

BROOKINGS

COMMENTARY

The three challenges of AI regulation

Tom Wheeler

Thursday, June 15, 2023

The drum beat of artificial intelligence corporate chieftains calling for government regulation of their activities is mounting:

- Sam Altman, CEO of OpenAI, [told](#) the Senate Judiciary Committee on May 16 there was a need for “a new agency that licenses any effort above a certain scale of capabilities and could take that license away and ensure compliance with safety standards,”
- Brad Smith, President of Microsoft, who had [previously endorsed](#) (<https://www.brookings.edu/blog/techtank/2022/04/15/time-for-a-new-digital-regulatory-authority/>) the idea of a digital regulatory agency, [echoed](#) Altman’s call a few days later: “Companies need to step up... Government needs to move faster,”
- Sundar Pichai, CEO of Google, on May 23 [announced](#) an agreement with the European Union (EU) to develop an “AI Pact” of voluntary behavioral standards prior to the implementation of the EU’s AI Act.

As Senate Judiciary Committee Chairman Richard Durbin (R-IL) [observed](#), it is “historic” to have “people representing large corporations... come before us and plead with us to regulate them.”

Just as it began to look as though AI might be the impetus for the lions lying down with the lambs and cats and dogs becoming friends, however, peace and harmony ran up

against reality. The difficulty of moving from a generic discussion about AI regulation to its actual implementation was illustrated by what happened next:

- Nine days after the Senate testimony that garnered Sen. Durbin's praise, Mr. Altman spoke out against the European Union's pending AI regulation, [warning ↗](#), "We will try to comply, but if we can't comply, we will cease operating [in Europe]."
- Such a threat was "blackmail," Thierry Breton, the EU's Industry Commissioner, [quickly responded ↗](#). "There's no point in attempting blackmail – claiming that by crafting a clear framework, Europe is holding up the rollout of generative AI."
- Yet, Mr. Pichai's chatbot AI product illustrates the problem at hand. Google Bard which is available in 180 countries, is not being offered in the EU or Canada [reportedly ↗](#) because of those countries' privacy rules.

Expanding upon his European comments, Mr. Altman [explained ↗](#), "The details really matter." Those "details" surface three challenges for AI oversight: dealing with the velocity of AI developments, parsing the components of what to regulate, and determining who regulates and how.

CHALLENGE #1: VELOCITY (aka THE RED QUEEN PROBLEM)

In Lewis Carroll's 1871 surrealistic classic [Through the Looking Glass ↗](#), the [Red Queen tells Alice ↗](#): "Now here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run twice as fast as that!" It is an appropriate admonition for oversight in fast-paced AI era.

Artificial intelligence has been quietly evolving behind the scenes for some time. When Google auto-completes a search query, or Amazon recommends a book, AI is at work. In November 2022, however, the release of ChatGPT-3 moved AI out of the shadows, repositioning it from a tool for software engineers, to a tool that is consumer-focused and ordinary people can use themselves without any need for technical expertise. Using ChatGPT, users can have a conversation with an AI bot asking it to design software rather than having to write the code itself. Only four months later, OpenAI, the developers of ChatGPT unveiled GPT-4, the newest iteration of the foundational large

language model (LLM) that powers ChatGPT, which OpenAI claimed "exhibits human-level performance" on a variety of tasks. ChatGPT became the [fastest growing](#) website in history, garnering over 100 million users in two months.

Suddenly, an AI race was on. Microsoft, after [investing \\$13 billion](#) in OpenAI, incorporated ChatGPT into its products, including a revamped, AI-powered Bing. Google, which made headlines in 2016 when its DeepMind AI model [beat a human champion](#) at the Chinese game of Go, [immediately responded](#) with Bard, its own AI chat bot. Meta CEO Mark Zuckerberg [told](#) employees, "Our single largest investment is in advancing AI and building it into every one of our products." Multiple smaller companies, aided by the availability of [open-source code](#), have joined the AI chase as well.

As Microsoft CEO Satya Nadella [observed](#) at the time of his company's Bing announcement, "a race starts today in terms of what you can expect." The challenge becomes how to protect the public interest in a race that promises to be the fastest ever run yet is happening without a referee.

