Data Privacy For Airports

Michael A. Stephens, Esq.

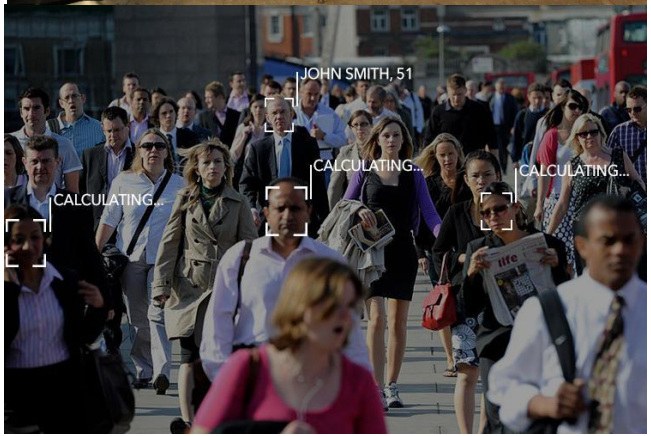
General Counsel & EVP Information Technology

Tampa International Airport

Hillsborough County Aviation Authority
Tampa International, Peter O. Knight,
Plant City and Tampa Executive Airports

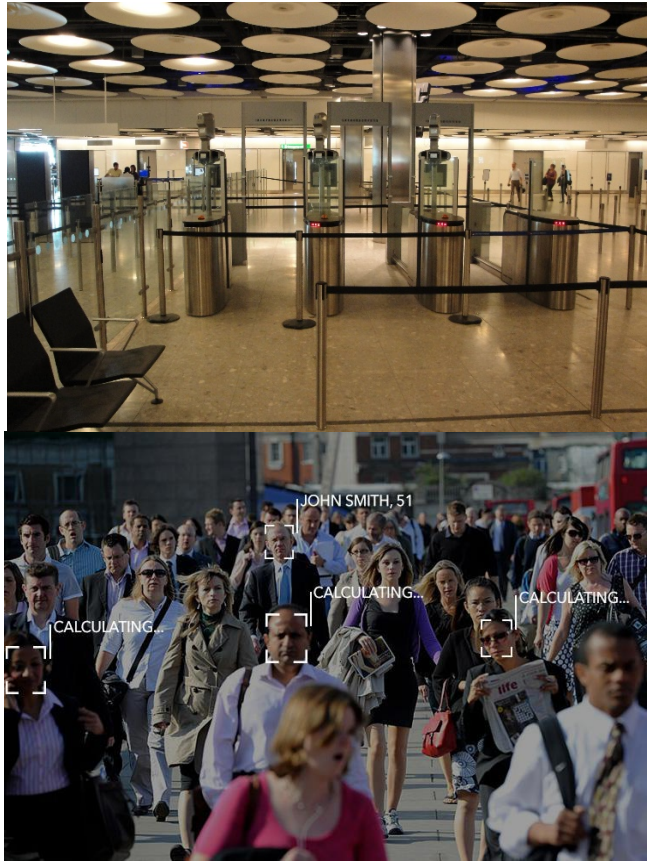
What We Will Talk About

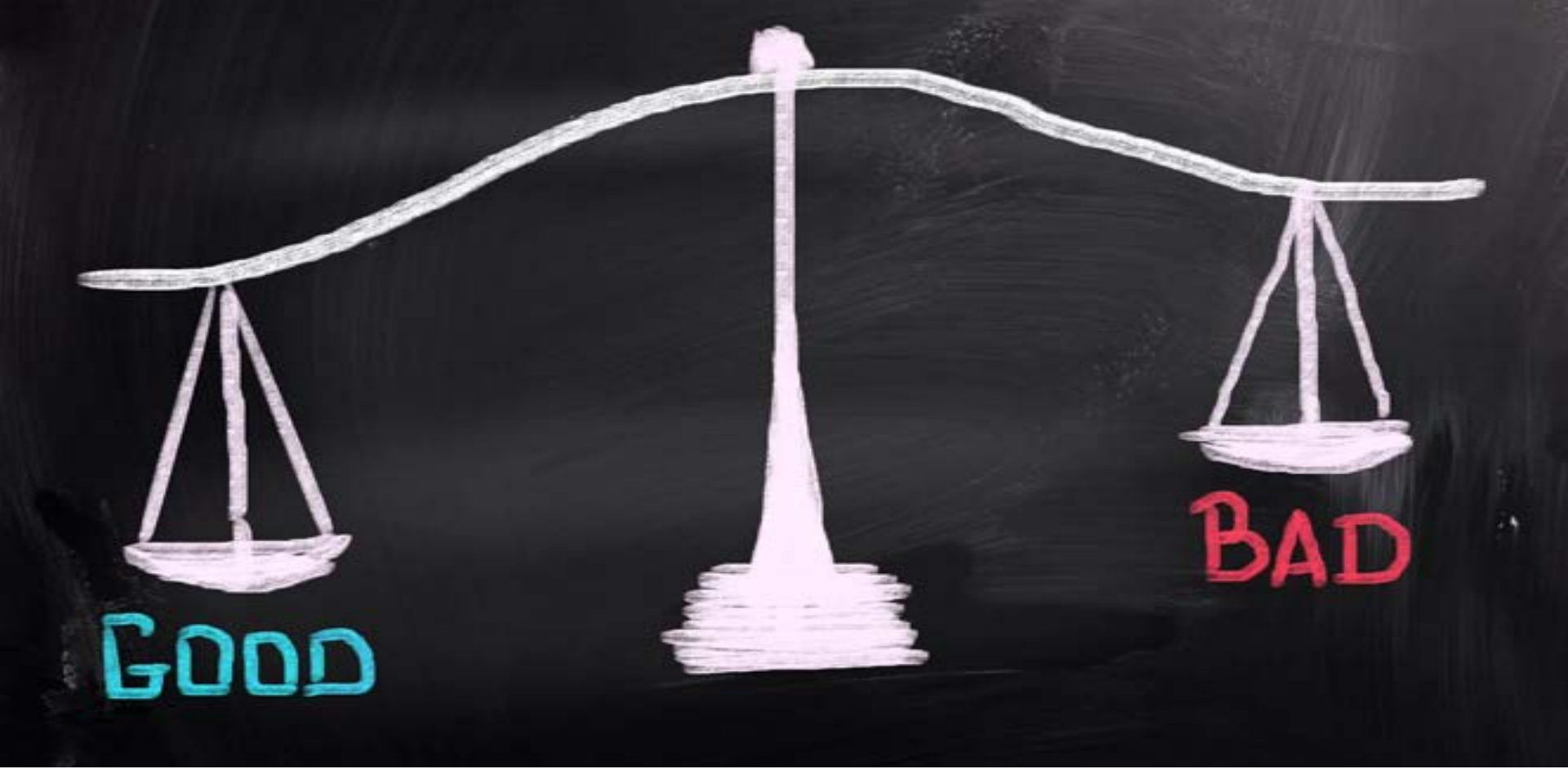
- ✓ What
  - ➢ Ethical and Social Considerations
- ✓ What
  - ➢ Legal Implications of Use Data and Privacy
- ✓ What
  - ➢ Inherent Risks in Airports
- ✓ What
  - ➢ You can do to mitigate the risks



