Getting Ready for 2026 – Data Privacy Compliance Priorities

Gretchen Ramos | ramosg@gtlaw.com | 415.374.0216
Darren Abernethy | abernethyd@gtlaw.com | 415.655.1261

December 10, 2025

For information purposes only – not legal advice

Presenters

Gretchen A. Ramos
Global Co-Chair,
Data Privacy & Cybersecurity Group
Greenberg Traurig, LLP

Darren J. Abernethy
Shareholder,
Data Privacy & Cybersecurity Group
Greenberg Traurig, LLP

Today's Agenda

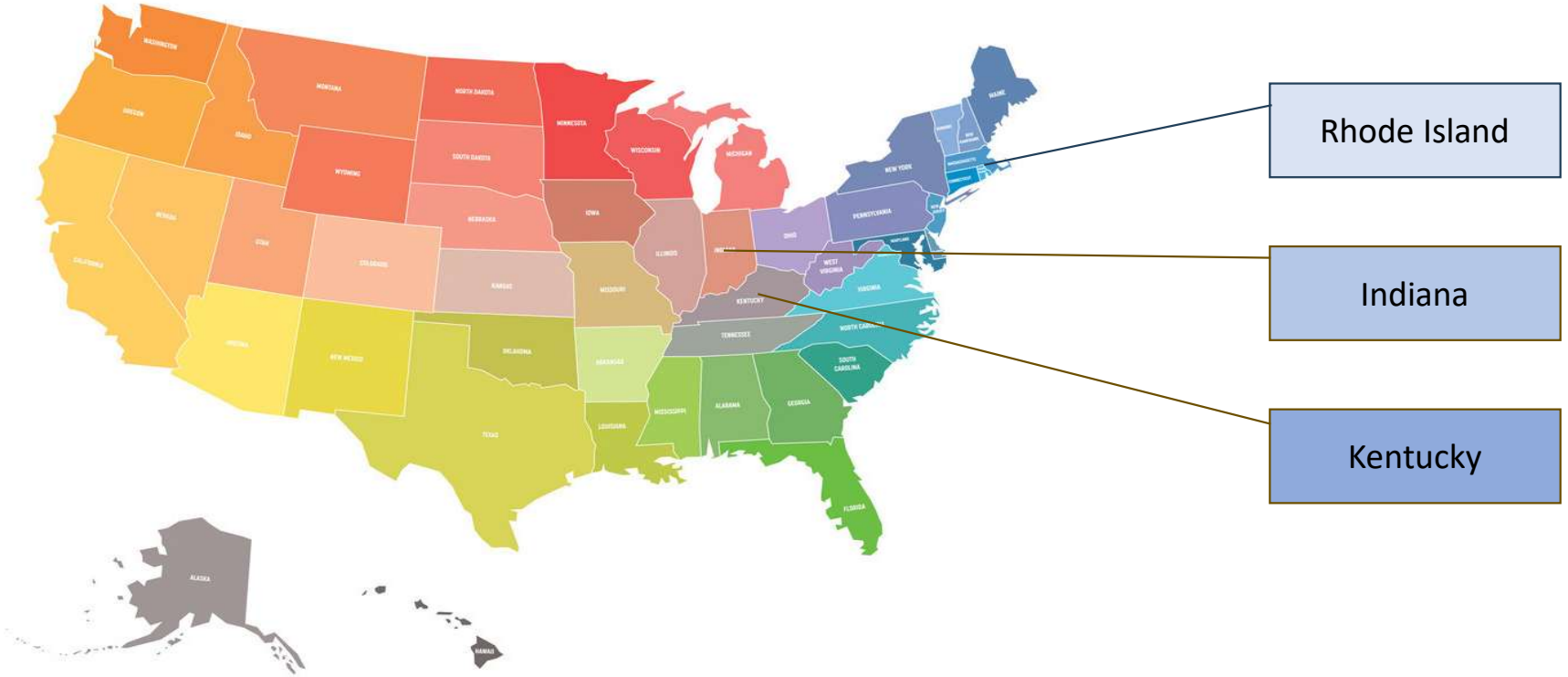
- ✓ New State Privacy Laws
- ✓ 2025 Regulatory Enforcement
- ✓ Litigation Trends
- ✓ 2026 Privacy Compliance Priorities
- ✓ Your Questions