To keep the corporate AI race from becoming reckless requires the establishment and development of rules and the enforcement of legal guardrails. Dealing with the velocity of AI-driven change, however, can outstrip the federal government's existing expertise and authority. The regulatory statutes and structures available to the government today were built on industrial era assumptions that have already been outpaced by the first decades of the digital platform era. Existing rules are insufficiently agile to deal with the velocity of AI development.

Former Google Executive Chairman and current AI evangelist Eric Schmidt has [warned](#), "There's no one in government who can get it [AI oversight] right." While Mr. Schmidt recognizes the need for behavioral expectations, his [solution](#) is, "I would much rather have the current companies define reasonable boundaries." Such a self-regulatory approach is the same kind of "leave us alone" solution that has been championed by digital platform companies for the last 20 years. The results of this strategy speak for themselves in well-known current online harms, such as the unprecedented invasion of personal privacy, market concentration, user manipulation, and the dissemination of hate, lies, and misinformation. AI demands something better

than corporate self-regulation when we know the chase for profits is likely to outstrip the implementation of meaningful guardrails.

Allowing the companies to become pseudo-governments and make their own rules to govern AI would be to repeat the mistake made when they were allowed to make their own rules for online platforms. As Senator Richard Blumenthal (D-CT) has [explained](#) ⁷, "Congress failed to meet the moment on social media. Now we have the obligation to do it on AI before the threats and the risks become real."

Dealing with the velocity challenge is a matter of focus and agility. Focus that places AI at the front and center of an agency's remit rather than bolting it on to existing authority. Agility that frees the agency from the old ways of regulatory micromanagement to keep pace with technology.

In the industrial era, the Congress produced oversight that followed the precepts of the industrial management guru Frederick W. Taylor. "Taylorism," as it was known, [preached](#) ⁸, "It is only through the *enforced* standardization of methods" that satisfactory outcomes can be achieved [emphasis in original]. It was a management technique that worked largely because of the slower pace of industrial innovation and adoption. The same slower pace also allowed such command and control to be implemented in government through regulatory dictates.

For many years, tech companies have rejected such management techniques. To be responsive to the rapid pace of change in technology and the marketplace, these companies practice agile management that embraces transparency, collaboration, and responsiveness rather than hierarchical dictates. Agile regulation should be constructed in a similarly responsive manner. To accomplish this, the Congress needs to be as innovative in its thinking as the digital companies themselves.

The industrial revolution was built on replacing and/or augmenting the physical power of humans. Artificial intelligence is about replacing and/or augmenting humans' cognitive power. To confuse the regulatory needs of the former with those of the latter would be to fail to keep pace with the digital era's velocity of change to the detriment of both consumers and companies.

CHALLENGE #2 – WHAT TO REGULATE?

Because AI is a multi-faceted capability, “one-size-fits all” regulation will over-regulate in some instances and under-regulate in others. The use of AI in a video game, for instance, has a different effect—and should be treated differently—from AI that could threaten the security of critical infrastructure or endanger human beings. AI regulation, thus, must be risk-based and targeted.