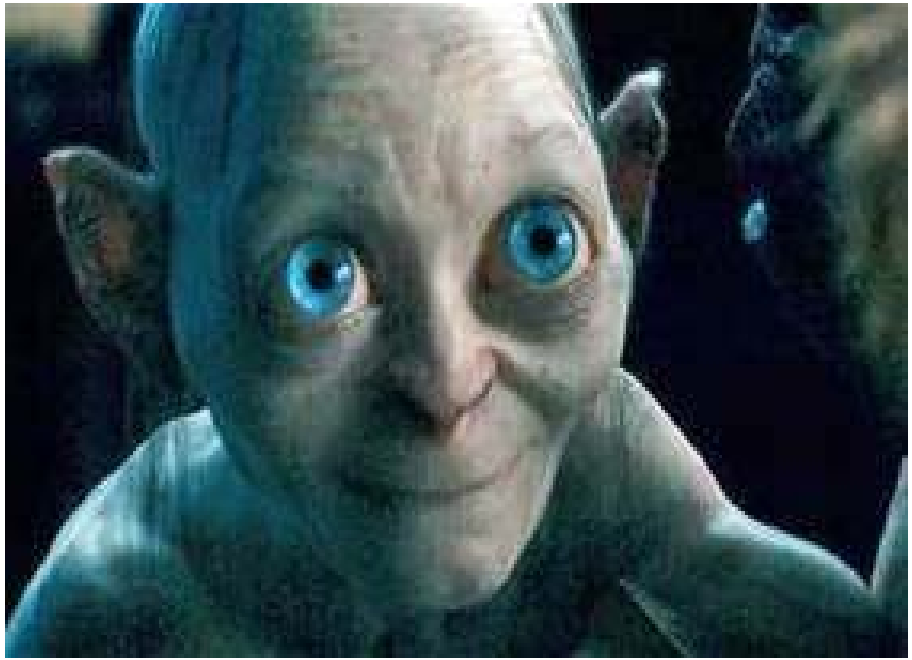
What I Will Not Do

- ✓ What
  - ➢ Deep Dive into Legalese or a treatise on the granularities of the 4th Amendment and other Constitutional or international privacy protections
- ✓ What
  - ➢ Make your eyelids close with a bunch of "Legal Jargon"
- ✓ What
  - ➢ Create an undue delay between you and the next break




GOOD
BAD

The Inherent Conflict Between Gathering Data vs. Legal, Regulatory and Ethical Considerations



Convenience, Security, IT, Marketing, Concessions

Legal, Security, Audit and Data Risk

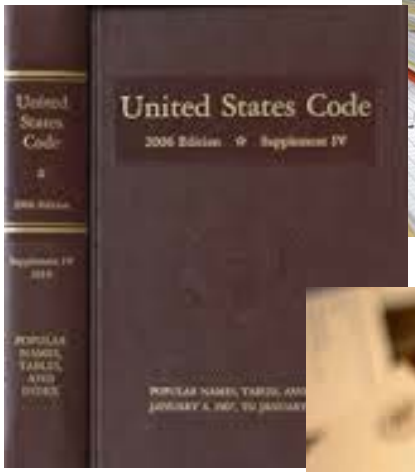
U.S. Privacy Legal Framework

Fair Information Practice Principles (FIPPs) 8 generally accepted principles:

1. Collection limitation
2. Data quality
3. Purpose specification
4. Use limitation
5. Security safeguards
6. Openness
7. Individual participation
8. Accountability

Federal Statutory & Regulatory Data and Privacy Frameworks

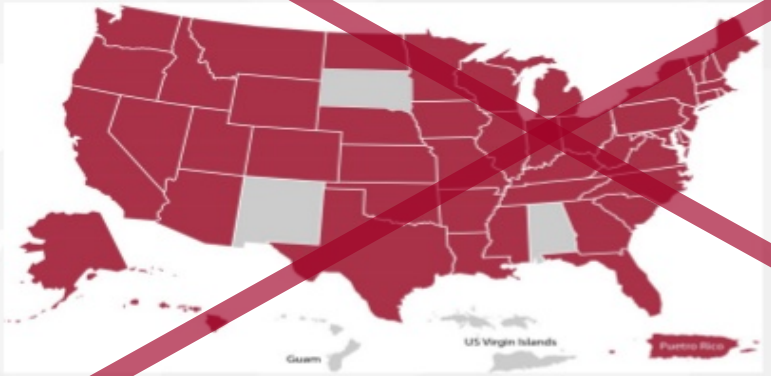
- Executive Order 13636 (February 12, 2013) "Improving Critical Infrastructure Cybersecurity"
- FAA's requirement for certificated airports to adhere to PCI standards
- Federal Trade Commission Act
- SEC disclosure requirements
- Federal Sector Requirements
  - Privacy Act
  - Federal Information Security Management Act
  - OMB's Breach Notification Policy
  - Veterans Affairs Information Security Act
- Children's Online Privacy Protection Act of 1998 (COPPA)
- HIPAA/HITECH
- 49 CFR 1520 protects SSI
- Financial Privacy
  - Fair Credit Reporting Act (FCRA)
  - Fair and Accurate Credit Transactions Act (FACTA)
  - Gramm-Leach-Bliley Act (GLBA)
- Communications and Marketing Privacy
  - Telephone Consumer Protection Act of 1991 (TCPA)
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
  - Telecommunications Act of 1996
  - Cable Television Privacy Act of 1984
  - Video Privacy Protection Act of 1998 (VPPA)



States With Data Breach Statutes

Complex web of breach laws

Organizations that hold regulated data must comply with data breach notification laws.

