IBTTA
TOLLING. MOVING SMARTER.

OCTOBER 6th, 2020

FDOT

FLORIDA'S TURNPIKE

Data Security Measures in US Tolling Industry

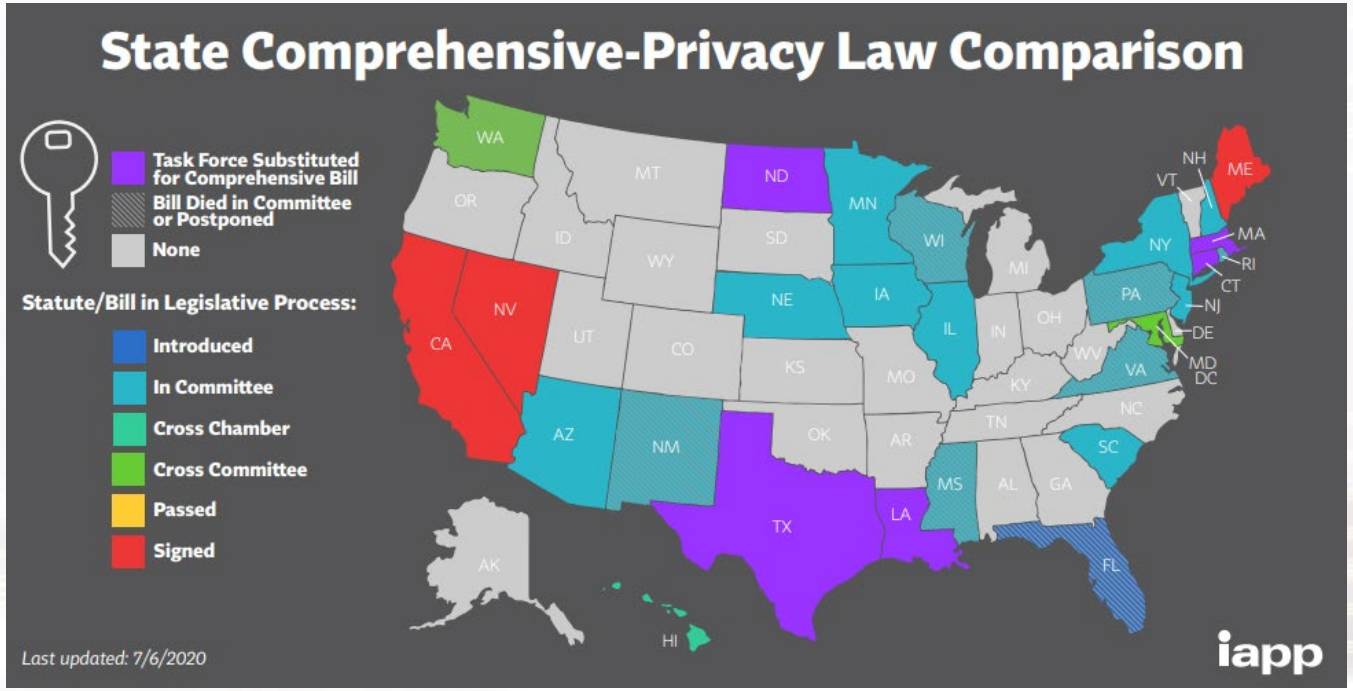
Juan Gomez Lobo
Tolls Data Center Director
Florida's Turnpike Enterprise
Florida Department of Transportation

US Tolling Industry

- **US Tolling industry landscape adds complexity to unified requirements.**
  - Protocols/cash vs. cashless/payment processing strategies/public vs. privately run facilities, etc.
- **US Tolling industry mainly driven by industry requirements with a component of local (state) privacy laws, status, and compliance requirements.**
  - PCI framework is the main driver regarding data security standards and requirements.
- **Tolling facilities at different stages in the technology lifecycle.**
- **Gradual adoption of National Standards (NIOP) for Interoperability.**
- **Public vs. private sector disparities in data security requirements.**
- **Privacy and Sunshine laws are common practices across the Country.**

US Data Protection Regulations

- **Federal Trade Commission (FTC)**
  - Enforcing power regarding data protection regulations
- **State and Local**
  - Lack of strong Federal regulations.
  - States within the US differ in approach to privacy and data security standards.
  - States at different stages of adoption.
  - California leading with CCPA* (California Consumer Privacy Act) leading to other states mimicking the approach.
  - Personally Identifiable and Financial Information must be protected.
  - Entities must have logical, administrative, and physical controls in place to protect consumer PII, PCI, and other personal data.