New State Privacy Laws

Comprehensive Privacy Laws

In Place (1.1.26)	Active Bills	No Mandatory Cure Period
• California • Colorado • Connecticut • Delaware • Florida • Indiana • Iowa • Kentucky • Maryland • Minnesota • Montana • Nebraska • New Hampshire • New Jersey • Oregon • Rhode Island • Tennessee • Texas • Utah • Virginia	• Michigan • North Carolina • Pennsylvania • Wisconsin	Jan 2026 • California • Colorado • Connecticut • Delaware • Minnesota • Nebraska • New Hampshire • Oregon • Rhode Island July 2026 • New Jersey • Minnesota

2026 – Three More States



Who Is Subject to New Laws

- Indiana Consumer Data Protection Act (INCDPA), and Kentucky Consumer Data Protection Act (KCDPA)
  - Doing business in or targeting state residents plus annually either (1) processes personal data of **100,000+ residents** OR (2) processes personal data of **25,000** and derives **50%** of gross revenue from sale of personal data
- Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)
  - All commercial websites or online services doing business in RI must have a privacy notice compliant with law.
  - Entire law applies to For profit business doing business in or targeting state residents plus annually either (1) processes or controls personal data of **35,000**+ residents OR (2) processes or controls personal data of 10,000 and derives 20% of gross revenue from sale of personal data

Unique Provisions

- **Rhode Island**
  - Mandatory notice requirement for all commercial websites that process personal information and does business in RI, regardless of data-volume thresholds, must post compliant privacy notice
  - Must identify specific third parties to whom PI has or **may** be sold, along with data categories and contact info
  - No cure period; any intentional disclosure of personal data in violation of the Act will result in a fine between $100 and $500 for each disclosure
  - No obligation to honor global privacy control signal
- **Maryland**
  - Bans selling or using personal data of individuals under the age of 18 for targeted advertising if the controller "knew or should have known" the person was a minor (more stringent than the willful disregard threshold)
  - Controllers may collect and process **only data that is reasonably necessary** and proportionate to provide or maintain a specific product or service requested by the consumer
  - Restricts the collection, use or sharing of sensitive data, **unless it is strictly necessary** to provide or maintain a specific product or service **requested by a consumer**

Key Amendments Eff. 2026

- **Oregon (OCPA)** *[effective Jan. 1, 2026]*
  - Ban on sale of precise geolocation data: ' "precise geolocation information" (that identifies present or past location within a ~1,750-foot radius of a device or individual) may no longer be sold — even with consent
  - Enhanced protections for minors (under 16) — ban on sale of personal data; restrictions on profiling and targeted advertising
- **Connecticut (CTDPA) – SB 1295** [*effective July 1, 2026*]
  - More organizations subject to law:
    - Lowered consumer-data threshold to 35,000 from 100,000
    - Applies to any that processes "sensitive data" regardless of volume or that offers personal data for sale
    - Removes the old broad, entity-level exemption under GLBA; now, only certain traditional financial institutions (e.g., banks, credit unions, regulated insurers, investment advisers/brokers when regulated) exempt
  - Privacy notices must disclose if process/sell data to train LLM, engage in profiling, targeting advertising or sell personal data
  - Expanded right to access to include inferences derived from data, and whether those being used for profiling
  - Right to opt-out of automated decisions expanded to any automated decision, even if human is involved that procedures legal/similarly significant effects; right to contest such decisions
  - Right to contest profiling decisions
  - Prohibits processing of minors' personal data (under 18) for targeted advertising (known or willfully disregarded); consent does not permit use

California - 2026

- CCPA amendments with no delayed enforcement grace period
- As of Jan. 1, 2026:
  - In-scope businesses must provide a means for CA consumers to confirm that their opt-out request to 3Ps has been processed, including GPC.
  - Confirmation that "a consumer closing or navigating away from a pop-up window on a website that requests consent without first affirmatively selecting the equivalent of an "I accept" button shall not constitute consent.
  - Mobile applications "must" (no longer "may") include a link to a PP in Settings.
  - Must provide opt-out notices in IoT/connected devices, AR/VR before or at the time of PI collection.

