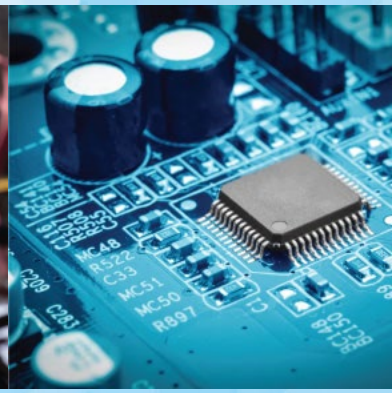






IEEE Digital Privacy Project

Christopher Gorog, Chair, IEEE Digital Privacy Project
Sin-Kuen Hawkins, Program Director, IEEE Future Directions Committee

8.30.2021

Background – IEEE Digital Privacy

- **Mission/Goals**
  - The IEEE Digital Privacy effort is dedicated to advancing solutions that ***champion Digital Privacy of personal and private information***
  - Promoting the development and use of organizational and global architectures, public frameworks, privacy enabling technologies, standards development, compliance with user enacted control of personal data, devices and applications privacy parameters, neutral governance bodies, and policy-supporting legislation
  - Fostering alliances within IEEE OUs, and between IEEE and other global organizations institutions with similar objectives to achieve widely-accepted solutions and standards
  - Maintaining neutrality of operations and public visibility of controls to the greatest extent possible

- **Driving Needs**
  - Most privacy regulation and protection efforts are focused on Corporate Data Protection
  - Individual privacy is a top social concern, but personal Digital Privacy solutions are under-developed and inadequate
  - Privacy should be implemented as a primary architectural facet (not an afterthought)

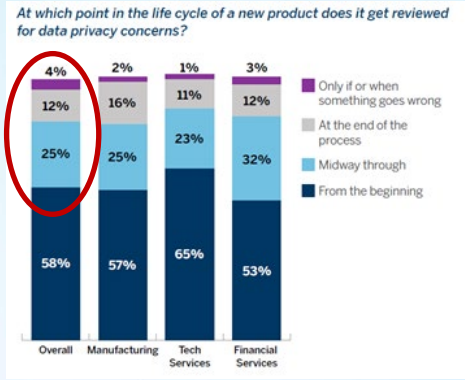
Policy makers and legislators are looking at digital privacy from a legal perspective

- What is Digital Privacy ? What does it mean?
- What happens if it's violated? What are the punishments?
- What are the rights of individuals - to own and control their data?
- What data can be collected, stored, shared, and accessed?
- What are the responsibility and obligations of the data "holders"?

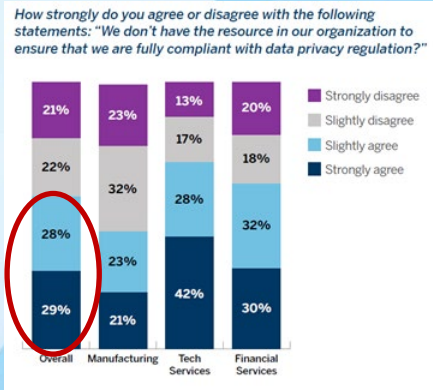
Big companies are not addressing individual privacy rights adequately

