The Ins & Outs of Understanding Data Rights in Advertising Agreements

November 3, 2022

Armand ("A.J.") Zottola
Partner, Venable LLP

Channing Gatewood
Associate, Venable LLP

VENABLE LLP

1

Agenda

- Data and the Advertising Industry
- Intellectual Property Categories for Data
  - Data as a Trade Secret; Copyright Protection; Patent Protection; Intangible Property
- Licensing Data
  - Confirming ownership; Setting use limitations; Determining the license scope
- Privacy Implications of Data Use and Licensing
  - Vendor risks; Privacy laws; Best practices

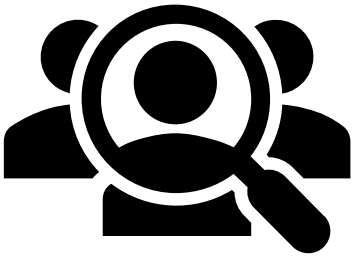
VENABLE LLP

2

Data and the Advertising Industry

Advertisers are increasingly using the personal and confidential information of its customers to generate targeted ads.

- The sale or licensing of customer data is increasingly valuable for advertisers.
- The owner of the data has a valuable asset that should be managed accordingly.
- Data can be sold and licensed according to certain restrictions imposed by the owner.



VENABLE LLP

3

Why?

Data is a business asset.

VENABLE LLP

4

Data as Intellectual Property

VENABLE LLP

5

IP Categories for Data

- Trade secret
- Copyright
- Database patent protection
- Intangible property (non-IP)

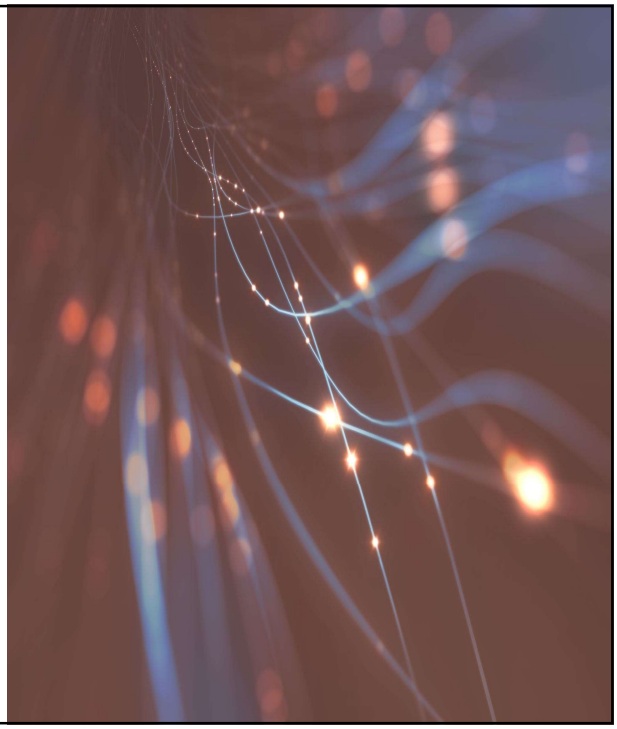
VENABLE LLP

6

Trade Secret Protection

The Uniform Trade Secrets Act (UTSA) defines a "trade secret" as…

- "**information**, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from **not being generally known** to, and **not being readily ascertainable** by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of **efforts** that are reasonable under the circumstances to **maintain its secrecy**."



VENABLE LLP

7

Data as a Trade Secret

A company licensing out information for which it wants to retain trade secret protection must make efforts to maintain the secrecy of the information. This can be evidenced by:

- Limiting the data to "need to know" employees
- Binding such employees by a confidentiality and restricted use obligation
- Using internal systems to prevent improper disclosure of the information

VENABLE LLP

8

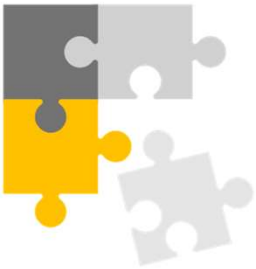
Copyright Protection

- Data complications may also be protectible under copyright law, which grants the owner the right to make copies of, distribute, perform, display, and prepare derivative works of the data.
- Must have a minimal modicum of creativity and be tangible.
- For a corporate author, protection lasts either 95 years from publication or 120 years from creation (whichever occurs first).