California – 2026 (cont.)

- As of Jan. 1, 2026:
  - Confirmation that the number of steps a consumer must take to request to opt-out of the sale or sharing of their PI – as measured from when the consumer clicks on a "DNSSMPI" link to completion of the request – should be "the same or fewer" than the number of steps for submitting a request to opt-in to the sale/sharing of PI
  - Financial incentive programs may not be selected by default or made easier to opt-in to than to not participate in the rewards program
  - Privacy policies must identify any categories of PI disclosed in the last 12 months not just to 3Ps but now to service providers and contractors as well

California - 2027

- A “business” using automated decision-making technology (ADMT) for a “significant decision” prior to Jan. 1, 2027 must comply with new ADMT requirements by that date.
- No reference to “AI” but ADMT refers to any technology that processes PI and uses computation to “substantially replace human decision-making,” a defined term.
- Key features: (1) a pre-use notice re: how ADMT will be used, how to opt-out, and how it works; (2) consumer access and opt-out rights.

California - 2027

- California Opt Me Out Act
- Starting Jan. 1. 2027, web browser developers must "include functionality configurable by a consumer that enables the browser to send an opt-out preference signal"
- TBD re: whether browser devs will turn the OOPS functionality on be default; prominence in settings; mobile web; and affect on number of opt-out of sell/share requests businesses receive

California - 2027

- Privacy risk assessments (recall CCPA applies to B2B and HR data!)
  - A business whose processing of PI presents "significant risk" to consumers' privacy must conduct a risk assessment before initiating that processing.
  - processing presents "significant risk" when it involves any of the following activities: (1) selling or sharing personal information; (2) processing sensitive personal information (other than processing employee data for certain HR purposes); or (3) using ADMT to make a significant decision concerning a consumer.
  - Required to submit a report annually to CalPrivacy starting Apr. 1, 2028 containing PRA details (e.g., # of PRAs, use of SPI, and an attestation from a directly responsible "member of the business's executive management team…under penalty of perjury under the laws of the state of California."

California - 2028

- Phased in cybersecurity audit requirement based on the gross global revenue of the business. Audits must cover 18 components of a cybersecurity program.
- Applies to businesses whose processing of CA residents' PI presents "significant risk" to consumers' security, defined by the regulations as the business having:
  - Earned 50% or more of its gross global revenue from selling or sharing PI; or
  - Had $26.625 million in gross global revenue and processed either (1) the PI of 250,000 or more consumers/households, or (2) the sensitive PI of 50,000 or more consumers
- Due dates:
  - April 1, 2028 (>$100 million revenue in 2026)
  - April 1, 2029 (>$50 million revenue in 2027)
  - April 1, 2030 (everyone else)

2025 Regulatory Enforcement

California – 2025 Enforcement

Date	Regulator	Company & Sector	Settlement Amount	Key Alleged Violations & Highlights
March 12, 2025	CPPA	American Honda Motor Co. (automaker / connected-vehicle context)	$632,500	Required excessive info for opt-out requests; asymmetry in user privacy portal; inadequate contracts with ad-tech vendors
May 6, 2025	CPPA	Todd Snyder, Inc. (clothing retailer)	$345,178	Opt-out requests not processed for ~40 days; required excessive verification for opt-out of sale/sharing
July 1, 2025	CA AG	Healthline Media LLC (health & wellness website)	$1,550,000	Shared sensitive health-related tracking data without proper opt-out; failed contracts with third-parties
Sept 30, 2025	CPPA	Tractor Supply Company (retail / rural lifestyle)	$1,350,000	Largest CPPA fine to date; failures include job-applicant rights notice, opt-out preference (GPC) non-compliance, inadequate third-party contracts
Oct 30, 2025	CA AG	Sling TV LLC / Dish Media Sales LLC (streaming service)	$530,000	Opt-out link buried / redirected to cookie pref tool; in-app/TV device opt-out lacking; children's profile ad-targeting issues
Nov 21, 2025	CA AG	Jam City, Inc (mobile gaming-app developer	$1,400,000	Selling/sharing without providing compliant opt-out; sold/sharing of minors' data without obtaining required consent

