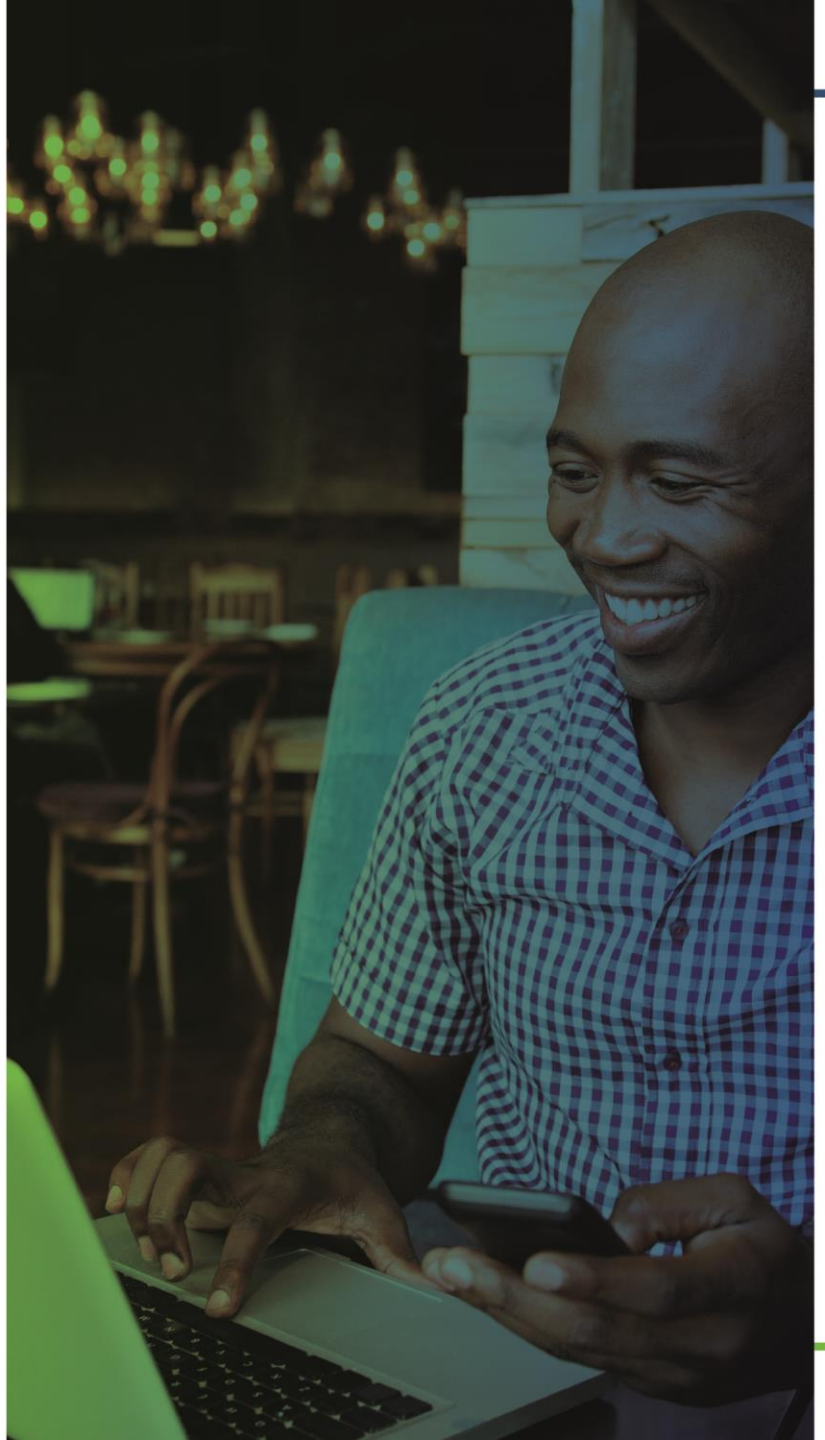

What to expect when you're acquiring data: New rules for data brokers

Tuesday, 18 June 2024
07:00–08:00 PDT
10:00-11:00 EDT
16:00–17:00 CEST

Welcome and Introductions

Panelists

Julia Tama
Co-Chair, Privacy & Data Security
Venable LLP

Rick Gardner
Global Data Protection Officer
LexisNexis Risk Solutions

Cobun Zweifel-Keegan
Managing Director, Washington, D.C.
IAPP

U.S. State Omnibus Privacy Laws

- Requirements for Providing and Acquiring Personal Data:
  - Offer opt-out choices:
    - For “sharing” for targeted advertising
    - For “selling” of personal data, where applicable
  - Consent for processing “sensitive” personal data
    - Narrow exceptions
  - Uniquely in California, prescriptive contracting terms for personal data sold or “shared” (for targeted advertising) by a business to a third party

What is a “data broker”?

- **California:** “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.”
- **Oregon:** “a business entity or part of a business entity that collects and sells or licenses brokered personal data to another person.”
- **Texas:** any business whose “principal source of revenue is derived from the collecting, processing, or transferring of personal data that the entity did not collect directly from the individual. . .”
- **Vermont:** “a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.”

Data Broker Registries

- California, Oregon, Texas, and Vermont require entities that meet the definition of a "data broker" to register with the state.
  - Due to varying definitions, entities required to register in one state may not be required to register in another.

- Each state maintains a public list of registered data brokers, which can provide a way to conduct some preliminary diligence.

- However, not all entities that sell or license data are required to register.
    - Selling personal data collected through a direct consumer relationship does not trigger registration in any state.