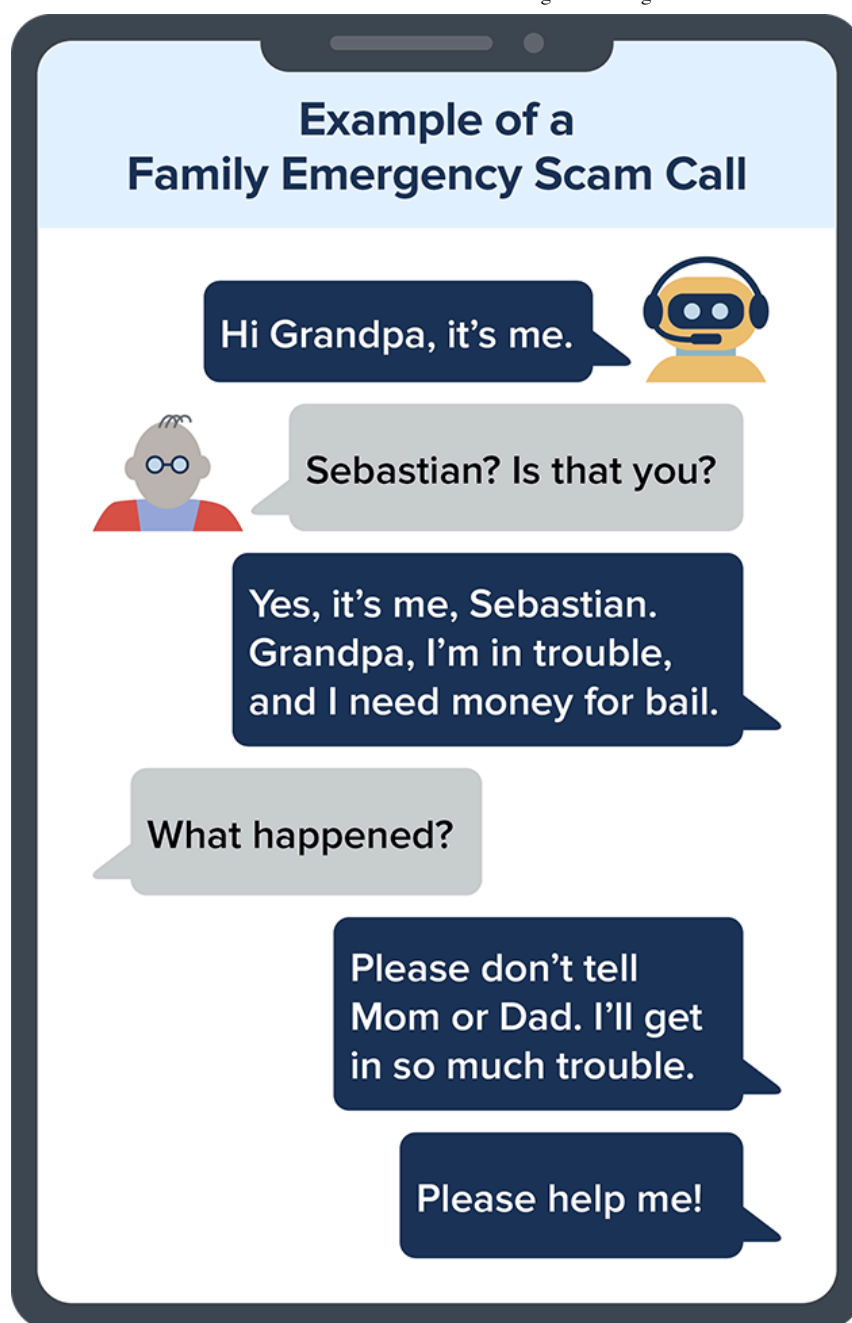
Considering AI regulation can be facilitated by parsing such analysis into three threshold areas.

Dealing With Old-Fashioned Abuses

Artificial intelligence can, with or without malicious intent, bring automated scope and scale to illegal activities. Artificial intelligence may be a new-fangled technology, but its application expands old-fashioned abuses. In this area, it is possible to look to the old regulatory tools to address threats.

Thanks to AI, [consumer scams](#) and criminal enterprises, whether via email or telephone, can reach an unprecedented level of productivity and sophistication. Formerly, a scam was a piecemeal process of combining components such as an email address or phone number with a convincing message; the result was then distributed, and the results harvested. With AI the entire process can be automated, from the selection of the target to the creation and delivery of the message.

The Federal Trade Commission’s (FTC) [advisory](#) on AI-enabled voice scams illustrates the power of the technology. The scammer first obtains a short audio clip—as [little as three seconds](#)—from an online post and feeds it into an AI model to produce a realistic sounding message from a friend or loved one. The AI voice model is even capable of engaging in a “conversation” with the target as this illustration from the [FTC advisory](#) demonstrates:



Scams or manipulative applications are not the only illegal uses of AI, however. Discrimination is another old problem that AI can exacerbate. The Equal Employment Opportunity Commission (EEOC) has [warned](#) that the use of AI models “in hiring workers, monitoring worker performance, [and] determining pay or promotions” can produce discriminatory results in violation of federal law. The Department of Justice has [similarly warned](#) about discrimination resulting from the application of AI to screen and select among rental applications.