California – 2025 Data Broker Enforcement

Date	Regulator	Company & Sector	Settlement / Order	Key Alleged Violations & Highlights
Jan 29 2025	CPPA	Key Marketing Advantage, LLC (data broker)	$55,800 fine plus injunctive terms.	Failed to register and pay annual data-broker fee under the California Delete Act for period Feb 1–Nov 5 2024.
Feb 27 2025	CPPA	Background Alert, Inc. (data broker)	Order to shut down operations through 2028 or face $50k penalty	Collected/aggregated billions of public records, created inferences/profiles, sold them — failed registry obligations.
Jul 29 2025	CPPA	Accurate Append, Inc. (data broker)	$55,400 fine + injunctive terms.	Washington-based broker failed to register in California timely; violated Delete Act registration regime.
Dec 3 2025	CPPA	ROR Partners LLC (Nevada-based marketing firm)	$56,600 fine	Nevada-based marketing firm that created and sold detailed consumer profiles, inferences about customers, and customer audience lists used for targeted advertising was a data broker; failed to register.

CCPA Enforcement

- Regulation is not limited to big tech or certain industries
- Broad interpretation of data brokers
- Focus has been on public-facing issues
  - Failure to implement compliant notices
  - Opt-out and rights mechanisms that do not function properly
- Larger fines, and onerous remedial obligations

Other Notable State AG Privacy Fines

State	Date	Company & Sector	Settlement / Action	Key Alleged Violations & Highlights
Texas	July 30 2024	Meta Platforms (social media / biometric data)	US $1.4 billion	Texas AG alleged Meta collected facial geometry/biometric data of Texans without proper consent, under the Texas Capture or Use of Biometric Identifier Act (CUBI).
Texas	May 09 2025	Google LLC (tech / data privacy)	US $1.375 billion	Texas AG alleged Google improperly tracked users' geolocation, incognito browsing, biometric identifiers of Texans, violating state consumer protection laws.
Connecticut	Jul 9 2025	TicketNetwork (ticket-retail)	US $85,000	CT AG alleged failure to comply with the Connecticut Data Privacy Act (effective 2023): inadequate reporting of consumer rights metrics, false reporting of compliance.
Connecticut / New York / California	Nov 6 2025	Illuminate Education, Inc. (ed-tech / student data)	US $5.1 million (total across states)	Joint multi-state settlement for a 2021 breach exposing students' data (including sensitive/medical info) — focused on student data security and inter-state cooperation.

Consortium = More Enforcement

- Consortium of Privacy Regulators formed currently includes CA, CO, CT, DE, IN, NJ, OR, MN and NH. The Consortium's Memorandum of Understanding (MOU) notes shared goals:
  - Sharing expertise and resources across states.
  - Coordinating investigations/enforcement of consumer-privacy laws.
  - Promoting consistent enforcement of the core rights (access, delete, opt-out of sale/sharing) across jurisdictions.
- Why this matters
  - Heightened risk of multistate investigations: regulators are now formally aligned, a lapse in one state may trigger coordinated follow-up in multiple states.
  - Harmonization of enforcement expectations: Although state laws differ in details, the Consortium notes the "fundamental similarities" across laws (rights to delete, access, opt-out), companies may find that enforcement expectations converge even if statutory texts differ

FTC Enforcement in 2025

- ✓ Deceptive enrollment and cancellation practices
- ✓ Deceptive sales and marketing practices
- ✓ Failure to disclose how data used/shared
- ✓ Children / COPPA violations

2025 Litigation Trends

AdTech/Wiretapping Litigation

- Wiretapping theory of liability: Recording or monitoring the contents of a communication without the required consent (laws like ***CIPA in California***)
- Why? Availability of statutory damages up to **$5,000 per violation**
- ~12 states require a form of *two-party consent* for wiretapping / invasion of privacy acts

California	Connecticut	Delaware
Florida	Illinois	Maryland
Massachusetts	Michigan	Montana
Nevada	New Hampshire	Oregon
Pennsylvania	Vermont	Washington

AdTech/Wiretapping Litigation

- **Hundreds of** website-based wiretapping suits filed nationwide, predominantly in California, Pennsylvania, Florida, Massachusetts and Maryland
  - Wiretapping-based suits, increasingly encompassing broader range of torts (invasion of privacy, conversion, trespass to chattels)
- Initially focused on ***session replay*** – then focus on ***chatbots***, website ***pixels*** and ***VPPA***
- Changes in mass arbitration provisions
- Don't overlook HIPAA and the FTC Health Breach Notification Rule

