Successful Data Buying Strategies

Privacy + Security Forum: Spring 2024 Academy

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

Rick Gardner | Global Data Protection Officer, LexisNexis Risk Solutions

Hilary Wandall | Chief Ethics & Compliance Officer, Dun & Bradstreet

VENABLE LLP

Speakers

Julia Tama
Venable LLP

Rick Gardner
LexisNexis Risk Solutions

Hilary Wandall
Dun & Bradstreet

VENABLE LLP

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.

VENABLE LLP

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
  - Vendor Questionnaires
  - Security
  - Controls
  - Audits

- Legitimate providers will welcome the vetting.

VENABLE LLP

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
  - Customer Questionnaires
  - Security
  - Controls
  - Audits

- Legitimate buyers will welcome the vetting.

VENABLE LLP

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.

VENABLE LLP

Data Broker Registries

- In the United States, state “data broker” registrations are required in some instances and can also provide a way to conduct some preliminary diligence.

- California, Oregon, Texas, and Vermont require entities that meet the definition of a “data broker” to register with the state. Each state maintains a public list of registered entities.

- 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.
  - Triggering definitions of personal data vary by state.

- Entities that are required to register in one state may not be required to register in other states.

VENABLE LLP

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.

VENABLE LLP

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?

VENABLE LLP

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.

VENABLE LLP

Additional Considerations

- In addition to compliance considerations, entities acquiring personal data should also consider best practices around the usage of data. For instance, entities acquiring data should consider:

  - ***Data Governance Practices.*** Entities should have a robust data governance process in place to ensure the responsible use of the data.

  - ***Consumer Expectations.*** Consideration should be given to consumer expectations around what sort of data may be acquired and how it will be used given the context of the product or service the consumer is seeking as well as how best to prevent fraud and ensure security.

VENABLE LLP

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.
    - ***Protecting Americans' Data from Foreign Adversaries Act of 2024:*** Starting June 23, 2024, "data brokers" will be prohibited from making available "personally identifiable sensitive data" of U.S. individuals to a "foreign adversary country" or an "entity that is controlled by a foreign adversary."
    - ***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.

International Data Purchasing

- Over 150 countries and territories around the world have similar requirements to the U.S. In some cases, the requirements are more stringent. For example:
  - In European Economic Area markets:
    - Acquisition of data is a processing purpose that must be disclosed in a privacy notice. Like in the U.S. states, existing privacy notices may need to be updated to disclose new sources of data, the legal basis of processing for both the acquisition and subsequent uses, as well as applicable data subject rights, such as the right to object and a retention period.
    - Unless an exception applies, data subjects must be notified directly (e.g., by email, mail, or other direct means) within one month after the data is received.
    - Data about individuals in the personal or household capacities, professional capacities, or as the owner/operator of a sole proprietorship is covered.
    - Cross-border data acquisition may require special data transfer considerations.
  - In the People's Republic of China:
    - Similar notice and scope requirements to Europe. Legal basis of processing is more restrictive (no legitimate interests), so contract language for data acquisitions may need to be structured to address.
    - Data export requirements may be triggered based on a range of factors, including data volume and type.

VENABLE LLP

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.

VENABLE LLP

Moderated Discussion

Julia Tama

https://www.linkedin.com/in/julia-tama-16374547/

Rick Gardner

https://www.linkedin.com/company/lexisnexis-risk-solutions

Hilary Wandall

https://www.linkedin.com/in/hwandall/

VENABLE LLP

© 2024 Venable LLP.
This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

VENABLE LLP