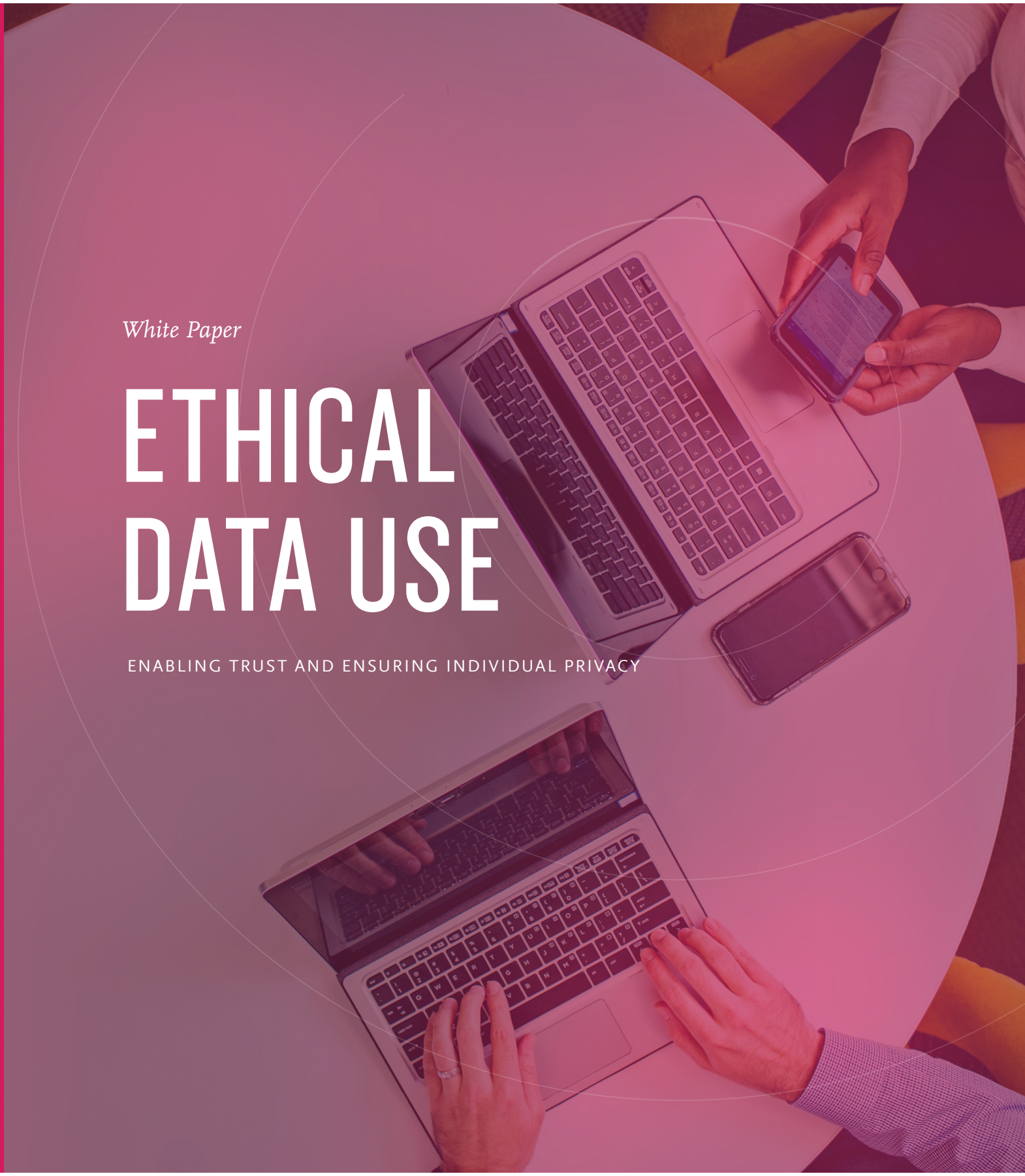
Booz | Allen | Hamilton®



White Paper

ETHICAL DATA USE

ENABLING TRUST AND ENSURING INDIVIDUAL PRIVACY

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

As the government continues to evolve in its use of technology and data, purpose specification and use limitation, increased transparency, data minimization, and the rest of the Fair Information Practice Principles (FIPP) are essential for enabling citizens' trust in government, protecting privacy, and ensuring ethical data use while allowing for technological innovation in the 21st Century.