Quiet Hour Laws

- TCPA + FCC Rule: No calls or marketing texts before 8:00 a.m. or after 9:00 p.m. (recipient's local time)
- Lawsuits have increased from under 100, to over 500 filed
- Greatest risk in: Florida, California, Illinois, New York, Pennsylvania, Texas
  - All have mini-TCPA laws that support private suits
  - All have statutory damages (most $500 per violation)

Other Litigation Trends?

- Social media pixels
- Video Privacy Protection Act re: website videos
- Biometric information privacy lawsuits re: employee fingerprinting
- Mobile application data leakage
- Search bars used on websites – sharing of data with 3Ps
- Making available private data for vendor's AI training
- CA "Shine the Light" requests

2026 Privacy Compliance Priorities

Notices

- Proper Privacy Notices, Policies, Transparency
- Website / App Requirements
- California Specific
  - Employee Privacy Notice
  - Job Applicant Privacy Notice

Opt-Out of Sharing & Selling

- All current state privacy laws provide consumers with right to opt-out of selling and sharing:
  - **Selling** – disclosing PI to a third-party for money or other valuable consideration.
  - **Sharing** – sharing PI for targeted advertising purposes. **CA** is the only state that refers to it as "sharing for purposes of cross-context behavioral advertising" (and ***no consideration is required***)
- Big implications for the use of third-party trackers on websites or third-party SDKs/integrations on mobile
- If consent obtained from the consumer to share or sell PI, then it is not considered selling or sharing under these laws

