**Senate Judiciary Committee**
**Subcommittee on Crime and Counterterrorism**
**Hearing on "Your Data, Their Profit: The Consumer Cost of AI Surveillance Pricing"**
**August 4, 2026**
**QFR Responses: Lindsay Owens, President and CEO of Groundwork Collaborative**

Questions from Senator Amy Klobuchar

***1. In an economy in which consumers are facing rising costs, one of the few ways people can push back is by comparing prices among sellers to find the best deal. How do constantly changing prices affect a consumer's ability to engage in meaningful price comparisons?***

Markets only work if shoppers can walk across the street or open a new tab for a better deal. When prices change from moment to moment, or vary by customer, device, location, or any other piece of personal data, consumers cannot reliably comparison shop. A shopper can only see the price presented to them, with little visibility into what another customer is charged or why their own price changed. Most consumers have no practical way to know whether they are making a meaningful price comparison: detecting personalized pricing requires comparing prices across users, devices, and locations at the same time – a difficult task even for trained researchers.

Consider the JetBlue customer the Subcommittee discussed at this hearing. While trying to book travel to a funeral, he watched the fare rise by $230 in a single day. In a now-deleted social media post, JetBlue's own account advised him to clear his cache and cookies or try booking in a private window. This implied that the personal information the company had collected from his browsing history factored into his price. He has no way to know whether his price was set by the market or by his tragic circumstances. When prices change rapidly or vary based on personal data, shopping around becomes a much weaker check on higher prices. Consumers rarely have the power to negotiate prices directly, so finding a lower price elsewhere is one of the few ways they can push back.

***2. We need to pass a comprehensive federal data privacy law based on the principles of data minimization, transparency, consumer control, and opt-out rights to reduce the amount of information companies can collect and use across the internet. How would passing comprehensive data privacy reform reduce the risk that companies can engage in predatory surveillance pricing?***

Comprehensive federal data privacy reform would curb predatory surveillance pricing by reducing the personal data companies can collect and use to set individualized prices. Surveillance pricing relies on detailed consumer data to estimate consumers' willingness to pay, including purchase history, urgency, income, and more. A January 2025 FTC report found that companies can make those estimates using detailed behavioral data, including how a consumer moves a cursor across a webpage. By restricting the collection and use of personal data, new data privacy legislation would cut off surveillance pricing capabilities at the source.

Some states have advanced comprehensive data privacy reform. However, in the absence of federal protections, consumers are forced to bob and weave through a patchwork of laws which vary across state lines. Thanks to California's privacy reforms, a *WIRED* reporter recently requested the data McDonald's had amassed on him. In response, he received a 515-page dossier. An Oregon customer similarly requested the data Kroger had collected on him and received a 62-page file that included detailed behavioral estimates, including how likely he was to take a cruise – a perplexing detail for a grocery store to want to know. The lucrative business of buying and selling customers' data and the rapid advancement of AI-powered technology have made it possible – and even easy – for companies to use consumers' data to set individualized prices.

Stronger privacy protections would also reduce companies' incentive to collect troves of consumer data. Each new piece of consumer data can help a company refine its estimate of what someone is willing to pay, giving firms a financial incentive to keep collecting more personal information. Companies with the largest consumer datasets can more precisely estimate what individual shoppers will pay, pushing competitors to expand their own data collection through sharing, acquisitions, and consolidation. Further, many retail companies have generated revenue streams well beyond selling products to customers by selling their customers' data: Kroger, for example, sells data from its 63-million-member loyalty program. This book of business is part of its "alternative profits" stream, which accounts for over 35% of its net income. Privacy rules like the European Union's General Data Protection Regulation limit that cycle by restricting unnecessary data collection and requiring companies to justify how they use personal data. A federal law that enshrines data minimization, consumer control, and opt-out rights would similarly make it harder to accumulate the extensive profiles that personalized pricing systems rely on.

The most effective way to protect consumers is to pair upstream approaches, like privacy reform and limits on data collection, with downstream approaches that regulate the use of data that's already been collected, like banning the practice of surveillance pricing altogether.