The low-hanging fruit of the AI era is dealing with its impact on such traditional abuses. The Biden administration [brought together](#) four of the nation's consumer-

facing regulatory agencies—the FTC, EEOC, Department of Justice (DOJ), and Consumer Financial Protection Board (CFPB)—to announce a focused initiative to apply existing statutes to deal with AI-enhancements of traditional abuses. This effects-based approach can be the model for the oversight of AI writ large: focus less on the technology *per se* and on what it delivers. In this case, those effects are already covered by existing statutory authority. All that is required is regulatory initiative.

In a succinct statement worthy of being posted in the halls of every regulatory agency, FTC Chair Lina Khan [explained](#), “There is no AI exemption to the laws on the books.”

Dealing With Ongoing Digital Abuses

The next effect-focused AI initiative revolves around how the ongoing digital abuses for which there has yet to be effective oversight can be amplified by AI. Harms such as the violation of personal privacy, expansion of non-competitive markets, manipulation of individuals, and dissemination of hate, lies and misinformation—all currently rampant online—can be exacerbated by the application of AI. Dealing with how AI amplifies these problems begins with dealing with the baseline consequences of the digital activities themselves—activities that result from decisions made by the same companies that are in the forefront of AI.

For decades, policymakers have failed to address a threshold issue of the digital age: how the dominant digital companies harvest personal information, make it their corporate asset to be hoarded to maintain market control, and use that market dominance to control the information that consumers receive. There is nothing in the operation of AI models that will change those abuses, yet there is everything in the new reality that expands the power of the dominant AI companies to accelerate those abuses.

The “gateway drug” for digital exploitation is the collection of individuals’ personal information. The history of online platforms has been one of continued expansion of the amount of personal data collected to increase the granularity of the targeting the companies sell to advertisers. The present and future of AI is a similar continued expansion of the collection and use of data.

The large language models (LLMs) that drive generative AI are, by definition, “large” and growing. As of the spring of 2023, GPT-4 is [reported](#) to have one trillion parameters, six times more than GPT-3 (a [parameter](#) measures the input size of the training data with increases in parameters increasing accuracy). This included siphoning vast amounts of what users of online services have written, videoed, or uttered. The privacy-invading practices that platform companies such as Alphabet/Google, Meta/Facebook, Microsoft, and others have been allowed to pursue have created today’s well-recognized problems. Now, as those same companies venture into AI, these unregulated practices form the basis for further privacy intrusions, including AI-enabled video and audio surveillance of each of us.

The potential to use the control of data to control markets is also expanded in the AI environment. That AI models become more accurate with the expansion of the data on which they are trained means that those with the biggest data hoards have an advantage. It is not an accident that the companies in the lead of AI services are also the companies that have profited greatly from the collection and hoarding of their users’ information. Added to their competitive advantage is the vast computing capability each of the companies had to build to deliver their original service—computing power that now becomes the basis for computing-heavy AI and yet another barrier to entry.

Artificial intelligence can also increase the flood of misinformation, disinformation, and malinformation that has characterized the digital era. Thus far, platform companies, despite becoming major sources of news and information, have failed to embrace meaningful journalistic standards. “We’re different from a media company,” Sheryl Sandberg [explained](#) when she was Facebook’s chief operating officer, “At our heart we’re a tech company, we hire engineers. We don’t hire reporters.” The introduction of AI’s ability to create false images, audio, and text for companies that already consider themselves to be above any editorial or curatorial responsibility can only add to the information pollution that undermines truth and facts.

The challenges that have thus far not been confronted in the digital age become even more important to resolve as those same issues grow in the world of AI. It is impossible to deal with how AI exponentially expands assaults on privacy, competition, manipulation, and misinformation without first dealing with the consequences of the baseline activities of the dominant digital platforms. This becomes even more

important as the companies that created the problems in the first place expand to dominate AI as well.

Dealing With the AI Itself

The previous two subsections might be described as the “knowns” of AI’s impact—harms we have seen previously that AI can exacerbate. But AI also brings with it a tidal wave of “unknowns” ranging from highly beneficial to harmful.

