Developing Danger

Bryant Walker Smith

Whether it results from practice or principle, prospective licensing will likely play a significant role in regulating key applications of emerging technologies. This paper advocates a specific approach to licensing whereby developers of particularly safety-relevant systems define and then demonstrate reasonable risk. This approach could provide flexibility to developers and information to regulators.

Licensing is the most direct way that a government regulates a product or service. Although other forms of regulation are common, policy approaches to new technologies tend to contemplate legal prerequisites to sale, ownership, or use. Early policy proposals for automated vehicles, aerial drones, and lethal robots, for example, have each incorporated special licensing regimes. The case for licensing is strongest for those classes of products or services in which a technological failure would substantially, irreversibly, and noncompensably imperil the safety of nonusers.

The ubiquity of licensing demands a careful approach to defining safety that is flexible enough to accommodate a range of innovators, technologies, and applications. My proposal expands on an process I sketched in a recent book chapter on automated road vehicles: Regulators could "delegate the safety case" by requiring the developer of a particular system to publicly make and defend arguments about how well its system should perform and how well its system actually performs. In short:

1. A manufacturer documents its actual and planned product design, testing, and monitoring.
2. The manufacturer publicly presents this documentation in the form of a safety case.
3. The regulatory agency and interested parties comment on this safety case.
4. The manufacturer publicly addresses these comments.
5. The agency determines that the manufacturer has presented a reasonable safety case.
6. The manufacturer certifies that its product adheres to its safety case.
7. The manufacturer sells that product.

This process draws on several existing models. With respect to motor vehicles, it reflects both the type approval (homologation) typical in the European Union and the self-certification prescribed by US law. It could accommodate the kind of process standards used in functional safety standards like ISO 26262, the kind of alternatives discussion characteristic of environmental impact statements, and the kind of public dialogue foundational to notice-and-comment rulemaking. Unlike current approaches, a safety case could contemplate the entire product lifecycle: A developer might describe not only the steps it had taken to ensure reasonable safety at the time of sale but also the steps it would continue to take as it learned more about performance in the field.

By encouraging companies to disclose information necessary to their safety case, such an approach could help educate regulators and the broader public about the capabilities and limitations of these emerging technologies. What is reasonable will likely evolve, and this approach could afford companies greater flexibility to make nontraditional arguments for the safety of their systems and regulators greater flexibility to adapt to changing capabilities.