An Overview of Issues in

- Protection of Customer Data
- Data Privacy/ Protection Compliance
- Cybersecurity
- Trade Secrets

Presented by:

Francisco Tschen, PE, Esq.
Tschen Law, PLLC | Adjunct Professor of Law - FIU
ftschen@tschenlaw.com

And

Cheryl L. Booth, J.D., MLIS, Ph.D, LL.M | CIPP (US); CIPM; AIGP
Associate Director for Research and Reference Services |
Adjunct Professor of Law – NSU Law
cbooth1@nova.edu

PROTECTING CUSTOMER DATA
And Some Compliance Essentials

Risk Management & Managing Risk

- ***Customer information is BOTH an ASSET (can include Trade Secrets) and a potential RISK***
  - ***RISK can be monetary, of course, but also REPUTATIONAL***
- Businesses/ organizations need to PROTECT the ASSET and AVOID/ MITIGATE the potential Risk
- Implementing an appropriate PRIVACY/ DATA MANAGEMENT PROGRAM can help with BOTH.

Privacy vs. Security

Risk comes from both from the PRIVACY SIDE, and the SECURITY SIDE

Privacy ≠ Security -HOWEVER, they are sort of flip sides of the same coin.

- **Privacy** speaks to what information about ourself is disclosed or withheld from dissemination.
  - Risk here is that information that was NOT intended to be disclosed – or should NOT have been disclosed - is, in fact, disclosed.
- **Security** speaks to the manner in which the information is 'housed' or secured by the receiving party, including the technological and/or physical mechanisms used to control access to that information (Bambauer, 2013).
  - Risk here is that even though you MEANT to keep the customer's information private, the safeguards you had in place to do so were insufficient in some way.

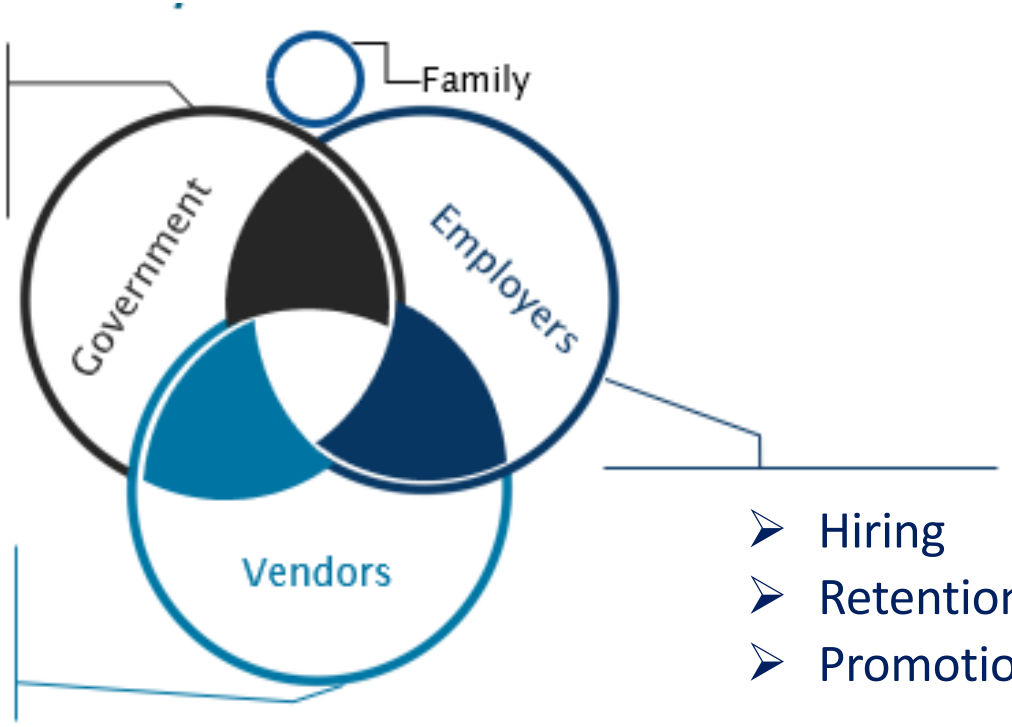
***Data security implements one's information privacy choices* (Bambauer, 2013).**

