Impact Assessments: A Key Part of AI Accountability

As companies develop and deploy AI systems, they should take steps to ensure the technology is used responsibly. Organizations should implement robust processes for performing impact assessments on high-risk AI systems to effectively manage risks. Impact assessments are a key accountability tool used in a range of other fields, from environmental protection to data protection.

BSA supports legislative requirements for companies that develop and deploy high-risk AI systems to conduct impact assessments.

Why Conduct an Impact Assessment?

Impact assessments have three purposes:

IDENTIFYING
potential risks that an AI system may pose.

QUANTIFYING
the degree of potential harms the system could generate.

DOCUMENTING
steps taken to mitigate those risks.

Identifying and Evaluating Risks of AI Systems

AI systems are used in a wide range of scenarios, from detecting and lowering background noise on a video call to optimizing manufacturing production. For truly low-risk systems—like an AI system used to predict the types of fonts used in a document—an impact assessment is not necessary. But for high-risk systems, companies should perform impact assessments to assess and mitigate risks. Importantly, there is no "one-size-fits-all" approach to evaluating and mitigating risks of AI; impact assessments should be tailored to address the nature of the system at issue and the type of harms it may pose.

Who Conducts Impact Assessments?

Organizations must conduct impact assessments that reflect the risks of their specific AI system and their role in developing or deploying that system. Both developers and deployers should conduct impact assessments—but those assessments must reflect their different roles. Because a developer is the entity that designs, codes, or produces an AI system, and a deployer is the entity that uses an AI system, these two organizations will have different roles in identifying and mitigating the potential risks of an AI system. Moreover, the two types of organizations will have access to different types of information—and will be positioned to take different steps to mitigate potential risks.

What Should Be Included in an Impact Assessment?

Developers of high-risk AI systems and deployers of high-risk AI systems should conduct assessments that focus on the risks they are positioned to identify and mitigate.

DEVELOPERS should consider:

- 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 should consider:

- 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.

Why It Matters for Policy

BSA supports legislation that recognizes the benefits of artificial intelligence while establishing workable guardrails focused on high-risk AI systems. Both developers of high-risk AI systems and deployers of high-risk AI systems should be required to conduct impact assessments, as an important component of a broader risk management program, and part of an overall policy solution that establishes a framework for the responsible development and use of AI.

HOW IMPACT ASSESSMENTS ARE USED IN PRIVACY AND DATA PROTECTION

Impact assessments are already used in a range of other fields, including privacy and data protection. A broad range of global and state privacy laws already require organizations to conduct impact assessments, and those processes can be leveraged to conduct AI-focused impact assessments. Impact assessments are an important and proven accountability tool to identify and mitigate risks, which can promote the responsible development and use of high-risk AI systems.

United States: At least 10 state privacy laws require data controllers to conduct impact assessments for specific types of data processing, such as processing involving sensitive personal data, targeted advertising, sale of personal data, and certain types of profiling.

European Union: Under the General Data Protection Regulation, controllers must conduct data protection impact assessments for certain activities, including those "likely to result in a high risk to the rights and freedoms of natural persons."

Worldwide: Privacy and data protection laws worldwide have also focused on the importance of impact assessments as a tool for improving accountability, ranging from requirements in Brazil, Korea, Singapore, and the UK, to guidance in Canada, Australia, and beyond.