500 leaders of large-sized companies were polled

- 79% still feel vulnerable to data privacy crisis



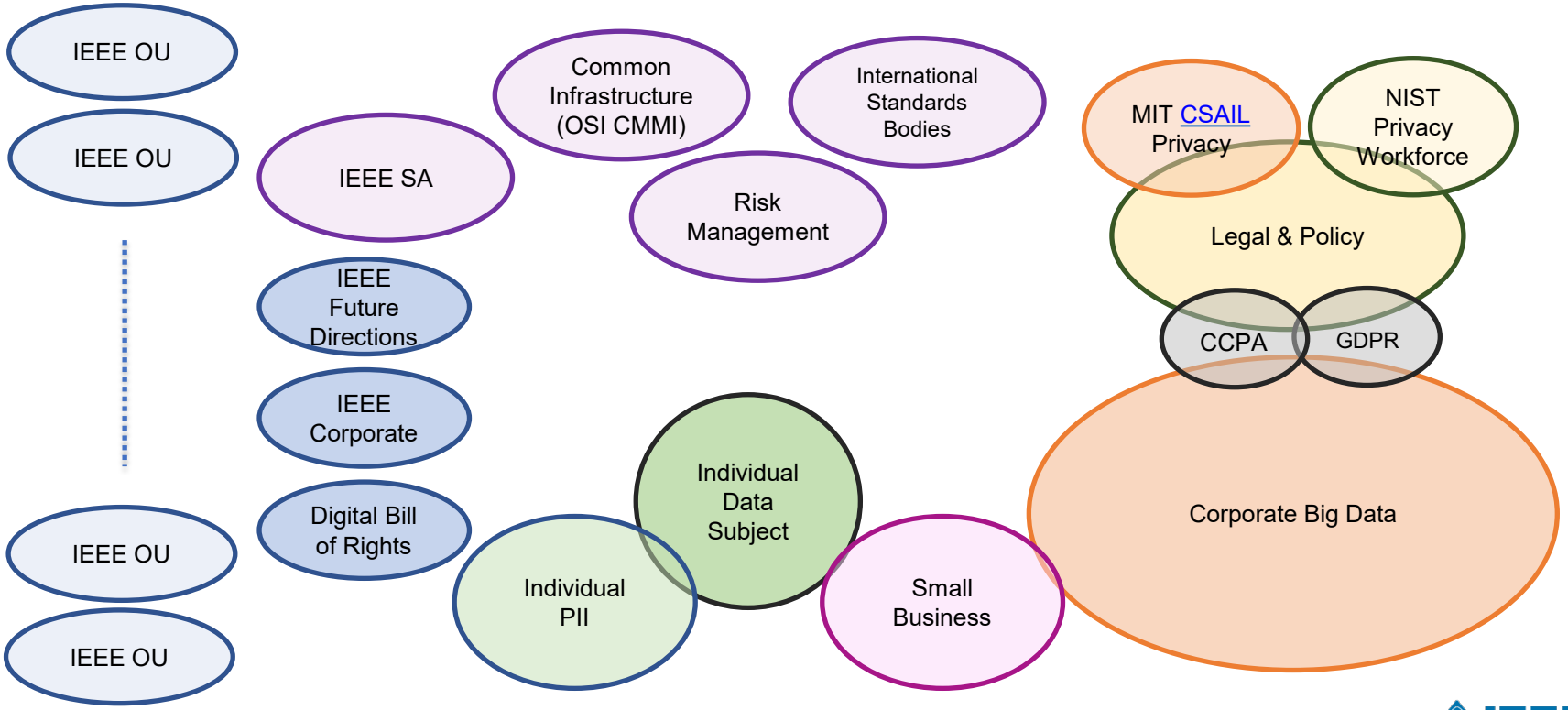
- More than 40% are not building privacy into the design of products & systems



- Nearly 60% do not have the resources to ensure full compliance with data privacy regulation

- Individual privacy is a top social concern, but even large-sized companies lag in providing the resources and solutions!
- In addition, companies are driven by own business incentives and not looking out for individuals.