SOURCES OF PRIVACY RISKS

Unlike cyber risks, the concerns are the lawful access and misuse of personal information

- Privacy risks stem from the lawful access to information considered personal or private by the individual
- Unlike cyber risks, the concerns are the lawful access and misuse of personal information

- Fourth Amendment
- Third Party Records
- Subpoena Power



- Insurance Coverage
- Health Care
- Digital Redlining
- Targeted Advertising

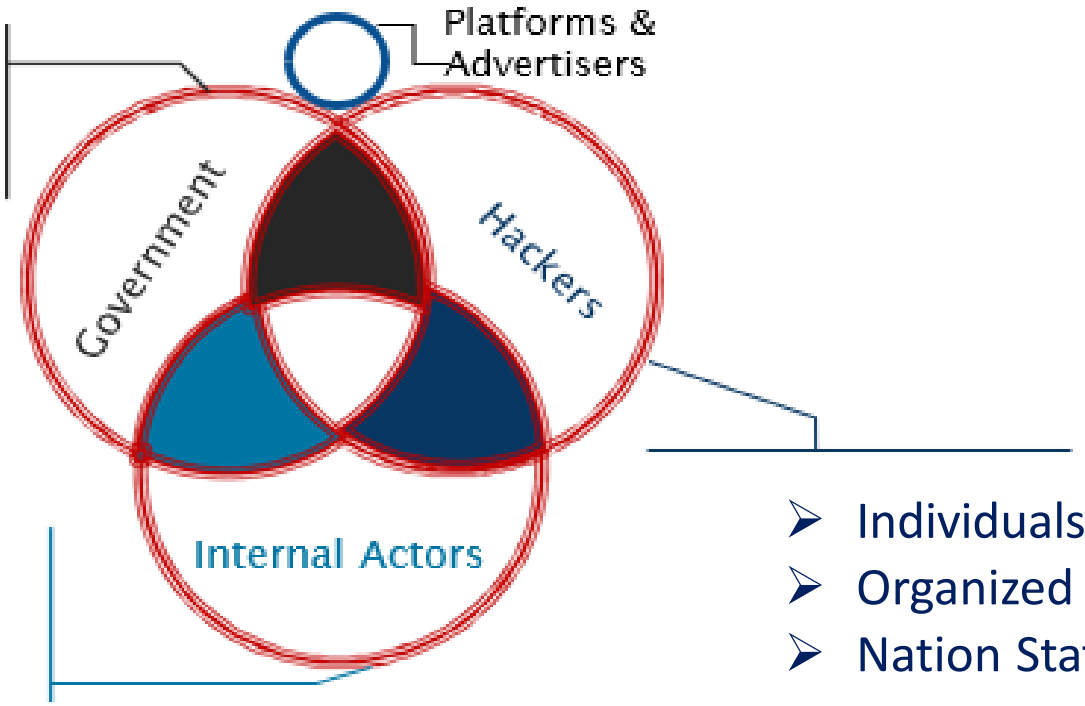
- Hiring
- Retention
- Promotion

SOURCES OF CYBER RISKS

Unlike cyber risks, the concerns are the lawful access and misuse of personal information

- The three sources of risk all seek to obtain private information
- Companies that have no private information have no cyber risk
- Platforms in violation of state laws are annoying

