This three-paper series was developed through three volunteer workshops at the Federal Identity Forum (FedID) in June 2024, each of which operated under "Chatham House Rules." These papers compile insights and recommendations from workshop participants, aiming to inform the 2024–2025 presidential transition teams on strategic actions to enhance identity security and public trust. Disclaimer: These papers reflect the perspectives of workshop participants and do not represent the formal views of FedID organizers, including federal agencies, MITRE, and the Armed Forces Communications & Electronics Association International (AFCEA).

Privacy, Security, and the Many Forms of Bias

SEPTEMBER 2024

FEDERAL IDENTITY

A significant challenge in identity management is the lack of a comprehensive national privacy framework for identity technologies. Such a framework is essential to guide the evaluation and measurement of identity technologies, instill public trust, and ensure consistency across federal and state levels of government. The incoming presidential administration should prioritize the establishment of this framework to address potential biases, enhance privacy protections, and balance security with economic benefits.

The Case for Action

Current privacy laws and regulations are fragmented and do not reflect modern technological advancements or the current marketplace, which has monetized consumer data and expanded the use of identity tools for various purposes, including law enforcement and access to public benefits. This patchwork approach fails to ensure consistency and public trust in how identity information is collected, used, shared, and stored.

Codifying generally accepted principles and practices for evaluating and measuring the performance of identity technologies is necessary to understand and address potential biases. These biases can result in performance differentials across demographic groups and must be considered in terms of accessibility, usability, and the digital divide. Additionally, it is crucial to evaluate the status quo to understand the baseline performance and biases of current systems. A comprehensive national privacy framework is needed to provide a consistent approach that reflects technological evolution and the current marketplace.

Key Challenges and Opportunities

The lack of a comprehensive national privacy framework for identity technologies is a significant challenge.
Such a framework is essential to guide the evaluation and measurement of identity technologies and tools, instill public trust, and ensure consistency across federal and state governments. Existing privacy policies are disjointed and outdated, failing to keep pace with modern technological advancements and the evolving marketplace.

Potential biases in identity technologies must be addressed.
Codifying principles and practices for evaluating and measuring the performance of identity technologies is essential to understand and mitigate biases. These biases can result in performance differentials across demographic groups and must be considered in terms of accessibility, usability, and the digital divide. Evaluating the status quo is also necessary to understand the baseline performance and biases of current systems.

A consistent approach is needed at all levels of government and sectors.
The current fragmented privacy laws and regulations do not ensure consistency or public trust. Establishing a cohesive set of guidelines is essential to provide a consistent approach that aligns with technological advancements and the contemporary marketplace.

Data-Driven Recommendations

Establish a comprehensive, modernized national privacy framework.
This framework should value privacy while balancing security and enabling economic benefits to industry. Combining legislative and regulatory approaches can provide a means for enforcement and achieve consistency in how identity information is collected, used, stored, and shared. The framework should include provisions for the public's agency over their identity information (e.g., opt-in) and a redress process for individuals adversely affected by identity tools.

Engage broad stakeholders in the development of the privacy framework.
The framework should account for input from various stakeholders, including government, industry, and the public. It should be written in plain language and be easily updated to keep pace with technological and societal changes. Care should be taken to ensure the framework does not unduly limit economic benefits and civil liberties.

Codify practices for evaluating and measuring the performance of identity technologies.
Establishing generally accepted principles and practices for evaluating and measuring identity technologies is essential to minimize potential biases and ensure consistent performance across demographic groups. Additionally, it is important to perform similar analyses on the status quo to properly understand the impacts (positive or negative) of new technologies. This comprehensive approach will help build public trust and confidence in how identity information is handled and ensure that any new implementations are genuinely beneficial compared to existing systems.

Implementation Considerations

- **Lead the charge to enact a national privacy framework.**
  The U.S. government should spearhead the effort to establish a comprehensive privacy framework that governs the evaluation and measurement of identity tools and technologies and guides the collection, use, storage, and sharing of identity information.

- **Ensure broad stakeholder engagement.**
  The privacy framework should be developed with input from various stakeholders, including government, industry, and the public. This will ensure the framework is comprehensive and reflects diverse perspectives.

- **Write the framework in plain language.**
  The privacy framework should be easily understandable and accessible to all stakeholders. It should also be designed to be easily updated to keep pace with technological and societal changes.

- **Balance privacy with economic benefits and civil liberties.**
  Care should be taken to ensure the privacy framework does not unduly limit economic benefits or infringe on civil liberties. The framework should provide a balanced approach that protects privacy while enabling innovation and economic growth.