BROOKINGS

COMMENTARY

With AI, we need both competition and safety

Tom Wheeler and Blair Levin

July 8, 2024

- → Regulatory oversight of AI must encourage collaboration on AI safety without enabling anticompetitive alliances.
- → Regulation must close the gaps in voluntary commitments with an AI safety model that includes a supervised process to develop standards, a market that rewards firms who exceed standards, and ongoing oversight of compliance activities.
- → This new model of AI safety should also look to the multitude of examples of industry-government alliances to create enforceable standards, such as FINRA and the NERC, as inspiration.

The Federal Trade Commission (FTC) and Department of Justice (DOJ) are currently investigating ↗ whether certain transactions and collaborations between artificial intelligence (AI) companies and others violate antitrust laws. Such investigations are warranted. As a nation, we should be concerned that not only is the development of cutting-edge frontier models controlled by a handful of companies, but also that AI is adjacent to, and dependent on, already concentrated markets, such as cloud platforms and high-powered microchips. We should want AI to grow in a competitive environment.

The country should also want AI models to be safe. Competition and safety should not be mutually exclusive. The FTC and DOJ should make clear that collaboration on AI safety is not only allowed, but also expected. AI should grow up in an environment where the companies cooperate on the delivery of safe products.

Building the AI future around competition and safety should be a no-brainer. The challenge is how to ensure that what could look like technology collaboration on AI safety does not mask what might be an anticompetitive alliance. Meeting that challenge will require a new type of regulatory oversight, although one for which there are historical precedents.

AI safety—an all-hands effort

Since the possibilities of AI came to the attention of the public, it has been clear that the technology combines the potential of enormous rewards with frightening risks—both of which are expanding at exponential speed. "By the time children born today are in kindergarten," AI pioneer Ray Kurzweil recently wrote ↗, "artificial intelligence (AI) will probably have surpassed humans at all cognitive levels, from science to creativity."

It is difficult for all but the most technologically sophisticated to understand where the risks are, let alone how to address them. Policymakers should encourage—and not discourage—those who know the most to set standards for what constitutes harmful AI, how to detect it, and how to protect against it.

That is not something that only one entity can do. AI safety must be an all-hands-on-deck effort. It is a challenge made all the more important—and difficult—by the proliferation of open-source AI models capable of being altered by anyone with the necessary skills.

Such an effort begins with an enforceable agreement for uniformly applicable safety standards. The absence of such standards promises a "race to the bottom" in which some enterprises cut corners to gain profits while forcing the rest of society to bear the costs of unsafe products and services.

AI safety standards

"The Rome Call for AI Ethics" created in 2020—with signatories as diverse as Microsoft, IBM, and the Vatican—has been described as ↗ the "gold standard" in AI practices. Reportedly, the G7 leaders have looked to it as the model ↗ for an AI code

of conduct. Experience has shown, however, that such self-regulation, while commendable, is too often insufficient.

There are two root problems with a voluntary AI safety code. The first is that the code's development and application is only as good as its weakest link. As the Internet Security Alliance's Cybersecurity Social Contract ↗ noted in the context of cybersecurity, an entirely voluntary approach to safety "does not have the expanse needed to address the broad-based issues in cyber space where the weak link in the chain can break the entire security perimeter." So too with AI, we need all the links in the AI ecosystem to live up to a minimum standard that protects all. The second issue with voluntary activities is that, by their very definition, voluntary means the absence of enforcement.

To overcome the problems inherent in a voluntary code, we should seek to create an AI safety model with three basic components. First, it would need to have a supervised process that identifies issues and convenes affected companies and civil society to develop standards. Just as the standard for mobile phones has been agile enough to evolve from 1G through 5G as technology has evolved, so can a standard for AI behavior evolve as the technology evolves.

Second, such a safety model must create a virtuous cycle in which the market rewards enterprises that not only meet baseline standards but exceed them. As the Cybersecurity Contract ↗ noted, the government and private sector should "create market incentives for higher tiers of standards and practices…Such a model would provide incentives for individual companies to invest, purely on a voluntary basis, in enhanced cyber security."

Finally, there should be ongoing oversight of compliance activities. Insight into the code's effectiveness requires the requisite levels of transparency to enable auditing and enforcement. Such efforts can neither be done by government alone, nor through individual enterprise efforts. It requires the collaboration between the multiple stakeholders—including government—to "inspect what you expect" and impose penalties for unacceptable behavior.

A new model for AI safety

AI may be new, but the responsibilities of AI companies to protect their users have been around for literally hundreds of years. As England was breaking free of the bonds of feudalism, a set of common law principles arose to protect the nascent middle class. Imported to the American colonies, one of those principles is the Duty of Care that holds that the provider of a good or service has the obligation to anticipate and mitigate potential harm that may result. Throughout history, the Duty of Care has been applied to a continuing stream of technological innovations. AI is but the latest in that parade.

AI is a departure from the linear world of step-by-step progress to an exponential experience characterized by the velocity of innovation and change. Assuring safety in this new reality must similarly cleave from the practices of the old analog world. This means the government behaving less as a dictator of practices and more of an overseer of AI safety standards.