- Fourth Amendment
- Third Party Records
- Subpoena Power



- Poor Policies
- **Disgruntled/ Former Employees**
- Vendors

- Individuals
- Organized Crime
- Nation States

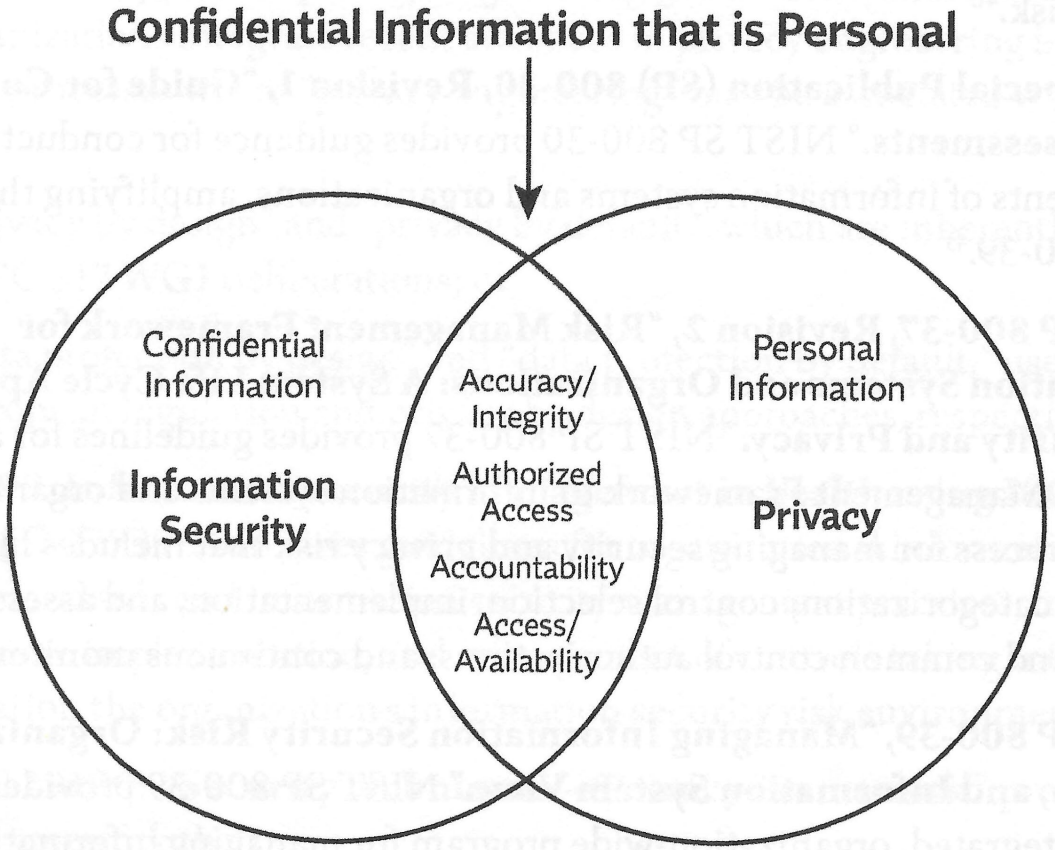
NSU Florida

Risk Management & Managing Risk

- ***A Privacy Management Program simply means having a PLAN in place that accounts for identifying and managing:***
- WHAT information you **NEED** to collect and your INTENDED PURPOSE for collecting and using it;
- HOW you will use it;
- HOW you collect it;
- HOW you protect it;
  - INCLUDING **WHO** you are allowing to access it.

Privacy ≠ Security

Figure 5-6: Privacy versus Information Security



IAPP. Russel Densmore, Ed.. Privacy Program Management (3rd Ed., 2022).

Don’t reinvent the wheel, though…

Leverage your existing Risk Management/ Compliance Framework, and incorporate these Data Privacy and Data Security practices.

If you are still developing one, so much the better!
Key here is to plan ahead and be aware of the potential risks to be mitigated.

Don’t reinvent the wheel, though…

You may already have some RISK MITIGATION/ security practices in place – such as

PHYSICAL CONTROLS – “govern physical access to hard copies of data and the systems that process and store electronic records.”

TECHNICAL CONTROLS – such as user authentication/ MFA; logical access controls

ADMINISTRATIVE/ POLICY CONTROLS – Incident response processes; management oversight; security awareness and training; policies concerning how the company handles data… Limiting access to certain types of information to only those employees whose role requires it.

Don’t reinvent the wheel, though…

You may already have some RISK MITIGATION/ security practices in place – such as

PHYSICAL CONTROLS – “govern physical access to hard copies of data and the systems that process and store electronic records.”

TECHNICAL CONTROLS – such as user authentication/ MFA; logical access controls

ADMINISTRATIVE/ POLICY CONTROLS – Incident response processes; management oversight; security awareness and training; policies concerning how the company handles data… Limiting access to certain types of information to only those employees whose role requires it.