ENABLING TRUST THROUGH ETHICAL DATA USE

In the United States and across the globe, governments' and organizations' collection and use of Personally Identifiable Information (PII)[1] is rapidly changing and expanding. Technological advancements in areas like cybersecurity and healthcare often rely on PII to operate, and this has made PII one of the world's most valuable and important resources. The U.S. Federal Government's use of PII is primarily regulated by the Privacy Act of 1974 (Privacy Act). While it contains most of the core privacy principles still in use today, it can sometimes be challenging to apply the Privacy Act to new technologies and uses of data. This challenge is significant because government agencies may collect more PII than any one organization, and while there are civil and criminal penalties included in the Privacy Act, agencies are not typically subject to the same level of financial penalties for data misuse as the private sector. Additionally, in the private sector, individuals can choose the companies with whom they provide their PII for benefits and services. If a company uses their PII unethically, individuals usually have the option to switch to another vendor. For essential benefits and services provided by government like Social Security and Medicare, citizens don't have the ability to switch vendors. As such, government agencies have a greater duty to collect and use PII responsibly and ethically to ensure public trust in essential government services, while innovating to improve those services for citizens.

PRIVACY CHALLENGE: HOW TO SUPPORT INNOVATION WHILE PRESERVING INDIVIDUAL PRIVACY

Using PII for innovative purposes presents risks both to the government agency or organization and to individuals. If data is used unethically or irresponsibly, agencies or organizations may suffer reputational harm and the loss of public trust, as well as potential fines and other legal repercussions. As

The U.S. Federal Government's use of PII is primarily regulated by the Privacy Act of 1974 (Privacy Act). While it contains most of the core privacy principles still in use today, it can sometimes be challenging to apply the Privacy Act to new technologies and uses of data.

1. The term "PII," as defined in Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, means "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

for individuals, unethical data use or disclosure may result in financial harm, such as an unauthorized access to an individual's credit card or bank account, or embarrassment, such as sensitive private health data being exposed. Unethical data use can include practices such as over-collecting information, retaining information longer than necessary, sharing information inappropriately, not adequately protecting information, or using information for purposes other than what was originally intended.

PRIVACY CONSIDERATIONS FOR ETHICAL DATA USE

As discussed above, within the Federal Government the use of PII is largely governed by the Privacy Act. The core principles from the Privacy Act (such as an individual's right to access and correct his/her own records) form the foundation for data protection in the Federal Government and throughout the United States, and are based on the Fair Information Practice Principles (FIPP). The FIPPs are a collection of widely accepted best practices that organizations can use as a framework for protecting privacy when implementing policies and procedures and developing systems that impact individual privacy. As such, the FIPPs substantially define ethical data use. For example, the Purpose Specification and Use Limitation Principle states that PII should only be used, processed, stored, maintained, disseminated, or disclosed for a purpose that is explained in a privacy notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.[2] Respecting the Purpose Specification and Use Limitation Principle is a critical part of ethical data use; however, governments can be tempted to retain PII longer than necessary or use PII for purposes other than those for which it was originally collected, leading to unnecessary privacy risk.

Another core FIPP is transparency. The principle of transparency states that organizations should provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII prior to collecting or using PII.[3] Ensuring transparency through unambiguous and straightforward Privacy Notices and Privacy Policies enables individuals to understand how their information will be collected, used, and shared, which ultimately builds trust. When individuals understand how an entity will use their PII, they will likely be more willing to share their data and participate in studies and pilot programs that can spur innovation and lead to breakthroughs in medicine and technology.

Lastly, minimization is a very important FIPP when it comes to ethical data use. The minimization principle states that organizations should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.[4] Only using PII that is relevant and necessary to accomplish the purpose—and doing so for a limited amount of time—will ensure that the organization is not over-collecting PII and creating unnecessary risk.

BALANCING PRIVACY AND INNOVATION: ETHICAL DATA USE AND THE FIPPS IN PRACTICE

Let's discuss two examples that demonstrate how federal agencies are implementing these principles in their innovative initiatives.

