AI Developers and Deployers: An Important Distinction

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.

The success of AI products and services will be based on public trust and confidence in these technologies. To earn that trust, organizations that develop and use AI must account for the unique opportunities and risks the technology poses. Policymakers can also enhance public confidence and trust in AI by establishing a legal and regulatory environment that supports responsible innovation. In doing so, they should (1) focus on high-risk uses of AI and (2) recognize the different roles and responsibilities of developers and deployers of AI systems.

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 platforms. The company is both a developer and a deployer.

By recognizing the different roles of developers and deployers, policymakers can tailor obligations to an organization's role in the AI marketplace. For example, a deployer using an AI system does not generally have control over design decisions made by another company that developed the AI system. Likewise, a developer of an AI system generally does not have control over subsequent uses of the AI system by another company deploying the system.

EXAMPLE

A developer designs an AI system that helps a bank sort loan applications. The developer of that AI system will have information about data used to train the AI system to recognize common responses and how certain features operate. However, the developer has no interaction with consumers applying for a loan, and it does not select which loan applications are approved. Instead, the bank interacts with the consumer and decides which applications to approve or deny. As the deployer, the bank is the entity that will use the results of the sorting process, will be best positioned to assess the fairness of its lending practices, and is capable of implementing safeguards to mitigate potential risks.

WHY IS THE DISTINCTION BETWEEN DEVELOPERS AND DEPLOYERS IMPORTANT?

Just as privacy and security laws distinguish between different types of companies that handle consumers' personal data, distinguishing between developers and deployers ensures that legal frameworks accurately assign obligations to a company based on its role in the AI ecosystem. As a result, companies are better able to fulfill those obligations and better protect consumers. For example, a developer would be able to describe the features of data used to train an AI system, but it generally would not have insight into how the AI system is used after another company has purchased and implemented the AI system. Instead, the deployer using the system is generally best positioned to understand how the AI system is being used, whether that use aligns with its intended use, whether and how to incorporate human oversight, the outputs from the AI system, any complaints received, and real-world factors affecting the system's performance.

Any legislation that creates obligations for companies that design and use AI systems should reflect these different roles and assign obligations accordingly. This ensures that the appropriate company within the various real-world AI supply chains can identify and mitigate risks. For the same reasons, this kind of distinction is considered best practice in privacy and security legislation around the world. For example, privacy laws in the United States, Europe, Asia, and Latin America 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.

What Obligations Should Developers and Deployers of High-Risk AI Systems Have?

BSA supports requiring companies to conduct impact assessments for high-risk uses of AI. These assessments are important accountability tools that help businesses identify, document, and mitigate AI risks. Notably, they are also helpful tools in detecting and mitigating potential bias that could result in unlawful discrimination.

Any legislation creating impact assessments should apply to high-risk uses and clearly distinguish requirements for developers and deployers.

DEVELOPERS
design, code, or produce AI systems

Developers conducting design evaluations of high-risk AI systems should document information including, as appropriate:

- The intended purpose of the AI system;
- Known limitations of the AI system;
- Known, likely, and specific high risks that could occur and steps taken to mitigate those risks;
- An overview of the data used to train the AI system; and
- A summary of how the AI system was evaluated prior to sale.

DEPLOYERS
use AI systems

Deployers conducting impact assessments of high-risk AI systems should document information including, as appropriate:

- The purpose for which the deployer intends to use the AI system;
- Transparency measures, including notices to impacted individuals about the AI system's use;
- A summary of how the AI system is evaluated, if applicable;
- Known, likely, and specific high risks that could occur and steps taken to mitigate those risks; and
- Post-deployment monitoring and user safeguards, if applicable.