There are many examples how industry collaboration can be done in the public interest. For example, the American Medical Association ↗ sets standards ↗ for doctors. Failure to follow those standards becomes the basis for legal action and court decisions as to whether they were being followed as the key factor in determining liability. Fordham University Law Professor Chinmayi Sharma ↗ has likened this to a Hippocratic Oath for AI: standards and enforcement against those expectations. ↗

There are multiple examples of industry-government alliances to create enforceable codes or standards. The National Society of Professional Engineers (“NSPE”) Code of Ethics ↗, which has several safety-related principles, such as engineers holding “paramount the safety, health, and welfare of the public” and performing “services only in areas of their competence” is enforceable through disciplinary action, civil and criminal liability, and state oversight. The Financial Industry Regulatory Authority ↗ (FINRA) regulates aspects of the financial industry through an industry-developed code overseen by the Securities and Exchange Commission ↗ (SEC). The North American Energy Reliability Corporation ↗ (NERC) is an industry-led group that has developed policies to prevent blackouts and is overseen by the Federal Energy Regulatory Commission ↗ (FERC).

The establishment of enforceable safety standards—this time for AI—is a well-paved pathway. We should want to already be on that path.

Collaboration for safety and antitrust law

Of course, such a safety collaboration should be structured so as not to affect prices, output, or competitive intensity. This is a doable task. The U.S. government has a history of not challenging competitor collaborations as antitrust law violations when those efforts served the national interest.

As a starting point, the law recognizes that the Sherman Act could lead to overdeterrence that could harm the public interest. As the Supreme Court noted in United States v. United States Gypsum Co ↗., a rule of reason should govern review of collaborative activity designed to produce public benefit. "With certain exceptions for conduct regarded as *per se* illegal because of its unquestionably anticompetitive effects, the behavior proscribed by the Sherman Act is often difficult to distinguish from the gray zone of socially acceptable and economically justifiable business conduct," the Court observed. "The imposition of criminal liability… for engaging in such conduct which only after the fact is determined to violate the statute because of anticompetitive effects… holds out the distinct possibility of overdeterrence; salutary and procompetitive conduct lying close to the borderline of impermissible conduct might be shunned by businessmen who chose to be excessively cautious in the face of uncertainty regarding possible exposure to criminal punishment for even a good-faith error of judgment."

But the nation does not have time, and there is too much at stake for the rules of the road to wait upon a case winding its way through the courts. We need clarity on collaborations involving AI sooner. And we can get that clarity through government providing a blessing for industry collaborations that clearly serve the public interest.

Once again, a good model to study is that used for cybersecurity. It became clear in the early days of the Obama administration that the government had to do more to upgrade defenses against cybersecurity attacks. After congressional efforts stalled, in 2013 former President Obama signed Executive Order 13,636 ↗, which called for creating voluntary public-private partnerships that would collaboratively define standards and best practices for both industry and the government.

Then, in 2014, the FTC and DOJ issued a joint policy statement ↗ that, while not enforceable or binding, gave joint ventures the go-ahead on information sharing related to addressing cyberthreats. As the statement noted, "Some private entities

may be hesitant to share cyber threat information with each other, especially competitors, because they have been counseled that sharing of information among competitors may raise antitrust concerns. The Agencies do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing. While it is true that certain information sharing agreements among competitors can raise competitive concerns, sharing of the cyber threat information mentioned above is highly unlikely to lead to a reduction in competition and, consequently, would not be likely to raise antitrust concerns. To decrease uncertainty regarding the Agencies' analysis of this type of information sharing, the Agencies are issuing this Statement to describe how they analyze cyber threat information sharing."

As the statement further noted, "Cyber threat information typically is very technical in nature and very different from the sharing of competitively sensitive information such as current or future prices and output or business plans." That is true for AI as well.

Getting to yes on both competition and safety for AI

Recently, the New York Times asked ↗ Assistant Attorney General Jonathan Kanter, the head of the Justice Department's antitrust division, whether media outlets should be allowed to collaborate to suppress misinformation. He responded "This is a thorny issue. We stand for the proposition that competition is good for our democracy and the free flow of information. There are no legal prohibitions, under the right instances, under the right circumstances, of efforts to improve safety. But it doesn't need to come at the expense of competition."

He's right. The same logic should apply to AI and safety. Yes, the FTC and DOJ antitrust investigations should continue. But so should efforts to set standards and otherwise address safety, which also encompasses cybersecurity. We need to make sure neither undercuts the two goals that must be achieved, both a competitive and a safe AI market. Whether through an executive order, a joint FTC/DOJ statement, or through some other means, the government should clarify that while it will remain focused on addressing collaborations and acquisitions that reduce competition, it is possible—and encouraged—for AI enterprises to collaborate to protect safety without sharing information about prices or business plans.

AUTHORS

Tom Wheeler Visiting Fellow - Governance Studies, Center for Technology Innovation @tewheels

Blair Levin Nonresident Senior Fellow - Brookings Metro @BlairLevin

Acknowledgements and disclosures

Microsoft and IBM are general, unrestricted donors to the Brookings Institution. The findings, interpretations, and conclusions posted in this piece are solely those of the authors and are not influenced by any donation.