumer Protection and Privacy

To the Commission on Enhancing National Cybersecurity

August 23, 2016

I'm Susan Grant, Director of Consumer Protection and Privacy at Consumer Federation of America (CFA), an association of local, state, regional and national consumer organizations and state and local government consumer protection agencies from across the Unites States. I appreciate your inviting me to speak with you today about the challenges confronting consumers in the digital economy. The challenges are many, from unfair and undisclosed digital rights restrictions to Internet fraud, problems with interoperability to systems failures such as the recent computer meltdowns at Southwest and Delta Airlines. My focus today will be on concerns about privacy and security. I am not a technologist, which is a good thing for my work on these issues, because my views are from the perspective of the average consumer.

Consumers want and need to use digital products and services

The Internet and digital products and services have become essential parts of our lives. We use them to access government services; to buy and sell things; to bank, invest and borrow; to pay our bills; to raise money for charitable causes and make donations; to create art, music and literature; to obtain health care services; to teach and to learn; to keep in touch with friends and family; to publicly share our experiences; to entertain ourselves and others; and to participate in our democracy. Seventy-two percent of Americans own smartphones and 89 percent use the Internet, according to a February 2016 Pew Research Center study.

Indeed, we have little practical choice about using the Internet and digital products and services. Many government benefits are delivered electronically. Smart cards are replacing cash and tokens for public transportation. In some communities smart meters are mandated for our homes. Other appliances that were once "dumb," such as refrigerators, are being turned into digital devices that do much more than the basic functions they used to perform, including track our behavior. Dedicated short range communications services will be installed in new cars starting next year. Some schools require students to use computers. Electronic health records systems are being implemented. In some cases, the only way to communicate with companies, obtain owners' manuals, and get service when we have problems is online. We live in a brave new world built on ever-accelerating technological advances.

These advances can help make our lives easier and safer, save us time and money, spur creativity and civic discourse, and enlarge our voices individually and collectively. But they can also make us more vulnerable to commercial and government surveillance, unfair discrimination, anti-competitive practices, and identity theft and other hazards.

Consumers are concerned about their privacy and security but have little control

Privacy is a fundamental human right, but in the U.S. we lack a comprehensive legal framework to protect it. Instead, we rely on narrow sectoral laws and self-regulation, leaving huge gaps. For example, the privacy of our health care records is protected but the data generated by Fitbits and other wearable health devices and health-related apps are not. While financial institutions are under some legal constraints concerning the collection, use and sharing of our personal information, most businesses are not. There is no federal law that requires them to even disclose their privacy practices or to give us any say in what they do. For instance, we have no privacy protection under federal law for the one of one of the most intimate types of personal data, our facial images. The privacy best practice recommendations for the commercial use of facial recognition technology are so weak that even if they were widely adopted, they provide no meaningful privacy protection. The privacy of our telephone records is protected, but there is a fierce battle underway right now over the Federal Communication Commission's (FCC) proposed rules to protect the privacy and security of the personal information that our Internet Service Providers can derive from our online activities.

Verizon's acquisition of Yahoo is the latest illustration of the fact that these days, the product or service that is being provided may be ancillary to the *real* commodity, our personal data. Information about us – our financial situations, our health conditions, our sexual orientations, our affiliations, our interests, our political positions, and more is gleaned from our activities online and offline, across platforms, analyzed, combined into digital dossiers and used by companies and their affiliates and business partners, or sold to the highest bidder, for profit. We have little insight or control over the accuracy of this information, who has it, and how its use may impact us. Are you receiving solicitations for prime loans while I'm being solicited for predatory financial products? Are you seeing a different price than I am for the same product or service? Are you being unfairly discriminated against on the basis of "big data?" Can your personal information be used in ways that might embarrass you? You can get your credit score and understand the factors that go into it, but do you know about the secret scores that are being compiled about you?

Most descriptions that are provided about companies' privacy practices are deliberately opaque and any controls that consumers may be offered are usually unclear and fairly limited. Where the default is placed matters, and for the most part the burden is on consumers to opt out, rather than on the data collectors or users to obtain their affirmative agreement. AT&T's "pay for privacy" option for some of its high-speed Internet services is wrong-headed because privacy shouldn't be an option only for those who can afford to pay more – it should be everyone's right.

But don't consumers want to exchange their personal information for a discount or other benefits? As a 2015 study showed, that's a fallacy. Consumers recognize that they have little control and that the deal is lopsided. Their resignation should not be interpreted as enthusiasm.

Surveys show that consumers are concerned about their privacy and the risks of disclosing their personal information, even to save money.

Consumers are also concerned about the security of their personal information. A government study showed that 19 percent of Internet-using households reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to July 2015. It seems that not a day goes by without another data breach in the news. Consumers should do what they can to secure their own devices and use safe online practices. But when the data is out of their hands there is nothing they can do to secure it – they have to trust that the data holder will do so. Most of the data breach bills that have been introduced in Congress are not about improving security, they are about setting weak requirements for data breach notice and preempting states that have stronger standards.

When consumers' information is compromised, whether through breaches or trickery such as phishing, it is important to not only learn from the experience in order to prevent it from re-occurring in the future but to mitigate the damage and help consumers recover from whatever fraud might have resulted.

The "Internet of Things" exacerbates concerns about privacy and security because of the amount and sensitivity of data that can be collected about us will increase dramatically and the consequences of privacy or security failures can potentially be far more severe. It is urgent to address privacy and security issues now, rather than wait until business models based on the unfettered collection and use of our personal information, coupled with the lack of investment in adequate security, become so entrenched that it will be impossible to change the facts on the ground. Business will innovate within the public policy parameters that we set.

While my focus today is on privacy and security in the marketplace, there are challenges for digital consumers in government's collection, use and security of personal information as well.

Recommendations for government and industry

- **Privacy should be the default.** We should be asked for our consent before our personal information is used for purposes other than those for which we provided it and not be forced into agreeing or to pay to protect our privacy.

- **Data security should be automatic.** We don't allow consumers to use unsafe products. We have safety standards and recalls. We shouldn't let consumers use unsafe digital products and services. Security should be built in.

- **Industry should be required to protect consumers' privacy and security.** We need enforceable laws, not more self-regulation, which has not sufficed and never will.

- **The Administration should back rulemaking for privacy and security.** The Administration should express strong support for the FCC's broadband privacy and security rules and

advocate for the Federal Trade Commission to have the ability to promulgate such rules for the business sectors over which it has jurisdiction.

- **The United States should establish a Data Protection Authority.** We need a central authority that will coordinate government policies concerning privacy and security.

- **A central source should be created to access data brokers and the information they hold.** We have a central source through which consumers can access the credit reporting agencies and their credit reports. This gives them the ability to see what information has been collected about them and correct it if it is inaccurate. We need a similar system for data brokers.

- **Government agencies should consider privacy and security in promoting technology.** For instance, we support calls for the FCC to require car manufacturers to implement privacy and security safeguards in using the spectrum that they have been allocated for the operation of dedicated short-range communications services in automobiles.

- **Government should support the development and use of secure communications tools and technologies such as encryption.** Policies that prevent or undermine these tools expose consumers and businesses to unwarranted security threats.

- **Measures should be mandated to protect consumers' data from abuse.** The Administration set a good example by requiring both chip and PIN for credit cards used by the federal government. Two-factor authentication and other security measures should be encouraged and the use of Social Security numbers as identifiers for purposes other than validation for government benefits should be eliminated.

- **More should be done to educate consumers about privacy and security.** That education should begin early in schools and there should also be more support for programs to educate adults. This will require a major and sustained effort by government, industry and nonprofit organizations and adequate resources.