Effective Accountability Along the AI Value Chain: Right-Sizing AI Responsibilities for the Role

Artificial intelligence (AI) fuels digital transformation in every sector of the economy. Manufacturers use AI to design safe and sustainable products; small businesses rely on AI-based translation tools to reach global customers; health researchers use AI to improve patient care and drive new medical breakthroughs; and companies in all industries can use AI systems to improve the accessibility of their products for people with disabilities. In these areas and countless more, AI creates new opportunities to solve complex challenges.

Successful AI adoption requires trust and confidence in these innovative technologies. As policymakers create frameworks for increasing trustworthiness and accountability, they should recognize a key principle: responsibilities should fit the role of the company.

Creating role-based responsibilities for different AI actors is important for several distinct but related reasons. First, it assigns responsibilities to companies that they can implement based on their access to relevant information and position in the AI supply chain, preventing unworkable obligations for things outside of their control. Second, it ensures that consumers and business customers are better protected because the companies that are best positioned to identify and address risks are the entities designated to take relevant steps to protect them. Third, it creates a policy framework that is workable in practice.

Key Actors in the AI Ecosystem

The AI supply chain is complex and evolving and includes a variety of companies, including AI developers, integrators, and deployers. In many scenarios, a developer may create an AI system, and a deployer will use that system in the real world.

DEVELOPERS design, code, or produce AI systems

EXAMPLE

A company that designs, codes, or produces an AI system, such as a software company that develops an AI system for speech recognition, is a developer.

DEPLOYERS use AI systems

EXAMPLE

A company that uses an AI system, such as a bank that uses an AI system either developed internally or by a third party to make loan determinations, is a deployer.

An organization can act as both a DEVELOPER and a DEPLOYER

EXAMPLE

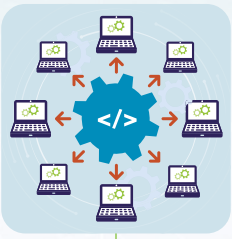
A cybersecurity company develops AI software that monitors network traffic and customer transactions and then uses it on its own systems. The company is both a developer and a deployer.

In other contexts, one company may develop an AI model, a second company may integrate that AI model into an application or platform (AI system), and a third company may use that AI system to perform a business function, such as summarizing documents on a content management platform that is generating insights into a company's financial transaction data.

DEVELOPERS

A model developer can create a generative AI model that summarizes text or generates images.

INTEGRATORS



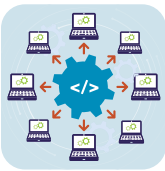
An integrator may incorporate that generative AI model into its own software application, enabling features such as transcribing meeting notes and summaries on a video communications platform or analyzing business contracts using document management software.

DEPLOYERS

A deployer may use the integrator's software application to assist with common business tasks, such as leveraging it to query key business documents to find answers to specific questions or generate summaries.

Developers

Developers include companies that create AI systems, including the underlying models, and sell or license the entire AI system to customers. Examples include human resource management or workflow collaboration software for businesses. In the general-purpose AI context, model developers create AI models, which can be used in a wide variety of different applications. For example, a company may develop a foundation model that can be adapted for many different use cases. The same foundation model can be used to power a range of AI systems including search engines, chatbots, spam detection software, tools that summarize long text documents, and a variety of other applications. Developers will have information about how their AI models or systems have been developed, but they generally lack information about how other companies deploy their AI tools.



Integrators

Other companies—"integrators"—may integrate an AI model into a particular application, for use by other companies. Some integrators may simply connect the AI model to a specific AI system or application, while other integrators may fine-tune or modify the AI model before including it in an AI system or application. For example, a company may act as an integrator when it develops an AI application that incorporates one or more third-party AI models. Integrators will generally have information about any changes they made to the AI model, but they usually do not have direct insight into the model's initial development or the later use of the AI system by deployers.