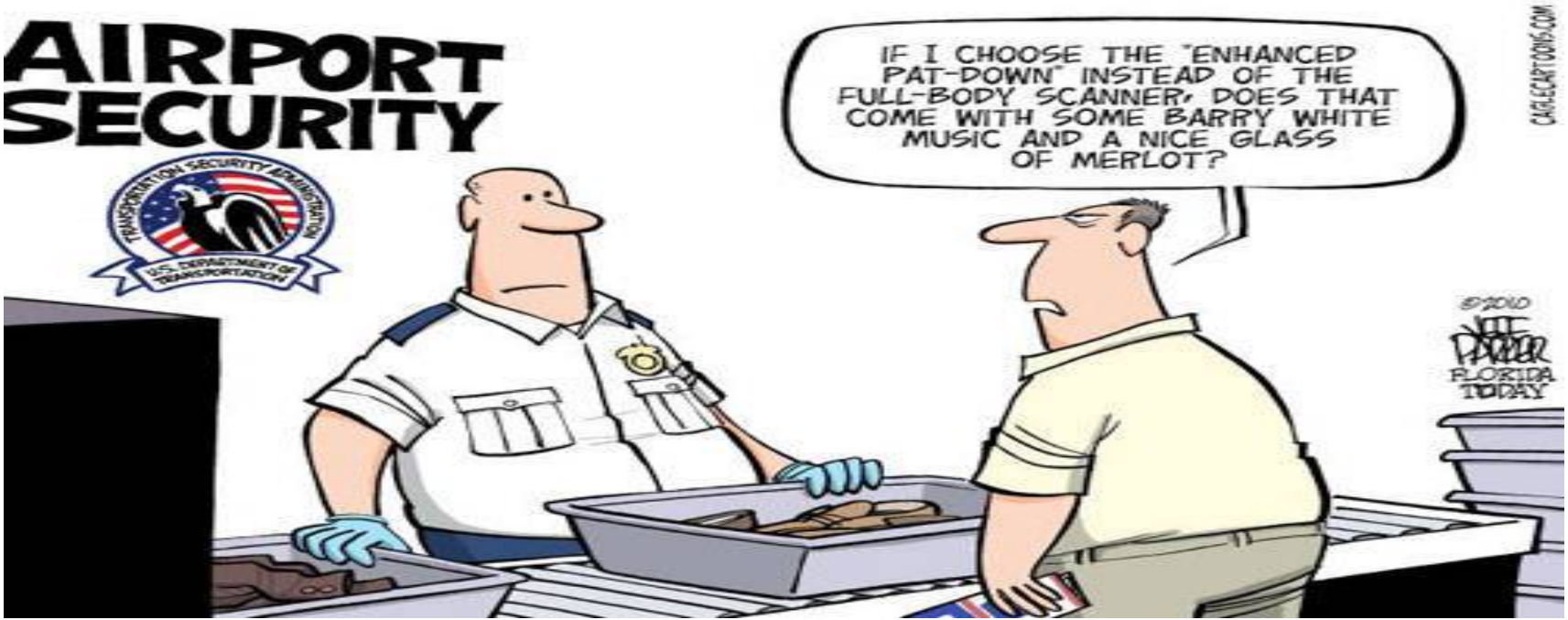


Data Breach Notification Laws:

- 47 state laws
- 3 U.S. territories
- HIPAA Final Breach Notification Rule
- Gramm–Leach–Bliley Act (GLBA)

