

▶ REPAIR ACCESS DONE RIGHT



MANUFACTURERS SUPPORT REPAIR ACCESS

Manufacturers in America are committed to providing customers with the ability to diagnose, service, and repair their equipment. From agricultural and construction equipment to vehicles, electronics, and defense systems, manufacturers provide technical documentation, diagnostic tools, authorized service networks, and self-repair programs. Voluntary industry frameworks and direct commitments to customer groups have expanded what owners and independent technicians can do on their own. In many cases, customers do not need access to proprietary software for basic repairs. Only a narrow category of controls are protected from modification for regulatory, safety, and security reasons, such as those involving core software or critical safety systems.

What's Really at Stake with “Right-to-Repair”

So-called “right-to-repair” proposals that treat all repair access equally, regardless of safety or regulatory function, often create a right to modify rather than to repair—inviting consequences that undermine the very consumers these proposals seek to protect. Proposals mandating broad access to proprietary software and technical data under the guise of “right-to-repair” introduce several interconnected risks:

- **Intellectual Property:** Forcing disclosure of source code and telematics or other technical data exposes years of R&D investment to both domestic competitors and foreign actors, eroding the innovation incentives that drive manufacturing competitiveness. IP rights provide an essential incentive for manufacturers to make investments in new technologies. Clearly defined and protected IP rights, supported by a stable policy environment, also encourage collaboration and continuous improvement of manufacturing processes and products. Mandates that force disclosure of proprietary data undermine this framework. Importantly, this information is not repair data, is not needed for maintenance, and could be used for modification (in contravention of regulatory or safety standards) rather than legitimate repair.
- **Regulatory Compliance:** Unrestricted software access, including engine control software or stability control systems, could lead to unintentional interference with controls necessary for compliance with applicable federal regulations, exposing manufacturers to liability and consumers to potential safety risks.
- **Cybersecurity:** Diagnostic access tools provide entry to sensitive user and operational data, and a single compromised unit can expose an entire system. Unauthorized and unsafe access thus raises the specter of a malicious actor bypassing cybersecurity protections and exposing the user to unsafe operation or a data breach.
- **Product Safety:** Bypassing authorized service safeguards can impact product integrity and disable safety features, which may expose operators and bystanders to harm. Many products are intentionally designed with specific controls to ensure that safety remains the top priority. If repairs compromise these controls, they can introduce safety risks in the future.

A Better Fix

Manufacturers support a balanced federal approach, developed in partnership with relevant industry experts, that protects IP, meets stringent safety and security standards, and allows manufacturers to stay in compliance with existing regulation. Congress must consider the full range of repair resources manufacturers already provide before taking sweeping action. Where true access gaps or bad actors are discovered, policymakers should pursue targeted solutions instead of generalized mandates that treat all products and industries the same. Each industry operates under a distinct framework, and blanket mandates that ignore product diversity and complexity can dismantle carefully balanced frameworks, deter industry participation, and cause cascading disruption well beyond the original policy's intent.

- **Federal policy must preserve meaningful safeguards against compelled disclosure** of proprietary source code and technical data to competitors or foreign actors.
- **The U.S. IP system must continue to incentivize innovation.** IP rights give legal protection to invention, providing an incentive for manufacturers to make bold investments that drive economic growth and job creation.
- **Repair frameworks must be consistent with maintaining product integrity** and compliance with applicable federal safety, cybersecurity, and environmental standards. Access that permits regulatory violations is not a consumer benefit.
- **Any repair legislation should explicitly state that it addresses specific, identified issues within a defined scope**, and should include clear guardrails to prevent expansion into broader data access, IP protections, or pricing structures, in that industry or any other.
- **Congress should ensure that any federal solution preempts a fifty-state patchwork** of state-level standards.

Beyond “Right-to-Repair”

Manufacturers share the goal of ensuring customers can maintain and repair the products they own. The repair access debate too often buries real challenges involving the protection of intellectual property that sustains American manufacturing competitiveness, the software controls that ensure regulatory compliance, the cybersecurity infrastructure that safeguards users and their data, and the safety systems that protect lives. Broad federal mandates are not the answer, and impractical standards could threaten U.S. innovation and the competitiveness of American manufacturing in the global economy. Manufacturers stand ready to partner with government on thoughtful policy that gets it right.