Existing Siloed Landscape for Privacy

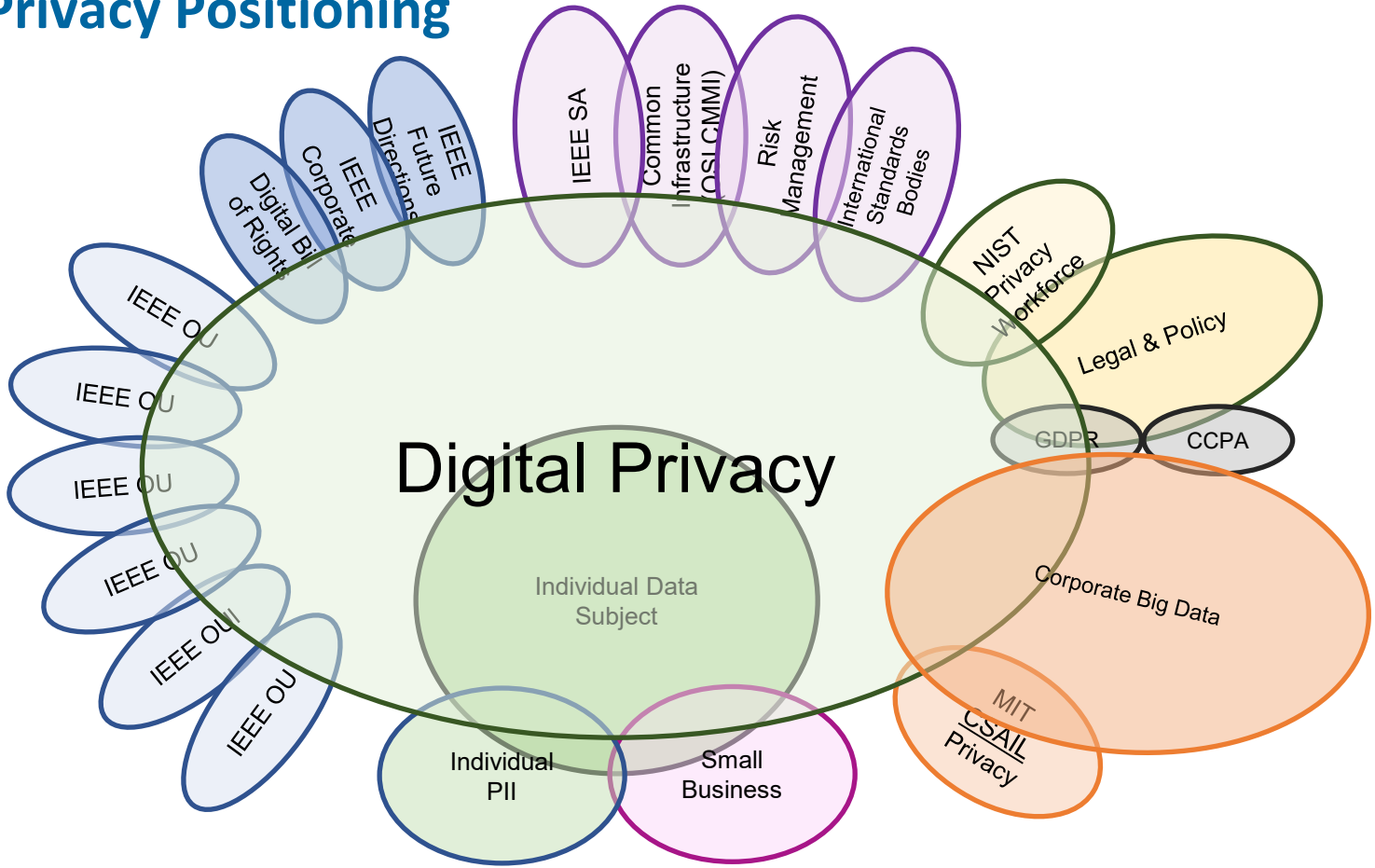


Where does IEEE fit in this conversation?

Digital Privacy Project Connecting Siloed Privacy Efforts

- Large Individual Membership Base
- Bring the technical know how to implement digital privacy
- International Presence - Identify gaps where more research are needed
- Help policy makers and legislators understand technical feasibility of their proposals
- Widely Industry Connections - Establish design guidelines to have privacy built into products & systems
- Represent IEEE Membership base in support of Digital Privacy of personal and private information
- Connect external efforts with IEEE Operational Units
  - Privacy Workforce Public Working Group | NIST
  - MIT Future of Data, Trust, and Privacy | CSAIL Alliances

Digital Privacy Positioning



What are some of the concerns that need to be addressed ?

- Scope, responsibility, and accountability policy of Data Holders
- Rights of individuals to own and to control their own data
- Requirements for data collection, storage, sharing, and accessibility
- Policy and ethics for consistent and fair data treatment
- Unique cultural and jurisdictional perspectives of data
- Confidentiality challenges of aggregated data
- Privacy preserving incentive mechanisms and economic models and business practices
- Evolving privacy enhancing technologies, methodologies, and standards to support changing data policies

Addressing Privacy Dimensions w/ Policy and Technological Enforcement

- Public Visibility
- Private/Confidential

- Non provable Metadata
- Searchability of Data/Metadata

- Value of Data as Economic Indicator
- Trend of Economic Data
- Visibility to Economic Indicators

- Owner Opt-in to Proxy Data Storage
- Owner Opt-out to Proxy Data Storage

- Local Machine Containment
- Remote System Persistence

- Provable Data Integrity
- Value of Individual Data

- Ability of Neutral Verification
- Owners Rights to Verify Data

- Fair Incentivization
- Dispute Resolution

- Data Priority
- Metadata Lineage
- Data Reliability
- Data Quality

- Value of Aggregated Data
- Jurisdiction of Aggregated Data

- Data Proxy Agent Rights
- Regulatory Responsibility to Owner

- Information Sharing
- Compliance Enforcement

- Data Accountability
- Data Trust
- Data and Transaction Risk

- Independence of Participants
- Vetting and Selection of Participants
- Penalization and Removal of Participants
- Participants Cohesion Risks

- Accountability of Transactor
- Anonymity of Transactor

- Restriction Audit Access
- Public Visibility

- Data in Transit
- Data in Rest

- Modularity for Multiple Use Cases
- Adaptability and Scalability

Get Involved !

- We welcome your participation and we want to hear from you!
- Contact: digitalprivacyinfo@ieee.org