- In healthcare, government agencies are increasingly utilizing sensitive PII, such as genetic and biometric data, to provide personalized services to citizens. An example of this is the National Institutes of Health's (NIH) collection of genetic and other health data for personalized patient treatments, as part of the Precision Medicine Initiative's All of Us Research Program.[5] This groundbreaking work has the potential to transform how the medical community and researchers understand public health and treat disease. The All of Us Research Program has its own internal set of Privacy and Trust Principles that go beyond those in the Privacy Act while balancing the need for innovation. For example:
  - Data Sharing, Access, and Use (similar to the Purpose Specification and Use Limitation FIPP): The All of Us Research Program uses multiple tiers of data access—from open to controlled—based on data type, data use, and user qualifications.[6] The All of Us Research Program participants are made aware of the tiers and the interested communities who may utilize their data and have the power of "ongoing consent"—which enables individuals to change their privacy preferences as data sharing, use requirements, and

2. OMB Circular A-130: *Federal Register.* July 28, 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
3. Ibid.
4. Ibid.
5. "What Is the Precision Medicine Initiative? Genetics Home Reference: NIH." U.S. National Library of Medicine. National Institutes of Health. Accessed on December 19, 2019. https://ghr.nlm.nih.gov/primer/precisionmedicine/initiative.
6. "Precision Medicine Initiative: Privacy and Trust Principles." National Institutes of Health. U.S. Department of Health and Human Services. Accessed on December 19, 2019. https://allofus.nih.gov/about/program-overview/precision-medicine-initiative-privacy-and-trust-principles.

As technology evolves, federal agencies will continue to use PII in new and innovative ways.

technology evolve—and withdraw consent for future research or data sharing at any time.[7] This type of engagement guarantees individuals are informed and empowered with control over their own data, while providing interested communities with the valuable resource of PII to conduct research and studies that benefit public health.

- Transparency: PMI has expanded upon the principle of transparency and has begun to develop a dynamic information-sharing process to ensure all participants are informed throughout their involvement in PMI.[8] This process ensures that information is communicated to participants regarding "how, when, and what information and specimens will be collected and stored; generally how their data will be used, accessed, and shared; types of studies for which the individual's data may be used; the goals, potential benefits, and risks of participation, including risks of inappropriate use or compromise of information about participants."[9] This level of detail about the program's data collection and use is critical for transparent, ethical data use and is a noteworthy example of a federal agency balancing privacy with innovation.

- In cybersecurity, the Cybersecurity and Infrastructure Security Agency (CISA) uses cyber threat indicators, which may include PII that is directly related to a cyber threat, received through their Automated Indicator Sharing (AIS) Initiative to better protect computer networks. This innovative approach to information sharing helps public and private sector entities receive cyber threat information in real time and take necessary actions to better protect their information systems. The AIS Initiative has baked in several privacy principles to ensure ethical use of PII. For example:
  - Minimization: CISA has automated and manual processes in place to ensure any PII not directly related to the cyber threat is removed and deleted prior to disseminating the cyber threat indicator through the AIS process.
  - Transparency: The Department of Homeland Security and Department of Justice issued the Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 to ensure transparency regarding the receipt, retention, use, and dissemination of cyber threat indicators under the Cybersecurity Information Sharing Act.[10] In addition, CISA has published a Privacy Impact Assessment (PIA) to help provide notice to the public that their PII may be submitted via AIS and the processes in place to ensure unrelated PII does not get disseminated.[11]

CONCLUSION

As technology evolves, federal agencies will continue to use PII in new and innovative ways. The Privacy Act and the narrow patchwork of governmental privacy laws that have followed are not equipped to serve as the only mechanisms for regulating new uses of PII and ensuring that individual privacy is protected through ethical data use. Agencies and government programs may need to develop their own, internal privacy principles and data use frameworks that are tailored to the agency's own collection and use of PII. PMI and AIS serve as examples of this ethical commitment to balancing privacy and innovation. As the government continues to evolve in its use of technology and data, purpose specification and use limitation, increased transparency, minimization, and the rest of the FIPPs are essential for enabling citizens' trust in government, protecting privacy, and ensuring ethical data use while allowing for technological innovation in the 21st Century.

7. Ibid.
8. Ibid.
9. Ibid.
10. "Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015." Department of Homeland Security (DHS) and the Department of Justice. Accessed June 15, 2018. https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines.pdf.
11. "Automated Indicator Sharing (AIS) Privacy Impact Assessment (PIA), DHS/National Protection and Programs Directorate/PIA-029(a)." Department of Homeland Security. Accessed March 16, 2016. https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_ais_update_03162016.pdf.

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia and more than 80 offices worldwide, our firm employs more than 26,400 people and had revenue of $6.7 billion for the 12 months ending March 31, 2019. To learn more, visit BoozAllen.com. (NYSE: BAH)

FOR MORE INFORMATION, PLEASE VISIT BOOZALLEN.COM OR CONTACT:

Dianna Carr
Lead Associate
carr_dianna@bah.com

Lindsay Madejski
Lead Associate
madejski_lindsay@bah.com