TESTIMONY OF

JEFFERSON ENGLAND, CHIEF FINANCIAL OFFICER

SILVER STAR COMMUNICATIONS

BEFORE THE U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

HEARING ON

SMALL BUSINESS PERSPECTIVES ON A FEDERAL DATA PRIVACY FRAMEWORK

Chairman Moran, Ranking Member Blumenthal, and other distinguished Members of the subcommittee. My name is Jeff England, and I serve as the Vice-President and Chief Financial Officer of Silver Star Communications.

Silver Star Communications, headquartered in Thayne, WY, is a small telephone and internet service provider, serving nine rural counties, comprising 16,922 square miles, located along the Western Wyoming and Eastern Idaho state border. We are both an independent local exchange carrier, providing regulated telephone services, and a competitive exchange carrier, delivering some of the most cutting-edge internet services available today.

Our company was formed in 1948, with the purpose of connecting rural farmers in the mountain valley in which we live. It is humbling to remember that while we now celebrate being the first company in both Wyoming and Idaho to deliver gigabit internet service to residential customers over a robust fiber optic network, we once delivered basic telephone services along the top wire of a barbed wire fence.

We have seen significant changes in our industry from the days when a “trouble ticket” consisted of determining who was moving cows that day and forgot to reconnect the jumper at the gate, and the largest “privacy concern” was that which was inherent with making a call on a party line.

What hasn’t changed in our company’s 71 years of existence, is our customers’ requirements for privacy and security. Because of this, we have adopted practices designed to maintain the privacy of our customer’s data. We do not sell customer data, and we do not collect and use customer data for the purposes of advertising or “click revenue.”

We have chosen to not collect and monetize this information as a competitive differentiator, and by choosing to not collect this information, we believe we have established trust in our interactions with our customers. We have also observed general trends in online services to suggest that the market is responding to customers desire for increased protections with regards to their data, and it is our position that any legislation considered by this committee should not limit the capability of a service provider to differentiate on the basis of privacy protection practices.

Because we already do not collect and monetize customer information, we do not anticipate online privacy legislation to be overly burdensome so long as it meets certain criteria:

First, there must be consistent application of privacy protections. Legislation should establish consistent privacy protections that are technology neutral and apply uniformly to companies that collect, use, or share consumers' online personal data.

Second, we believe the pathway to success is built upon a federal privacy framework that preempts state privacy laws. We provide services in multiple states, and having to manage a patchwork of state privacy laws will not only create an environment of uneven protections, but would create administrative burdens on small business.

Third, there must be a single federal agency identified with the responsibility to enforce the national privacy framework. Failure to do so would result in inconsistent requirements, uneven protections, and competing priorities. We believe the Federal Trade Commission should have exclusive authority to enforce privacy protection laws at the federal level, with State Attorneys General having the authority to enforce the new federal law. This will allow for consistency in privacy legislation across all industries and companies as well as provide a framework for new businesses and industries to operate within. As a rural internet service provider, we would add that the FCC should expressly be precluded from having authority to enforce privacy protection laws. Failure to prohibit the FCC from enforcing privacy protection requirements would endanger the deregulated status of internet services.

Fourth, legislation should require companies to have a privacy policy that gives users clear and comprehensible information about the categories of data that are being collected, how consumer data is used, and the types of third parties with whom data may be shared. This type of transparency would

enable consumers to make informed decision about the types of services they receive, the businesses with whom they engage, and the data privacy tolerances they are willing to accept in order to receive such services.

Fifth, legislation should not prohibit consumer-friendly incentives tied to privacy choices. Legislation should not interfere with business and consumer relationships that are based on mutually understood privacy protection tolerances. If a consumer is willing to release data in order to receive services, it should be the consumer's right to do so, and the business should be allowed to provide such services. Similarly, the market should be allowed to present data privacy alternatives as competitive differentiation so long as data privacy protection practices are clearly identified and accepted by the consumer.

Sixth, legislation should require companies to take reasonable steps to protect consumer data without prescribing a checklist of regulatory requirements.

Seventh, legislation should establish a consistent national framework and preempt the existing patchwork of state requirements on data security and breach notification. The existing environment causes consumer confusion and needless cost and complexity for companies.

Designing legislation that addresses these seven considerations would be most effective at balancing the privacy protection allowances we as consumers are willing to agree to, while at the same time, creating a business environment that can allow online services to grow and thrive in our digital economy.