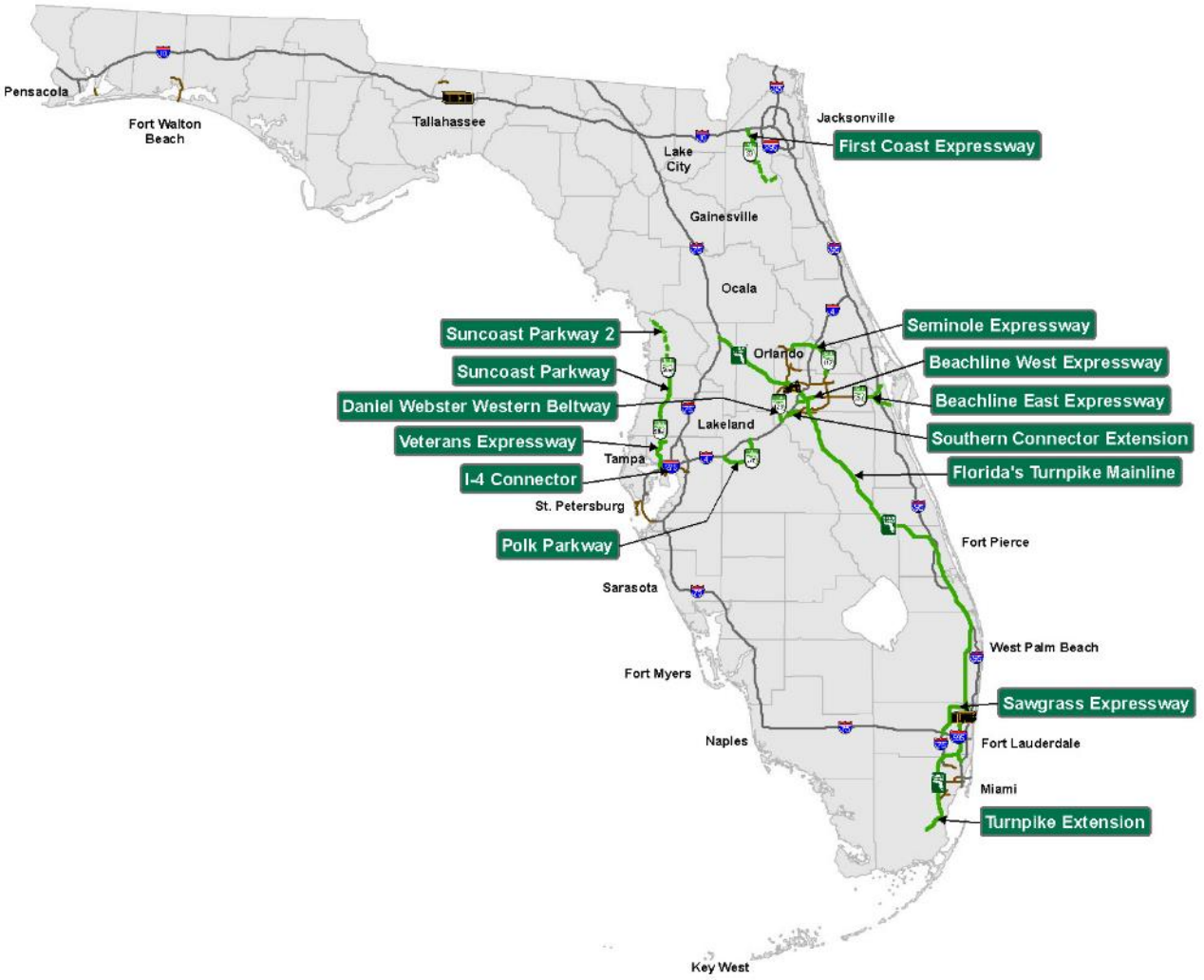
Tolling Path Through Data Security

Toll Agencies are moving towards adoption of:

- National interoperability
- Adoption of tokenization of PCI information
- Transition to All Electronic Tolling
- Addition of security levels based on PCI merchant level/volume of transactions.
- New technologies and new services present challenges regarding data management and security complexities:
  - Smartphone app products and services,
  - Increase in third-party service provider partnerships,
  - Increase of cloud-based operations and services,
  - Increase of IoT saturation – distributed/autonomous roadside sensors,
  - Early stages in multimodal services,
  - CV/AV penetration varies by state – early adoption stages.

Florida’s Turnpike Data Security Approach

- **Customer data privacy is a top priority when addressing strategy and technology lifecycle.**
- **Florida’s Turnpike is governed by Florida State Statutes and US Privacy laws, including PCI-DSS and NIST Cybersecurity Standards.**
- **Florida State Statute governance for Data Security:**
  - Information Technology Security Act (§ 282.318),
  - Security of Confidential Personal Information (§ 501.171),
  - Requirements for Data Security (§ 501.171-2),
  - Requirements for Disposal (§ 501.171-8),
  - Consumer Protection - Remedies of Enforcing Authority (§ 501.207).
- **Consumers presented with options – Opt In / Opt Out of certain services**



OCTOBER 6th, 2020

THANK YOU

Juan Gomez Lobo
Tolls Data Center Director
Florida's Turnpike Enterprise
Email: jigomez.lobo@dot.state.fl.us
Phone: 561-488-5345