PbD

- Privacy by Design (PbD) is the philosophy or approach of “embedding privacy into the design of technology, systems, and practices…”
  - It is specifically named in the EU’s GDPR (Article 25) as a requirement.
  - Basic tenets:
    - PROACTIVE (not reactive) | PREVENTIVE not remedial
    - PRIVACY IS THE DEFAULT (all decisions in favor of protecting privacy)
    - Privacy is embedded into the design of the system, procedure etc.
    - Full functionality – Positive-Sum (win-win) NOT zero-sum
    - End-to-End security – LIFE CYCLE protection (remember – Security implements Privacy’s choices…)
    - VISIBILITY and TRANSPARENCY
    - *******RESPECT FOR USER PRIVACY *******

FAIR INFORMATION PRACTICES

- Also leverage FIPs
- FIPs are “basic privacy principles central to several (legal) frameworks.”
  - Perhaps the most widely recognized among these is the OECD (Organization for Economic Co-operation and Development) Guidelines, which informs a number of legal frameworks.

FAIR INFORMATION PRACTICES

RIGHTS OF INDIVIDUALS

- Notice
- Choice & Consent
- Data Subject (customer) Access

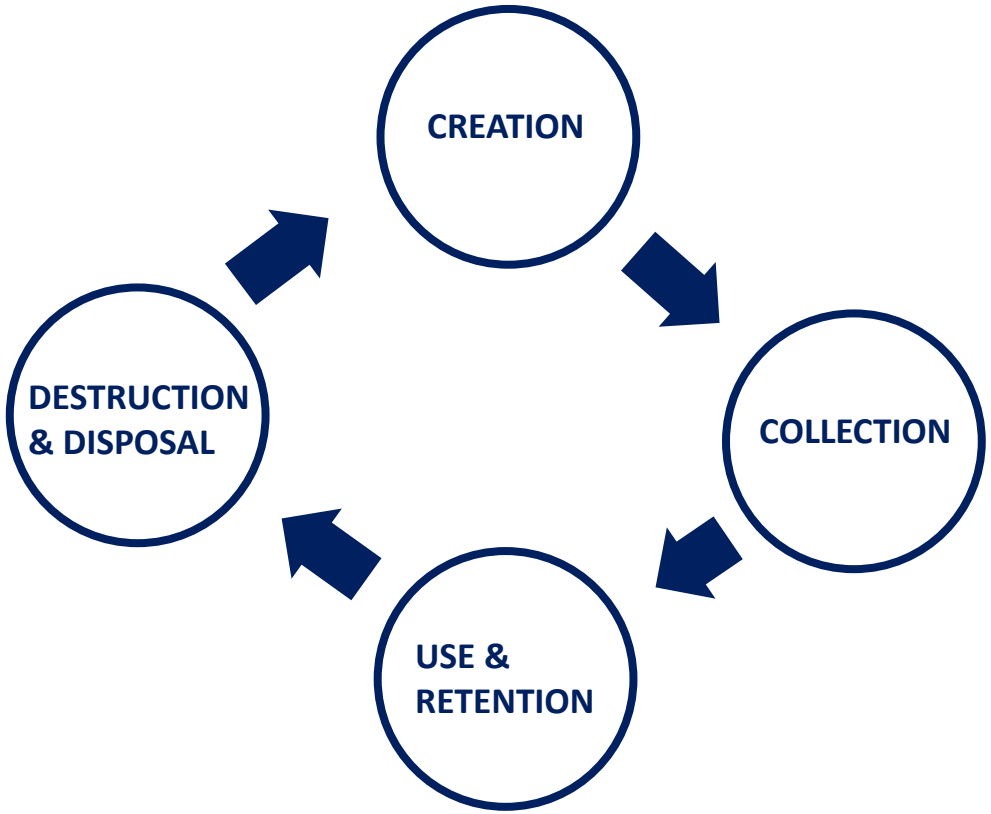
CONTROLS ON INFORMATION

- Information Security
- Information QUALITY

MANAGEMENT

- Management & Administration
- Monitoring & Enforcement

INFORMATION LIFE CYCLE



FAIR INFORMATION PRACTICES

- FIPs capture commonalties between and among many different privacy and data protection laws.

- Ex:
  - Notice requirements
  - Limits on Data Retention
  - Limits on Purpose
  - Choice and Consent provisions
  - Individual's rights
  - Access
  - Correction
  - Deletion
  - Organizational Safeguards (safeguarding data).