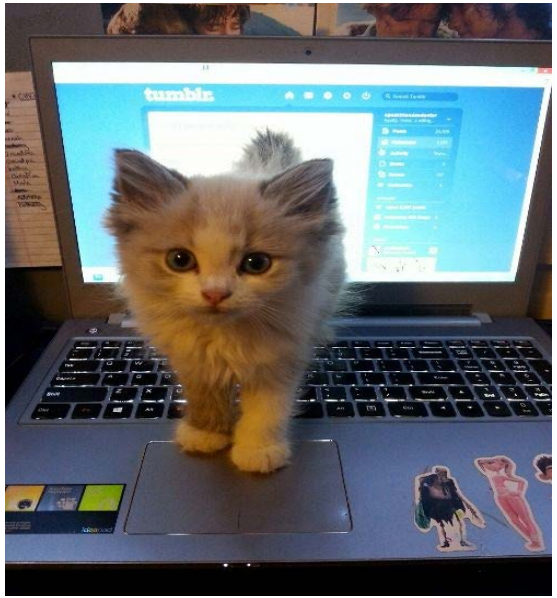
States With Data Breach Statutes

How Much is Too Much (Passenger Convenience)



How Much is Too Much (Privacy)

The Good Good Kitty

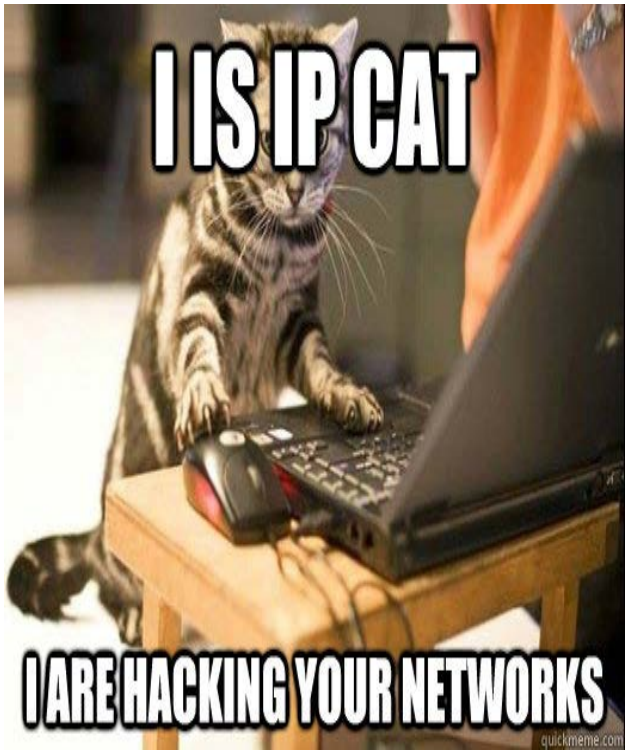


Enhanced Security

Passenger Convenience

Revenue Opportunity

The Not So Good **BAD** Kitty



What Are The Social and Ethical Considerations?

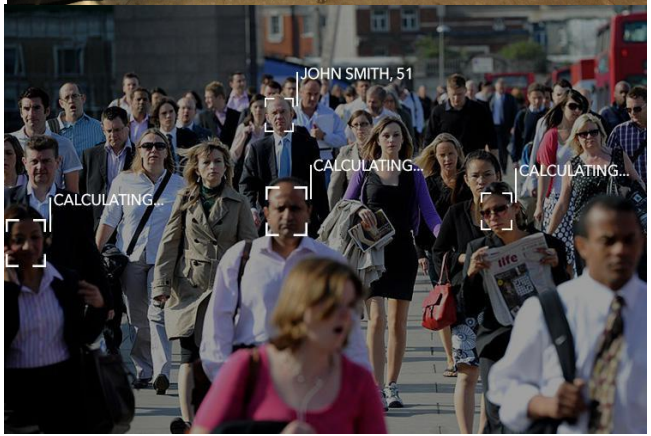
Traveling public are concerned about privacy

Increasing distrust In government's ability to protect data (misuse and data loss)

Error Rate of the Facial Recognition Technology

Potential for bias against certain genders and ethnicities

Over use and expansion for unintended purposes



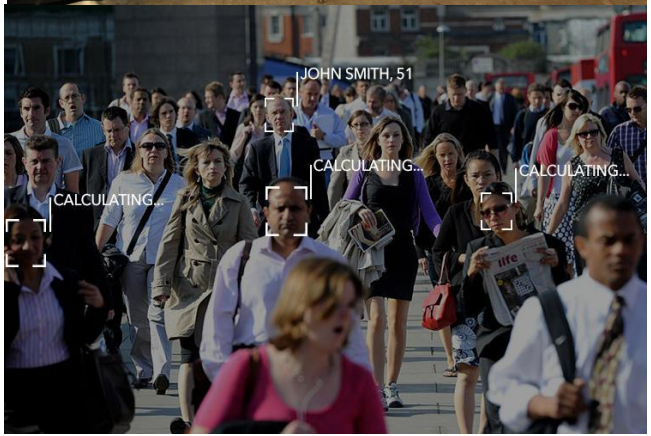
What Is the Legal Authority For Biometric Data Gathering?

