

**Written Testimony of Leland Miller, Commissioner
U.S.-China Economic and Security Review Commission
On Chinese Data Dominance and the Weaponization of Data Against
American Citizens**

United States Senate Special Committee on Aging

June 17, 2026

Chairman Scott, Ranking Member Gillibrand, and Members of the Committee, thank you for the opportunity to testify. On April 30, I co-chaired a hearing of the U.S.-China Economic and Security Review Commission titled, “Taking a Bigger Byte: China’s Expanding Strategy for Data Dominance.” What our witnesses described, and what I want to convey today, is that Beijing has stopped treating data as a commercial byproduct and now treats it as an instrument of state power – and that ordinary Americans, including our oldest and most vulnerable citizens, are increasingly the raw material.

The starting point is legal architecture. China’s National Security Law, National Intelligence Law, and Data Security Law together compel any Chinese company to hand its data to the state on demand, in secret, with no independent court able to refuse and no transparency to reveal when it happens. The obligations run one way. As one witness put it, Beijing’s operating principle is to control the outflow of data from China while expanding the inflow from everywhere else. A dataset does not have to hold national security value when it is collected. That value can emerge once the state fuses it with other data in its possession.

Three mechanisms make this concrete for Americans.

First, our networks. Chinese state-sponsored actors, in the campaign known as Salt Typhoon, penetrated the core of America’s telecommunications carriers and reached call-records data – who is calling whom, from where, and when – for vast numbers of Americans. The FBI has assessed that China’s hacking program is larger than that of every other major nation combined.

Second, our commercial data. Sensitive information about Americans – precise location, financial stress, health indicators, and family and professional networks – is openly bought and sold through the data-broker market and absorbed through apps, payment systems, and connected devices. None of it requires a hack. It can be purchased.

Increasingly, these data streams come from products Americans carry, wear, or drive every day. Modern smartphones, connected vehicles, fitness trackers, smart-home devices, and other internet-connected products continuously generate detailed records of where people travel, who they meet, what they buy, how they communicate, and even patterns in their physical activity and health.

In many cases, supposedly anonymous datasets can be re-identified and linked across multiple sources, allowing disparate pieces of information to be fused into highly detailed portraits of individual lives. What appears commercially mundane in isolation becomes strategically valuable when aggregated at scale and combined with other sources of data.

Third, our health and our biology. Witnesses were direct that Beijing regards genomic and clinical data as a strategic national resource and is investing heavily to acquire it — not only genetic sequences, but treatment histories and health records. Artificial intelligence is the force multiplier that ties all of this together: bulk data that was once too voluminous for any human analyst to use can now be fused automatically into detailed profiles of individuals — what one witness called the move from “observation to prediction.”

This is where the risk to older Americans becomes acute. Older Americans hold a disproportionate share of the nation’s wealth, carry the longest medical histories, and are the heaviest users of the health system — which means the financial, genomic, and clinical data Beijing prizes is, in large part, theirs. The same capability that lets an adversary build a targeting profile of a government official also lowers the cost of precision fraud and social engineering against an eighty-year-old: tailored, convincing, and delivered at scale. And the records most exposed to the harvest now, decrypt later strategy our witnesses described — collecting encrypted data today to break it with tomorrow’s quantum computers — are precisely the long-lived medical and financial records that follow an older American for the rest of their life.

The central lesson of our hearing is that Washington still treats privacy, telecommunications security, critical-infrastructure resilience, and artificial intelligence as separate problems. Beijing does not. It is assembling a single decision-advantage architecture, and it is doing so faster than our policy is adapting.

The Commission has not yet developed its recommendations in this space. That will not happen until our report comes out in November. Speaking now in my personal capacity, I would respectfully urge this Committee to act on that integrated view: to place a national-security data regime — covering geolocation, health, genomic, financial, and telecommunications data — on durable statutory footing; to harden the telecommunications and data-broker ecosystems that make American data purchasable

in the first place; and to treat the protection of older Americans' financial and medical data as the homeland-security matter it has become.

Thank you again for the opportunity to share these observations. I look forward to your questions.