While some fear the [dystopian effects](#) of AI, such a debate should not be permitted to derail or distract decisions dealing with the effects of what is being built today and in the near future. It is these decisions, made by humans, about the construction and operation of AI models that determine both the near- and long-term consequences of those models.

The next section—Challenge #3—proposes a new regulatory approach that is agile enough to respond to whatever harmful unknowns AI may throw at us. Before discussing the implementation of regulatory oversight, however, it is worthwhile to establish the four corners of regulatory involvement: a Duty of Care, transparency, safety, and responsibility.

Any oversight begins with the responsibility of the companies to exercise their common law [Duty of Care](#). The Duty of Care is essentially a “do no harm” expectation; this means the provider of a good or service has the responsibility to identify and mitigate any potential ill effects. Failure to exercise such duty can trigger legal action including regulation.

Transparency is the tool that provides ongoing insight into the identification and mitigation of the evolutionary risks of AI. Such transparency begins with continuous research into how the models work. After having built the algorithmic “black box,” even the providers of AI often cannot know exactly what their creation is doing. Access to the models for academic, government, and civil society representatives will help keep track of new threats and help pierce the “black box” veil.

Transparency is also important for individual users of AI. Disclosure that a consumer is interacting with an AI model and the source that model's training data would help level the playing field between the algorithm and the individual. Similarly, labeling the end product—especially audio and video—as being produced by AI would help resolve consumer confusion. Transparency can also help mitigate algorithmic bias. New York City, for instance, is [implementing a new law ↗](#) requiring employers to notify job applicants of the use of AI to review applications and to submit such systems to third-party audits.

Safety is an output of transparency (i.e., identification of problems) and its own principle. The dystopian fears, for instance, should encourage us to assure that AI remains under the supervised control of humans. Such human agency, however, is not an overall safety solution since competition, malfeasance, or simple error can also lead to the introduction of new threats.

A baseline for safe AI practices has been laid out in a [Framework for AI Risk Management ↗](#) by the National Institute of Standards and Technology ([NIST ↗](#)). The voluntary NIST Framework identifies “approaches that increase the trustworthiness of AI systems... [and] help foster the responsible design, development, deployment and use of AI systems.” It should be table stakes in AI oversight.

The third principle—responsibility—is at the heart of the White House [Blueprint for an AI Bill of Rights ↗](#). Each of its five Rights is accompanied by a description of how responsible actors can adopt the Rights into their activities.

The Duty of Care establishes an enforceable expectation; transparency, safety, and responsibility are only ideals until they are established as expectations through regulation.

CHALLENGE #3 – WHO REGULATES AND HOW

Thus far in the digital age in the United States, it is the innovators who have made the rules. This is in large part because the American government has failed to do so. It is entirely natural that such industry-developed rules would benefit their maker. With

general agreement that there need to be AI policies, the question becomes who will make those policies?

Regulatory First Mover Advantage

When OpenAI's ChatGPT leapt out in front of other AI models to become an online and media sensation it established a first mover advantage in the marketplace. Google had been working on AI since before its 2014 acquisition of Deep Mind, a British AI research laboratory, yet the announcement sent it reeling. "Scary AI ChatGPT could eliminate Google within two years," one [headline blared](#). A former Google executive [tweeted](#), "Google may be only a year or two away from total disruption. AI will eliminate the Search Engine Results Page, which is where they make most of their money." Having lost the first mover advantage, Google became a fast follower with the launch of its own AI chat bot, Bard.

In a comparable manner, there is a first mover advantage to regulation. Thanks in large part to the interconnected nature of 21st century networks, the government that establishes the first set of rules defines the discussion from that point forward for all nations. The classic example of this is the European Union's 2018 General Data Protection Regulation ([GDPR](#)), which has become the standard for privacy policy around the world.

Once again it appears as though the EU, which has been in the lead in establishing digital platform policy with its [Digital Markets Act](#) and [Digital Services Act](#), is also in the lead on establishing AI policy. On June 14 the European Parliament overwhelmingly [approved](#) the [AI Act](#). Following its adoption, the regulatory machinery of the European Commission will begin developing enforceable policies.