Div. F, Title I, of the Fiscal Year (FY) 2016 Consolidated Appropriations Act (P.L. 114-113) (DHS CBP Entry Exit Program)

American Citizens are being biometrically screened upon exit and or entry

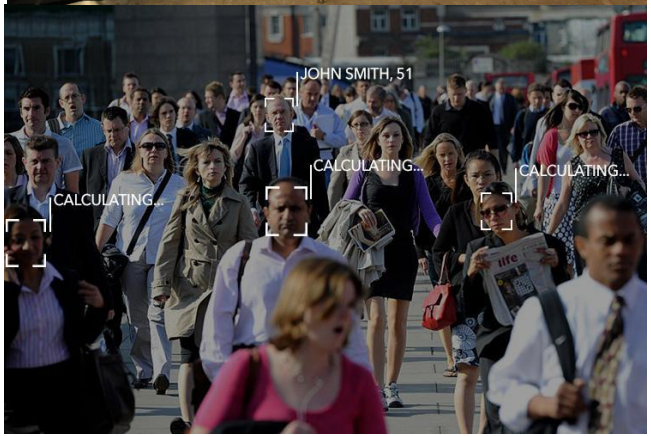
Legal Authority for program questioned by members of Senate from both sides

- Senators Ed Markey and Mike Lee



What Is The Cause For Concern

- Except for forensic analysis of things like fingerprints and DNA, law enforcement collection of biometric information has typically required submitting to a physical search of a person, suspect or individual e.g., taking Fingerprints role or mouth swab.
- The inherent nature of these types of searches may seem negligible, but has significant impact on the Fourth Amendment.
- Courts have historically been comfortable regulating the gathering of biometric data conduct under the Fourth Amendment.
- Courts have limited usage geolocation tracking but not face recognition.
- Face recognition is a game changer because of its great power and ability to allow tracking and identification outside of a traditional Fourth Amendment searches.



I Trust Our Team, Partners and Vendors

Trust But VERIFY

What Is The Cause For Concern

Case Study

The Pinellas County Sheriff ’s Office uses mobile biometric identification quite extensively based on facial recognition through driver license scans. They partner with FBI, CBP and other law enforcement agencies.

What Is The Cause For Concern

Case Study

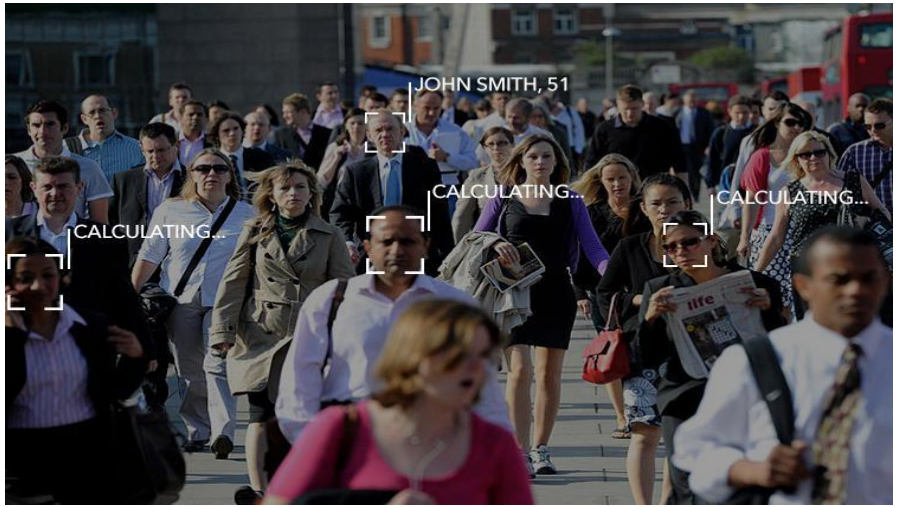
Facebook Faces Class Action Lawsuit Challenging Its Use Of Facial Recognition Data

The plaintiffs are three Illinois Facebook users who sued under a state law that says an entity such as Facebook can't collect and store a person's biometric facial information without their written consent.