New Data Transfer Restrictions

- Protecting Americans' Data from Foreign Adversaries Act:
  - Takes effect on June 23, 2024
  - Prohibits a "data broker" from disclosing "personally identifiable sensitive data" of US individuals to any "foreign adversary" - Russia, Iran, North Korea, China - or any entity "controlled by" a foreign adversary"
  - Federal Trade Commission enforcement with potential per-violation penalties
  - PADFA defines a "data broker" and "personally identifiable sensitive data" in potentially broad ways, e.g., online activities across properties over time.

- PADFA overlaps with prior Executive Order under which U.S. Justice Department will issue transfer restrictions as well.

Other Recent Legal Developments

- New U.S. laws, proposed regulations, and proposed legislation may impact the acquisition of certain types of personal data.
    - DELETE Act: Starting August 1, 2026, all registered “data brokers” in California will be required to process consumer deletion requests made through a centralized deletion mechanism maintained by the California Privacy Protection Agency.
    - Consumer Financial Protection Bureau (“CFPB”): The CFPB is considering new rules that would prohibit the sale of covered data for purposes other than those authorized by the Fair Credit Reporting Act.
    - America Privacy Rights Act: Proposed federal privacy legislation would require “data brokers” to comply with “Do Not Collect” requests made through a centralized request mechanism maintained by the Federal Trade Commission.

Compliance Considerations

- Entities seeking to acquire personal data should be attentive to how the acquired data impacts their compliance. For instance, entities acquiring data should consider:
  - ***Opt-Out Lists.*** When using purchased data for marketing purposes, entities may need to scrub new data against existing opt-out lists.
  - ***Data Minimization***. U.S. state privacy laws generally require entities to collect only personal data that is reasonably necessary and proportionate to achieve the entities' purposes. Entities should avoid purchasing unnecessary data.
  - ***Consumer Rights Requests.*** Purchased data may be subject to consumer rights requests. Entities should consider how purchased data can be integrated into existing processes.
  - ***Notice.*** Privacy notice updates may be necessary after purchasing personal data. Collection from third parties should be disclosed. Also, entities may need to disclose the categories of sources from which they collect personal data.

Regulatory Considerations

- Data type matters – U.S. privacy laws generally focus on consumer data – individuals acting in a personal, family, or household capacity.
  - Business data related to individuals is regulated in California.
  - "Sensitive" data is increasingly subject to state and federal regulation.

- Source matters – certain industries have sector-specific laws like healthcare, financial institutions, etc.
  - Access to such data can be limited to specific permissible purposes as allowed by law.

- Use matters – certain uses trigger the Fair Credit Reporting Act (FCRA); marketing uses may require opt-outs or, under certain conditions, opt-ins.

Responsible Data Acquisition 101

- When acquiring personal information, organizations should carefully consider what data is needed and for what purposes, and vet data providers to meet those needs.

- Considerations for responsible data acquisition include:
  - Types of data acquired
  - Sources of the data
  - Intended uses of the data
  - Data purpose limitations
  - Data minimization principles

- Personal information that was not acquired responsibly can create both legal and reputational risks.

Vetting Sources - Good Practices

- As part of a responsible data acquisition program, an organization should have in place a thorough process for vetting potential data providers.
  - Reputable
  - Due Diligence
  - Questionnaires
  - Security
  - Controls
  - Audits

- Legitimate providers will welcome the vetting.

Buyer Governance – Good Practices

- As part of responsible data provisioning, a data provider should have in place a process for assessing prospective data buyers.
  - Reputable
  - Credentialing
  - Questionnaires
  - Security
  - Controls
  - Audits

- Legitimate buyers will welcome the vetting.

Contracting Considerations

- Reputable data providers should be willing to make representations about the legality of the personal data to be provided.

- Under California Consumer Privacy Act ("CCPA") regulations (11 CCR § 7053), data sales contracts (consumer and business) must include specific provisions, including:
    - Specifying that data providers sell personal information to purchasers for only limited and specified purposes;
    - Requiring purchasers to notify the data provider if purchaser determines it can no longer meet its obligations under the CCPA; and
    - Granting data providers the right, upon notice, to take reasonable and appropriate steps to stop and remediate a purchaser's unauthorized use of personal information.

More Contracting Considerations

- DO NOT be surprised if data providers impose contractual requirements on the data purchaser, such as barring use of supplied data for certain purposes.
    - This protects both parties.

- DO try to make the contract resilient against potential future regulatory and business changes. For example:
    - What will happen if changed laws make it impossible to acquire some or all of the data?
    - What will happen if the acquired data is needed for a new purpose?

Takeaways

- Ensure:
  - Appropriate data governance by both data provider and buyer.
  - Data providers and sources are vetted.
  - Data being purchased is fit for purpose
  - Data provider's privacy notice is updated and clear, especially about individual rights.
  - Data provider offers a "Do Not Sell or Share" or similar opt-out mechanism for consumers, where applicable.
  - Contract meets current legal requirements, including CCPA and any international data acquisition requirements.
  - Contract includes appropriate purpose limitations and use restrictions.
  - "Data broker" registration, where required.

Questions and Answers

Panelists

Julia Tama
Co-Chair, Privacy & Data Security
Venable LLP

Rick Gardner
Global Data Protection Officer
LexisNexis Risk Solutions

Cobun Zweifel-Keegan
Managing Director, Washington, D.C.
IAPP

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/ACtQeZ21pN

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation
please contact: livewebconteam@iapp.org