Whether the United States will be a Google-like fast follower when it comes to AI oversight very much remains to be seen. The clock, however, is ticking; the success of a second mover very much depends on how much time has passed.

Who Regulates

OpenAI's Sam Altman [endorsed](#) the idea of a federal agency dedicated to AI oversight in his May 16 testimony. Microsoft's Brad Smith and Meta's Mark Zuckerberg have previously [endorsed](#) (<https://www.brookings.edu/blog/techtank/2022/04/15/time-for-a-new-digital-regulatory-authority/>) the concept of a federal digital regulator.

Two days after the May 16 hearing, Senators Michael Bennet (D-CO) and Peter Welch (D-VT) [introduced legislation](#) to create a Digital Platform Commission (DPC). The bill not only creates a new agency with authority to oversee the challenges imposed by digital technology, including AI, but also embraced an agile risk-based approach to developing that regulation. [Reportedly,](#) Senators Lindsey Graham (R-SC) and Elizabeth Warren (D-MA) are also working on a proposal for a digital agency.

The challenge facing the U.S. Congress is to be as expansive and creative in their thinking about a new agency and its operations as the innovators of the digital revolution have been in the developing the creations necessitating such a body.

How to Regulate: Licensing

In his Senate testimony, Sam Altman proposed the new agency should be responsible for licensing ["any effort above a certain scale of capabilities"](#) with the ability to "take away that license and ensure compliance with safety standards." Brad Smith [proposed](#) a similar licensing structure.

The federal government has for a long time engaged in the licensing of certain activities. The [Federal Communications Commission](#) (FCC) licenses the airwave spectrum for radio and television broadcasting, satellite communications, and mobile devices. The [Nuclear Regulatory Commission](#) (NRC) licenses nuclear materials and reactor installations. Drilling rights are licensed, commercial fishing is licensed, aircraft are licensed; the [list](#) of federal licensing activities is expansive. Accompanying such licenses are rules for their operation.

As a tool for regulatory oversight, however, licenses have their drawbacks. Principal among them, licenses tend to reinforce the strategic position of those who receive the license. It should not be surprising, therefore, that the companies that are already

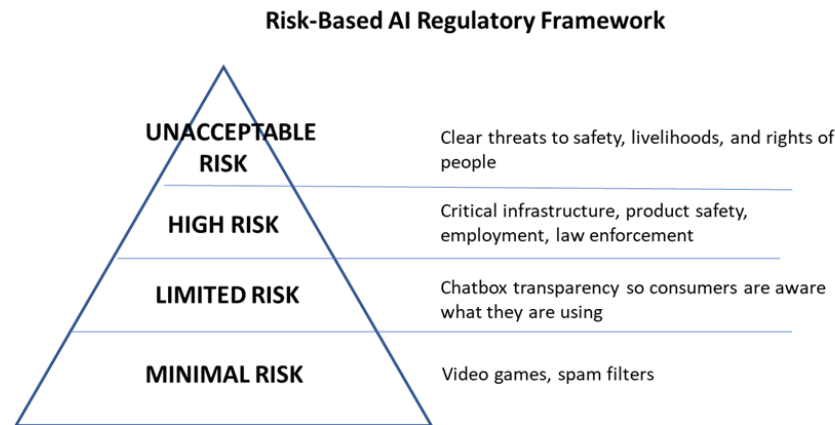
dominant in AI would embrace such a concept. Getting a federal license can be akin to building a moat around your castle and pulling up the drawbridge. Forcing a potential competitor to receive a license redefines the forum for competition from the commercial marketplace to the licensing authority. As such, a license reinforces dominance by creating a barrier to entry and adding costs to anyone seeking to assault that position. Creating a regulatory moat has the added advantage of occurring in a forum where the political influence of the big companies can be deployed.

While a new federal agency is important, as will be discussed subsequently, how an agency operates will be as important as the fact that it exists. There may be a role for some form of licensing, but its competitive pitfalls mean that it is not a one-stop solution

How to Regulate: Risk-Based Agility

The digital era requires not only a focused expert agency, but also an agency that eschews industrial style operations to embrace new forms of oversight—including the use of AI in that oversight. Such oversight must focus on mitigating the *effects* of the technology rather than micromanaging the technology itself. This means evolving the regulatory ethos from micromanagement to risk-based regulation with agile implementation.