DATA INVENTORY/ DATA MAPPING

- Another important tool in your box for protecting customer data

- A Data Inventory is “a complete record of all of the personal information your organization stores, uses and processes…”

- Includes at least:
  - What personal information you are collecting and using (type and purpose)
  - Documenting where the information is stored – INCLUDING 3RD PARTY SYSTEMS!!
  - Mapping where the information goes during the life cycle – both internally and externally
  - Sets guidelines for determining how long the information should be retained.
  - Documents what sort of format the information is in (is it identified; anonymized; pseudonymized; in a database with other related information where aggregation could be easy…)
  - Assigning both CATEGORIES and RISK LEVELS to the information (is the information public? Private? Sensitive-private?)
  - “creates a record of the authority of organizational systems that process the personal information.”

THE FEDERAL TRADE COMMISSION

- The Federal Trade Commission is the primary enforcement agency in the area of consumer privacy protection in the U.S.
  - §5 of the FTC Act to regulate consumer privacy; prohibits "unfair or deceptive acts or practices in or affecting commerce."
- The FTC bases its jurisdiction on the obligation of companies to refrain from operating in an unfair or deceptive manner.

  "Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information."
- Under the statute, a practice is unfair and deceptive if "***the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition***."

"***MEAN WHAT YOU SAY, AND SAY WHAT YOU MEAN***"

NSU Florida

THE NATION'S PRIVACY ENFORCER

- FTC Position: the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act, 15 U.S.C. § 45.
  - The Act prohibits "unfair or deceptive acts or practices in or affecting commerce." § 45(n).
    - **Deception**. A deceptive act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."
    - **Unfairness**. The FTC Act classifies a trade practice as unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).
    - Actions of a company can be both deceptive and unfair.

WHAT is being collected

- The U.S. legal framework around Information Privacy Law is SECTORAL
- This means that the type of personal information protected and the extent to which it is/ must be protected depends on WHAT TYPE OF INFORMATION IT IS.
  - Personally Identifiable Information ("PII") - information about the individual that can be connected back to them to the exclusion of any other (Office of E-Government and Information Technology, 2006).
    - PII is what we are really talking about when we discuss issues around information privacy/ data privacy compliance: IS the customer's identity somehow compromised either by a specific piece of information that identifies them, OR aggregated information that collectively points to them…
- Specific statutory protections around information pertaining to:
  - Health
  - Finance
  - Education
- Particular protections for information about/ pertaining to CHILDREN

SELECT FEDERAL LAWS ON PRIVACY

Beginning in the 1970s, Congress has passed a number of laws protecting privacy in various sectors of the information economy:

- **Fair Credit Reporting Act of 1970**, Pub. L. No. 90-32, 15 U.S.C. §§ 1681 et seq. — provides citizens with rights regarding the use and disclosure of their personal information by credit reporting agencies.
- **Privacy Act of 1974**, Pub. L. No. 93-579, 5 U.S.C. § 552a — provides individuals with a number of rights concerning their personal information maintained in government record systems, such as the right to see one's records and to ensure that the information in them is accurate.
- **Family Educational Rights and Privacy Act of 1974 [FERPA]**, Pub. L. No. 93-380, 20 U.S.C. §§ 1221 note, 1232g — protects the privacy of school records.
- **Right to Financial Privacy Act of 1978**, Pub. L. No. 95-630, 12 U.S.C. §§ 3401–3422 — requires a subpoena or search warrant for law enforcement officials to obtain financial records.
- **Foreign Intelligence Surveillance Act of 1978 [FISA]**, Pub. L. No. 95-511, 15 U.S.C. §§ 1801-1811 — regulates foreign intelligence gathering within the U.S.

SELECT FEDERAL LAWS ON PRIVACY

More laws passed in the 1980s

- **Privacy Protection Act of 1980**, Pub. L. No. 96-440, 42 U.S.C. § 2000aa — restricts the government's ability to search and seize the work product of the press and the media.
- **Cable Communications Policy Act of 1984**, Pub. L. No. 98-549, 47 U.S.C. § 551 — mandates privacy protection for records maintained by cable companies.
- **Electronic Communications Privacy Act of 1986**, Pub. L. No. 99-508 and Pub. L. No. 103-414, 18 U.S.C §§ 2510–2522, 2701–2709 — updates federal electronic surveillance law to respond to the new developments in technology.
- **Computer Matching and Privacy Protection Act of 1988**, Pub. L. No. 100-503, 5 U.S.C. §§ 552a — regulates automated investigations conducted by government agencies comparing computer files.
- **Employee Polygraph Protection Act of 1988**, Pub. L. No. 100-347, 29 U.S.C. §§ 2001–2009 — governs the use of polygraphs by employers.
- **Video Privacy Protection Act of 1988**, Pub. L. No. 100-618, 18 U.S.C. §§ 2710–2711 — protects the privacy of videotape rental information.