Illinois Biometric Information Privacy Act

Finish The Quote

"With Great Power Comes Great……."



Uncle Ben
Spiderman
circa 2002

Voltaire
French
Philosopher
circa 1720

The Conflict Between Gathering Data vs. Legal and Regulatory Risks

Convenience, Security, IT, Marketing, Concessions

Litigation Choking Your Organization

Litigation

- Consumer class action lawsuits
  - Statutory personal rights
  - Tort law negligence
    - **"Reasonable care"**
- Contract breach
  - Failure to use reasonable care to protect data under NDA or confidentiality covenants
  - First Circuit: Bank failed to provide **commercially reasonable** data security
    - Patco Construction Co., Inc. v. People's United Bank
- Privacy and Breach Laws
  - The law requires **reasonable care** to protect confidentiality and PII

Adapt and Overcome

Strategies to Implement a Privacy Program

- Know your organization's data
  - **What** data are you collecting (and from whom)?
  - **Where** are you processing data?
  - **Who** are you sharing data with?
  - **When** do you collect data?
  - **Why** are you collecting data (business/legal purposes)?
  - **How** are you using data?
  - **Do** you have clear legal authority to collect the data and or share it
- Avoid "Someday Syndrome" – don't collect more data than you need

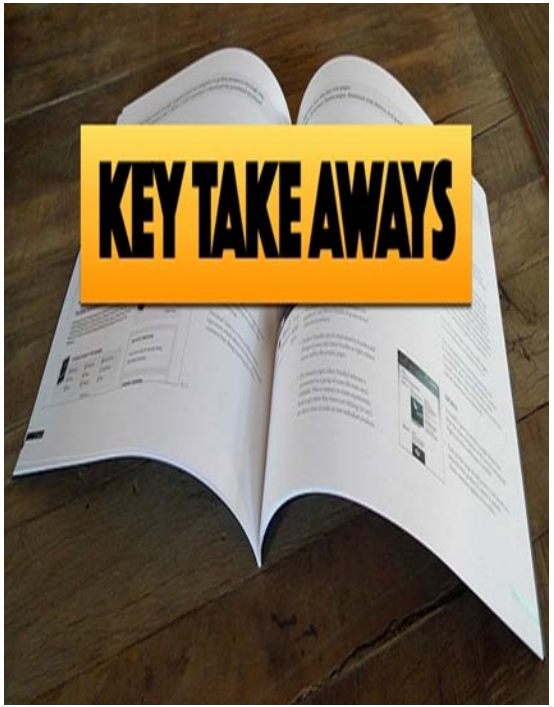
Strategies to Implement a Privacy Program

Vendors, agents, & third parties:

- Must manage risks when sharing information or engaging external service providers with clear parameters and penalties for misuse
- All agencies, partners and vendors, not just on IT vendors
- Vendor Assessments
  - Security standards
    - Request and review security audit reports
      - SOC 1 (SSAE 16): Internal controls over financial reporting
      - SOC 2: Data security, availability, integrity, privacy, etc.
    - Security policies and incident response policies

Final Key Recommendations

- Be able to demonstrate that your organization has taken reasonable steps to address the privacy and security of collecting Biometric and personal data, including:
  - Policies and procedures, including a data breach protocol
  - Training programs
  - Communications that promote privacy awareness
  - Monitoring and auditing electronic systems
- Have a data breach protocol in place including:
  - Who to involve in the privacy breach response team
  - How communications and notifications will be handled
  - Involvement of Legal counsel and IT Security Firms
  - **PRACTICE IT** Tabletop Exercises



Thank You

Michael A. Stephens, Esq.
General Counsel & EVP Information Technology

Tampa International Airport

Hillsborough County Aviation Authority
Tampa International, Peter O. Knight,
Plant City and Tampa Executive Airports