Sharing/Selling Opt-outs – Website Compliance

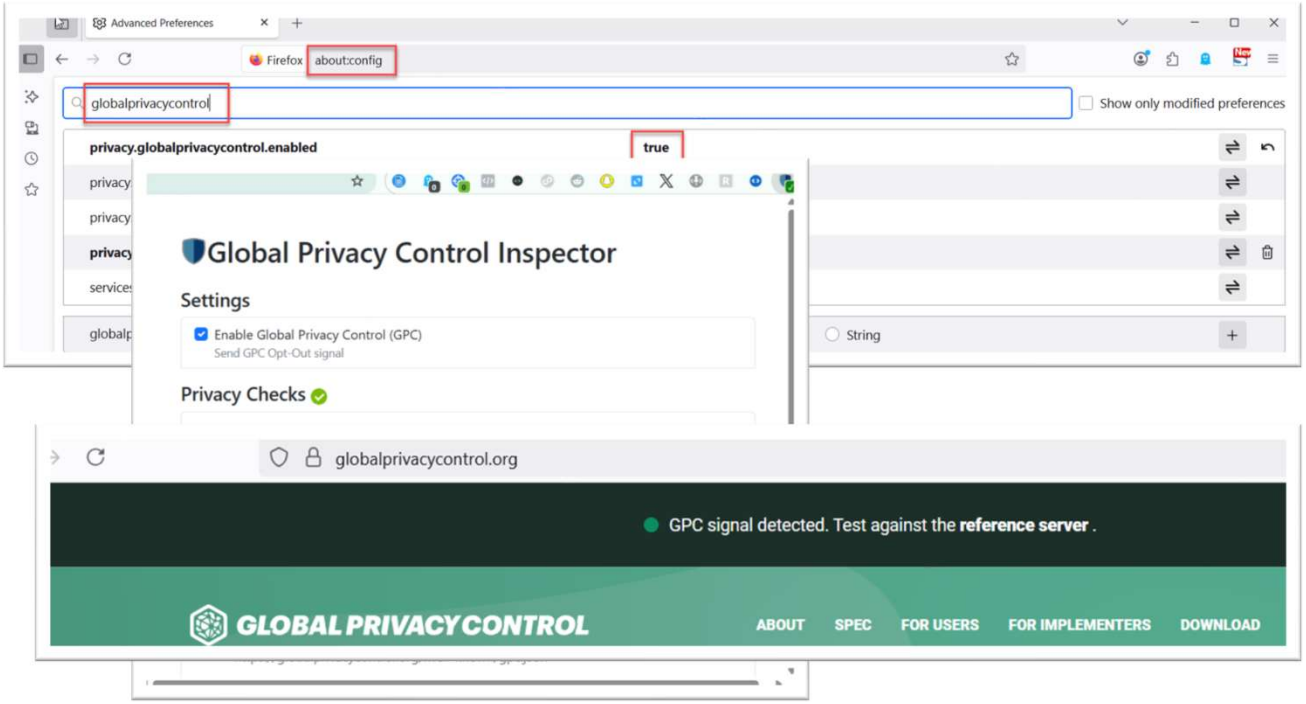
CALIFORNIA

- Websites currently required to honor opt-out preference signal (Global Privacy Control) for CA residents. *See* **https://globalprivacycontrol.org/implementation.**
- Businesses must provide 2 or more designated methods for submitting requests to opt-out.
  - Applies to collection of PI to sell or share over the phone, in a retail store, or elsewhere, thus businesses must provide notice orally or through other means to opt-out.
- Instead of posting the "Do Not Sell or Share My Personal Information" link in the footer, a business may provide the Alternative Opt-out Link in accordance with § 7015 (post "Your Privacy Rights") **OR** process opt-out preference signals in a frictionless manner in accordance with § 7025(f)-(g).

OTHER STATES

How to check if your Website is honoring GPC signals?

- Configure the browser to send GPC signals
  - i.e., Firefox about:config setting
- *OR* use a third-party plug-in tool such as “Global Privacy Control (GPC) Inspector”
- Check if less cookies/trackers are loading with the GPC signal on



Tracking Technology Trends

- Regulators inquiring as to how to apply opt-out preferences to "known consumers," e.g., someone changing from an unauthenticated web visitor to a signed in account holder.
- Technical solutions to push preferences across all environments, from mobile web, to desktop web to mobile app and even offline.
- Enforcement w/r/t consent tool (CMP) misconfigurations:
  - Uncategorized or miscategorized cookies / third parties
  - Pixels or SDKs fire before CMP
  - Tag manager misconfiguration
  - Pixels or SDKs implemented on pages collecting sensitive data
  - Not configured according to each location's privacy requirements

Tracking Technology Action Items

- Evaluate your program's methods for verifying and honoring privacy requests
- Establish or update your contact templates for use with vendors, customers or recipients of "sold" or "shared" PI
- Take action if children's PI may be collected, and be aware of age-appropriate design codes (<18 y.o.)
- Scan websites and mobile apps to understand whether your company may be "selling" or "sharing" PI to any third parties, or else solidify contractual grounds for "service provider" or "processor" relationships
  - If so, understand the different types of opt-outs that are possible or may be required (e.g., GPC in CA, CO or elsewhere)

GT GreenbergTraurig

Other Enforcement Priorities

CONTRACT PROVISIONS & FLOW DOWN

CALIFORNIA – CONTRACTS WITH THIRD PARTIES

DATA PRIVACY IMPACT ASSESSMENTS

GT GreenbergTraurig

Operational Action Items

Take action if children's PI may be collected, and be aware of age-appropriate design codes (<18 y.o.)

Evaluate your program's methods for verifying and honoring privacy requests

Scan websites and mobile apps to understand whether your company may be "selling" or "sharing" PI to any third parties

If so, understand the different types of opt-outs that are possible or may be required (e.g., GPC in CA, CO or elsewhere)

Establish or update your contact templates for use with vendors, customers or recipients of "*sold*" or "*shared*" PI

Risk Mitigation Action Items

- Revise and update your privacy notices
- Review your website, mobile app, and consumer UX for potential "dark patterns"
- Understand all tracking technologies used on your digital properties, and evaluate what events are set, what PI is captured (including sensitive PI, health info, tax/fin.-related, video titles, etc.), and whether proactive notice is provided
- Review all contracts with data processors/services providers and third parties, and make sure contracts have required provisions
- Helping educate senior management on new regulatory emphases on openness re: data breaches and cybersecurity (and possible personal liability if not)
- Explore a 2-3 year roadmap to understand your organization's goals in order to stay current on the regulatory environment and advise on risk


That's All Folks!