SELECT FEDERAL LAWS ON PRIVACY

Finally, the 2000s:

- **CAN-SPAM Act of 2003**, Pub. L. No. 108-187 — provides penalties for the transmission of unsolicited e-mail.
- **Fair and Accurate Credit Transactions Act of 2003 [FACTA]**, Pub. L. No. 108-159 — amends and updates the Fair Credit Reporting Act, providing (among other things) additional protections against identity theft
- **Video Voyeurism Prevention Act of 2004**, Pub. L. No. 108-495, 18 U.S.C. § 1801 — criminalizes the capturing of nude images of people (when on federal property) under circumstances where they have a reasonable expectation of privacy.
- **Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009**, Pub. L. No. 111-5 — expands HIPAA's coverage, strengthens penalties for HIPAA violations, and provides for data breach notification under HIPAA.

THE FTC OVERSEES/ ENFORCES MANY OF THESE…

- The Commission has enforcement or administrative responsibilities under more than 70 laws.
- The agency's primary statutes are:
  - the Federal Trade Commission Act;
    - Most privacy rules are enforced under § 5 of the FTC Act
  - the Clayton Act, covering unlawful tying contracts, corporate mergers and acquisitions, and interlocking directorates.
- Among other 70+ FTC-enforced consumer protection statutes are the following:
  - Equal Credit Opportunity Act
  - Truth-in-Lending Act
  - Fair Credit Reporting Act
  - Cigarette Labeling Act
  - Do-Not-Call Implementation Act of 2003
  - Children's Online Privacy Protection Act
  - Fair and Accurate Credit Transactions Act of 2003
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

State Deceptive Trade Practices Acts

- In addition to the FTC Act, which is enforced exclusively by the FTC, every state has some form of deceptive trade practices act of its own.
  - Many state courts have been heavily influenced by FTC cases.

- Many of these statutes not only enable a state attorney general to bring actions but also provide a private cause of action to consumers. Several of these laws have provisions for statutory minimum damages, punitive damages, and attorneys' fees.
  - Cal. Civ. Code § 1780(a)(4) (punitive damages)
  - Conn. Gen. Stat. § 42-110g(a) (punitive damages)
  - N.Y. Gen. Bus. Law § 349(h) (minimum damages).

FTC PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS

PRIVACY BY DESIGN (PbD)

- Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.
  - Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.
    - **Data Minimization** is a critical FIP: If you don't collect it, you don't have to protect it!! So only collect the data you need!
  - Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CHOICE

- Companies should simplify consumer choice.
  - Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.
  - For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

FTC PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS

GREATER TRANSPARENCY

- Companies should increase the transparency of their data practices.
  - Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.
  - Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.
  - Companies must provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected.
  - All stakeholders should work to educate consumers about commercial data privacy practices.

Privacy Programs & Privacy Program Management

- Many companies have a chief privacy officer (CPO) who, among other things, develops a "privacy program" within an institution.
- A privacy program typically has both elements involving compliance and strategy.
  - Compliance means developing safeguards, including training the workforce, to make sure that the company follows all privacy and security laws and regulations.
  - Strategy means assessing privacy risks, training the workforce about privacy awareness, helping to shape products and services so that they minimize any potential privacy concerns, and stopping or limiting a company's actions that consumers might find too privacy-invasive.
- The CPO often helps manage not only the information companies have about consumers but also the data maintained about the workforce.

Privacy Programs & Privacy Program Management

- In some industries, laws or regulations require that companies have a designated employee to handle privacy and security responsibilities.
  - An example would be the FTC's Safeguards Rule, issued pursuant to the Gramm-Leach-Bliley Act, which requires the designation of one employee at the covered entity to manage the company's responsibilities pursuant to the Rule.
- In other industries, and in large part due to the increase in privacy and security obligations, businesses voluntarily have CPOs.

Thank you!