1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

June 22, 2026

The Honorable Pavel Payano
Senate Chair
Joint Committee on Consumer Protection & Professional Licensure
24 Beacon Street, Room 413-B
Boston, MA 02133

The Honorable Tackey Chan
House Chair
Joint Committee on Consumer Protection & Professional Licensure
24 Beacon Street, Room 42
Boston, MA 02133

RE: CTA Opposition to S.3090 and H.5114, An Act Relative to Consumer Connected Devices

Dear Chair Payano, Chair Chan, and Members of the Joint Committee on Consumer Protection and Professional Licensure,

The Consumer Technology Association® ("CTA") submits this letter to respectfully oppose S.3090 and H.5114, an act relative to consumer connected devices.

CTA is North America's largest technology trade association, representing over 1200 American companies, many of which are based in Massachusetts. Our members are the world's leading innovators – from startups to global brands – helping support more than 17 million American Jobs. We also own and produce CES®, which convened tech leaders and over 4100 exhibiting companies in January.

CTA supports initiatives that empower consumers with greater transparency, including meaningful information about the technology they purchase. However, CTA respectfully opposes S.3090 and H.5114 because, in its current form, the bill imposes disclosures that will create confusion for consumers, inconsistent compliance burdens for companies, and unintended market distortions.

CTA supports consumer transparency regarding product lifecycle, security updates, and support commitments. When consumers understand how long products will receive updates and how vulnerabilities are managed, they can make better purchasing and security decisions. However, CTA believes that the mandatory disclosure regime in S.3090 and H.5114:

1. **Fails to align with federal and international frameworks** that provide standardized, actionable information to consumers across different products and markets.

2. **May mislead consumers** by focusing narrowly on a "minimum guaranteed support time frame" without considering the complexity of modern connected products (e.g., cloud-based services, varying update mechanisms, and security patch schedules). Further, establishing requirements on product packaging will no doubt result in consumers receiving outdated information even despite diligent compliance efforts.

3. **Covers too many products** by explicitly including devices that only indirectly connect to the internet. This could include cloud infrastructure, which manufacturers typically don't control or update.

4. **Imposes compliance burdens on small and medium manufacturers**, particularly those selling across multiple jurisdictions with differing disclosure regimes, without clear evidence that these disclosures improve consumer outcomes.

5. **Requires manufacturers to notify device owners in ways that aren't practical.** Consumer electronics are often reused, resold, or donated, making it difficult to identify and contact current owners—especially beyond the original purchaser, and only if the product was registered. Requiring six months' advance notice is also unrealistic, as manufacturers may not know that far ahead when support or updates will end.

6. **Creates unnecessary litigation risk through a private right of action**. Given the dynamic nature of software and cybersecurity updates, manufacturers may face litigation despite making good-faith efforts to provide accurate information. This exposure is particularly problematic where support timelines can change due to evolving security threats, third-party dependencies, or other factors beyond a manufacturer's control.

7. **Duplicates and potentially conflicts with emerging voluntary labeling systems** designed by federal policymakers and industry working together to present security and support information in a consumer-friendly way.

U.S. Cyber Trust Mark: A Better Model for Consumer Transparency

CTA strongly supports the bipartisan U.S. Cyber Trust Mark, a voluntary federal labeling program managed by the Federal Communications Commission that is designed to help consumers identify products that meet established cybersecurity best practices. To achieve the U.S. Cyber Trust Mark, participating manufacturers must undergo testing and meet criteria that includes transparency about support period, update mechanisms (e.g., automatic vs. manual), and patch availability.

Key features of the U.S. Cyber Trust Mark program that align with CTA's principles include:

- **Voluntary and market-driven:** Companies choose to participate and earn consumer trust through certification against rigorous, standardized security criteria.

- **Standardized information:** Information accompanying the mark (including QR-linked registry data) will provide consumers with up-to-date details on product support periods, software update practices, and security advisories.

- **Consumer education and clarity:** The label and associated data help consumers easily compare products at the point of purchase without overloading them with legalistic disclosures.

CTA's support for the U.S. Cyber Trust Mark reflects our belief that *harmonized, industry-wide frameworks* that give consumers clear and comparable cybersecurity information are preferable to disparate, state-specific disclosure mandates.

Concerns with S.3090 and H.5114's Mandatory Disclosure Framework and Associated Requirements

While the intent behind S.3090 and H.5114 is understandable, CTA respectfully highlights the following concerns:

1. **Complexity and Consumer Interpretation:** Mandating disclosure of minimum support periods and lost features may be confusing without context about update frequency, severity of issues patched, security priorities, and whether updates require user action. For example, requiring individualized notification in advance of a support period expiring would prove challenging for manufacturers, particularly if the product was never registered or has changed owners.

2. **Regulatory Fragmentation:** A patchwork of state laws with different requirements may complicate product labeling and compliance, increasing costs for manufacturers and, ultimately, for consumers.

3. **Overlap with Federal Standards:** The U.S. Cyber Trust Mark program already envisions consumers being able to access support period and update information via QR codes and a registry, rendering separate state requirements unnecessary and duplicative.

4. **Innovation and Competition:** Rigid support disclosures risk penalizing innovative business models where ongoing service quality and updates evolve over time beyond an initial minimum timeframe.

CTA appreciates the legislature's goal of empowering consumers with meaningful information regarding the lifecycle and security of connected products. However, S.3090 and H.5114 would impose a mandatory disclosure framework that is misaligned with effective transparency models and risks creating consumer confusion and regulatory fragmentation. CTA urges you to consider alternative approaches — particularly supporting the harmonized, voluntary U.S. Cyber Trust Mark program — as a more constructive path to achieving the shared goal of transparency and security for Massachusetts consumers.

For more information, please contact J. David Grossman (dgrossman@cta.tech) or Nabil Mai (nmai@cta.tech).

Respectfully submitted,

J. David Grossman
Vice President, Policy & Regulatory Affairs
Consumer Technology Association

Nabil Mai
Manager, Technology Policy and State Legislative Affairs
Consumer Technology Association