Science, Technology Assessment, and Analytics

SCIENCE & TECH SPOTLIGHT:

PRIVACY ENHANCING TECHNOLOGIES

GAO-26-109063, May 2026

WHY THIS MATTERS

Companies and organizations are collecting more personal data from Americans than before to improve technologies such as AI. But using and sharing large amounts of data carries security and privacy risks, like breaches of personal information. According to the FBI, Americans reported more than $1.4 billion lost due to personal data breaches in 2024. Privacy enhancing technologies, or PETs, can help reduce risks associated with collecting, using, and sharing data.

KEY TAKEAWAYS

- Privacy enhancing technologies are expanding to new datasets and evolving to counteract malicious actors.
- They also could enable more secure collaboration and research on sensitive information, such as medical records or proprietary company data.
- Lack of federal guidance, high resource costs, and workforce constraints affect implementation of these technologies and may hinder widespread use.

THE TECHNOLOGY

What is it? Privacy enhancing technologies modify, hide, or process data in ways that make it difficult to access sensitive information. Newer technologies that focus on minimizing shared data and limiting uses are improving the ways data can be used while protecting privacy. They can facilitate global collaboration on research and fraud detection while also reducing privacy risks associated with using and sharing data. For example, these technologies could enable responsible deployment of AI and other applications that are using increasing amounts of personal data, thereby reducing risks to data privacy.

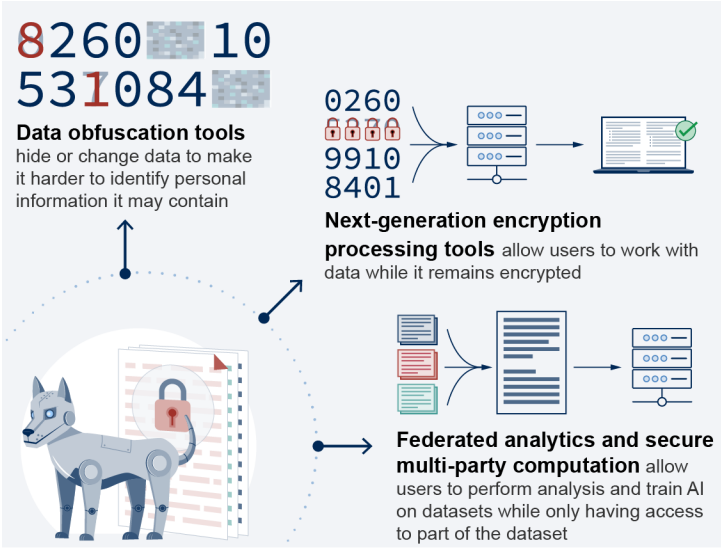
How does it work? Privacy enhancing technologies can be categorized by the different ways they protect data (see figure).

Data obfuscation hides or changes data to make it more difficult to accurately identify personal information. For example, data elements may be removed from datasets to depersonalize them or data can be randomly added as "noise."

Next-generation encryption processing tools keep data encrypted while in use. For example, AI could analyze encrypted documents, such as medical records, without decrypting them first through a process called homomorphic encryption.

Federated analytics and secure multi-party computation allow multiple entities access to parts of datasets, so that if one entity is compromised, the rest of the dataset remains secure. For example, each smartphone can conduct analysis for predictive text applications before manufacturers collect that information, keeping users' raw data private and decentralized.

How Some Privacy Enhancing Technologies Work



Source: GAO analysis and illustration. | GAO-26-109063

How mature is it? These technologies are largely mature, and their use is growing for applications such as AI. Some types are more widely used than others. For example, federated analytics are used by many companies to protect consumer privacy while using their data to train predictive text models. Other types of these technologies can require significant computing power and time, making them difficult to adopt and deploy. For example, analyzing data using homomorphic encryption can take up to a million times as long as analyzing unencrypted data.

Researchers are exploring how privacy enhancing technologies can be used to maximize the utility of existing datasets. For example, secure multi-party computation could enable secure sharing of protected genetic information, giving researchers more opportunities to collaborate.

OPPORTUNITIES

- **Increase privacy.** Limiting access to and obfuscating data results in fewer opportunities for data to leak, which limits opportunities for malicious actors to identify targets and helps mitigate risks in data-driven applications.
- **Make new data sources available.** When data remain private, companies can work collaboratively on proprietary or sensitive data that they might not normally share with competitors and outside groups. For example, banks can safely share information with foreign companies to identify fraud across borders. Researchers can more readily collaborate on sensitive data, like medical records, when those data are protected.

CHALLENGES

- **Reliability.** Some of these technologies, such as data obfuscation, may reveal data in certain cases. Malicious actors are using machine learning and other strategies to work around privacy enhancing technologies.
- **Resource and skill demands.** Some privacy enhancing technologies, such as homomorphic encryption, require more time and other resources than traditional data protection systems. Deploying these technologies effectively requires skill sets that companies and organizations may not possess.
- **Lack of federal guidance.** While the federal government requires certain data to be protected, federal guidance for how or when to use these technologies is limited. This leaves entities uncertain about how to best use them, which could slow adoption across different fields and make implementation difficult or ineffective.

POLICY CONTEXT AND QUESTIONS

- What additional steps could the U.S. government and industry take to protect personal data?
- What is the government's role, if any, in encouraging wider adoption and implementation of privacy enhancing technologies?
- How can institutions balance calls for privacy against calls for greater data transparency and accountability for using data collaboratively?

SELECTED GAO WORK

Artificial Intelligence: OMB Action Needed to Address Privacy-Related Gaps in Federal Guidance, GAO-26-107681.

SELECTED REFERENCE

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches," *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en.

GAO SUPPORT:

The Government Accountability Office (GAO) meets congressional information needs in several ways, including by providing oversight, insight, and foresight on science and technology issues. GAO staff are available to brief on completed bodies of work or specific reports and answer follow-up questions. GAO also provides targeted assistance on specific science and technology topics to support congressional oversight activities and provide advice on legislative proposals.

For more information, contact: Sarah Harvey at HarveyS@gao.gov

Media Relations: Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations: David A. Powner, Acting Managing Director, CongRel@gao.gov

Staff Acknowledgments: Katrina Pekar-Carpenter (Assistant Director), Charlotte Hinkle (Analyst-in-Charge), Hunter Graff, Rachael Johnson, Anika McMillon, Jenique Meekins.

Source (header): THAWEERAT/stock.adobe.com. | GAO-26-109063