This is the approach the EU has taken in its development of AI oversight. The first component of such oversight begins with the recognition that because the effects of digital technology are not uniform, oversight of those effects is not a “one size fits all” solution. To accomplish this, the EU has a multi-layered, effects-based analysis for AI that recognizes the many and varied use cases for AI are accompanied by differences in application, adoption, and inherent risk.



Based on an assessment of the level of risk, different behavioral expectations will be enforced. Whatever oversight may be necessary for AI-assisted spam filters, for instance, will be quite different from AI that threatens an individual's personal safety.

How to Regulate: A Plan

Basing oversight on risk analysis triggers the question of how to design such oversight in a manner that focuses on mitigating the identified risk but avoids deterring investment and innovation. To accomplish this, Congress, which looked to industrial management techniques for regulatory agencies in the industrial era, should now look to emulate the practices of the digital companies.

At the heart of digital management systems are standards for technology. These standards are designed by the affected companies to anticipate and mitigate unintended operational difficulties such as components not being able to work together. The process is also a mechanism that assures the standard evolves as technology changes. Such standards are everywhere, but one obvious example is the mobile phone standard. The evolution from the first-generation technology (1G), to 2G, 3G, 4G, and now 5G (with 6G standardization underway) demonstrates how standards keep pace with new technology and new marketplace opportunities.

The problem is these standards apply to the *technical* issues the companies confront. What they do not address are the *behavioral* issues resulting from the application of the technology.

Agile oversight would adopt a standards-like process to develop behavioral standards—expressed as codes of conduct—that would be enforceable by the new agency. Think of such a transparent, responsive, and agile approach in terms of the following steps:

- The digital agency identifies the issue(s) to be addressed and establishes a timeline for the code-setting process.
- The agency then presents its own detailed report on the problematic behavior(s), along with remedies to be considered. This analysis would be the “prosecutor’s brief” that identifies and quantifies the issue(s) to be addressed.
- The proposed response to the agency’s mandate would be developed by a multistakeholder group of experts representing a cross-section of interested and/or affected parties from industry, civil society, and government (including the agency itself).
- On or before the designated deadline the group would present its code recommendation to the agency for line-item approval and/or edits.
- Once approved, the new code becomes an agency-enforceable policy.
- Ongoing analysis by an industry-academic-civil society advisory group would track the policy outcomes and identify newly emerging issues to begin the whole process again.

Such a delegation of enforceable code development with subsequent agency approval is not a new model in government. The Financial Industry Regulatory Authority (FINRA) regulates aspects of the financial markets through an industry developed code overseen by the Securities and Exchange Commission (SEC). The North American Energy Reliability Corporation (NERC) was created by Congress after power blackouts as an industry-led group to develop policies to prevent blackouts. It is overseen by the Federal Energy Regulatory Commission (FERC).

PULLING IT ALL TOGETHER

All modern regulations walk a tightrope between protecting the public interest and promoting innovation and investment. In the AI era, traversing the regulatory tightrope

means accepting that different AI applications pose different risks and identifying a plan that pairs the regulation with the risk while avoiding innovation-choking regulatory micromanagement.

[Press reports](#) suggest divisions in the Biden administration over AI regulation. One group supports efforts like those of the EU; another group is concerned that could throttle innovation. The choice does not have to be a binary, however.


An American AI oversight plan can protect the public interest while also promoting innovation. The key to such an effort is to walk away from regulation based on industrial management assumptions to embrace agile digital management techniques. The digital companies long ago made that transition; it is time for the American government to make a similar pivot.

Lincoln's [admonition](#) from over one-hundred and sixty years ago rings true in today's AI era: "As our case is new, so must we think anew, and act anew."

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

AUTHOR



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

The Brookings Institution is committed to quality, independence, and impact.

We are supported by a [diverse array of funders \(/about-us/annual-report/\)](#). In line with our [values and policies \(/about-us/research-independence-and-integrity-policies/\)](#), each Brookings publication represents the sole views of its author(s).

Copyright 2025 The Brookings Institution