Deployers

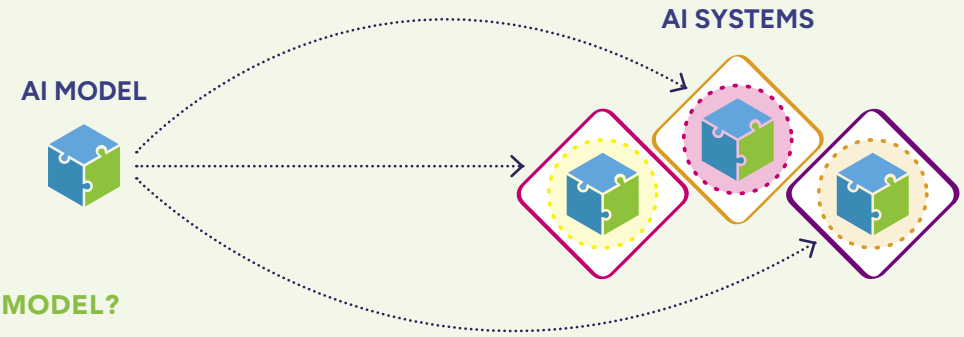
Companies that use an AI tool for a specific purpose are often called deployers. These companies decide when and how to use a particular AI technology, so they will have insight into the facts of a particular use case. But deployers often obtain AI tools from other companies, so they typically lack direct insight into the initial training of the AI tool. Deployers are often the companies that have direct relationships with consumers.

Effective policy and accountability frameworks must recognize these different types of companies to avoid one-size-fits-all requirements and ensure responsibilities fit the role. This is important because the various companies along the AI supply chain will have access to different information and be in different positions to take the necessary actions to identify and address relevant risks to protect consumers and business customers.

For example, a developer of a foundation model would be able to describe issues related to the design and training of its model, but it generally would not have insight into how an integrator customizes the model for a specific application or how a deployer subsequently uses that AI system in the real world. Instead, the deployer using the AI system is generally best positioned to understand how the AI system is being used, whether that use aligns with its intended use, how to incorporate human oversight in its operation, review the outputs generated from the AI system, receive any complaints from end users, and assess real-world factors that may affect the system's performance.

Like other contexts, any legislation or policy framework that creates obligations for companies that design and use AI systems should reflect these different roles and assign responsibilities accordingly.

WHAT IS THE DIFFERENCE BETWEEN AN AI MODEL AND AN AI SYSTEM?



WHAT IS AN AI MODEL?

An **AI model** is a piece of software trained on large amounts of data to, for example, recognize patterns, make predictions, or generate content.

Think of it like:

- A **trained expert** who has learned from many examples, or who continues to learn from experience, or
- A **brain** that can process language, images, or numbers.

Examples of what models can do:

- Predict the next word in a sentence
- Recognize objects in an image
- Generate text, images, or code

On their own, models are usually **not user-friendly.** They don't have user interfaces, buttons, screens, or workflows.

WHAT IS AN AI SYSTEM?

An **AI system** is a complete tool or product that uses one or more AI models to perform a task or solve a problem.

Think of it like:

- A **car** that includes an engine (the model), plus steering wheel, seats, and controls.

AI applications may include a chat interface, buttons, menus, or voice input, or rules, safeguards, and integrations (e.g., with email, calendars, databases).

Examples:

- A chatbot that answers customer questions
- A photo app that enhances images
- A writing assistant that helps draft emails

PRECEDENT FOR ROLE-BASED POLICY APPROACHES

Establishing role-based obligations is considered best practice in privacy and security legislation around the world. For example, privacy laws in the United States and around the world distinguish between the differing roles of controllers that determine how and why data is processed, and processors that handle data on behalf of a controller and according to its instructions. Similarly, in various jurisdictions, cybersecurity legislation generally differentiates between companies and their service providers.

Just as privacy and security laws distinguish between different types of companies that handle consumers' personal data, distinguishing among the different companies along the AI supply chain ensures that legal frameworks appropriately assign obligations to a company based on its role in the AI ecosystem, enabling them to meaningfully fulfill those obligations and better protect consumers.