UNITED STATES DEPARTMENT of JUSTICE

National Domestic Communications Assistance Center

Executive Advisory Board Meeting

September 21, 2016

Erika Brown Lee

Chief Privacy and Civil Liberties Officer

U.S. Department of Justice

I. The Fair Information Practice Principles (FIPPs) as a Foundation

- Transparency/Notice
- Individual Participation/Consent
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability/Auditing/Enforcement

FIPPs: Transparency/Notice

- Law enforcement organizations should be transparent and notify individuals regarding collection use, dissemination, and maintenance of PII when practicable for law enforcement.

- One way the Department of Justice incorporates the FIPPs is through its compliance process (e.g. Privacy Impact Assessments and Systems of Record Notices. It is important to consider the FIPPs in other contexts as well.

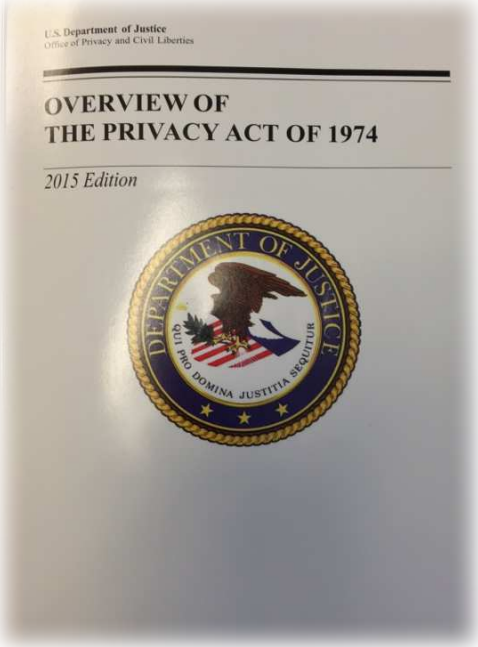
FIPPs: Individual Participation/Consent

- Law enforcement organizations do not typically provide an opportunity for individual consent regarding its, collection, use, and dissemination of PII.

- However, such law enforcement organizations should provide individuals with the opportunity for access to, correction of, and redress regarding the use on an individual's PII when doing so would not interfere with law enforcement activities.

FIPPs: Purpose Specification

- Law enforcement organizations should articulate the legal authority for and the purposes and uses of its collection of PII, this is provided for under the Privacy Act.



FIPPs: Data Minimization

- Law enforcement organizations should only collect PII that is relevant and necessary to accomplish the specified purpose.

- Law enforcement should only maintain and retain this information for as long as is necessary to fulfill the specified purpose.

FIPPs: Use Limitation

- PII should only be used for a purpose compatible with the purpose for which the PII was collected.

- PII should be collected solely in accordance with the notice provided to the individual.

FIPPs: Data Quality and Integrity

- Law enforcement should maintain PII in an accurate, relevant, timely, and complete manner.

- This concept was embedded into the Privacy Act of 1974. However, law enforcement organizations can exempt themselves from some of their requirements under the Privacy Act.

FIPPs: Security

- Law enforcement organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- This important privacy principle requires that DOJ use adequate safeguards, including the encryption of PII, to prevent unauthorized disclosures of information.

FIPPs: Accountability/Auditing/Enforcement

- Law enforcement should be accountable for complying with these principles by providing training on these principles to all employees and contractors who use PII, and auditing the use of PII to demonstrate compliance with these principles.

II. The Bureau of Justice Assistance (BJA) Global Justice information Sharing Initiative (Global)

- BJA provides a robust suite of privacy materials for use by state, local, and tribal law enforcement.

- For more information, visit http://it.ojp.gov/global.