VENABLE LLP

9

Data as a Copyright Asset



- Copyright protects data *compilations*, not underlying data itself.
- Standard for "minimal modicum of creativity" is low. Most compilations will satisfy the requirement so long as the company played a role in selecting, organizing, and arranging the data.

VENABLE LLP

10

Patent Protection

- Generally, a database will not qualify for patent protection.
- Database-related inventions may be protectible, however, if standards for patentability are met:
  - Novelty
  - Non-obviousness

VENABLE LLP

11

Intangible Property

- Some U.S. case law treats data as if it were any other property such that traditional tort principles and claims will apply:
- **Trespass to chattels** – may include use of a computer system without authorization
- **Conversion** – may include unauthorized taking of computer/website information

VENABLE LLP

12

Data License Agreements

VENABLE LLP

13

Data Licensing Overview

Third-party use of data requires a license from the data owner (or sublicense)

Third parties may want to use the data to provide services to their own customers or to enhance their own data collections, among other reasons.

VENABLE LLP

14

Data Ownership

- Licensor of the data should ensure that the contract acknowledges its ownership of the data rights.
- Should also acknowledge the resources used in gathering, assembling, and compiling the data.
- Narrow definition of the licensed data (scope).

VENABLE LLP

15

Data Use

Depending on the type of protection the data set qualifies for, the licensor should consider what rights it can grant to third parties.

Agreement can also detail the limitations on data use (e.g., in what context the data may be used).

Licensee and licensor will likely have different wants. The license terms should specify.

VENABLE LLP

16

License Scope and Restrictions

License scope and restrictions detail how the licensee may use the data:

- May the licensee sublicense the data?
- Create derivative works?
- Use the data for particular purposes?
- Use the data outside of X state, region, or country?
- Permit other individuals ("authorized users") to use the data?

VENABLE LLP

17

Original vs. Derived Data

Original Data

- The data that is licensed via the terms of the license agreement.
- The definition may vary depending on what type of IP analysis is done (e.g., copyright vs. trade secret).

Derived Data

- Generated or derived from the licensed data.
- May be generated by processing the licensed data to create new data or monitoring the licensee's use of a provider's service (usage data).
- Ownership is often enumerated in and protected by the contract.

VENABLE LLP

18

Original vs. Derived Data (cont'd)

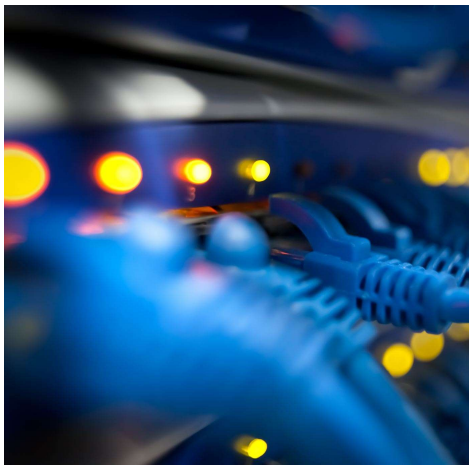
- The data recipient will be considering if the contractual terms re: derived data meet its needs.
- Ownership of data secures additional benefits (e.g., enforcing rights against third parties, remedies) as compared to solely contractual rights.

VENABLE LLP

19

Data Delivery

- License terms should detail delivery of the data:
  - **How** will it be delivered?
  - **When**?
  - In what **format**?
  - Via which technology **platforms**?
  - How **frequently**?



VENABLE LLP

20

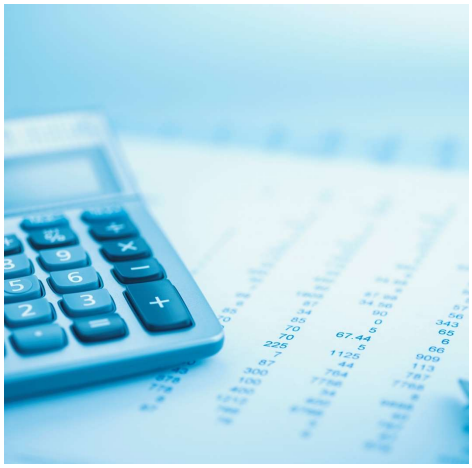
Privacy Implications

VENABLE LLP

21

Data Risks When Engaging Vendors

- Engaging third parties to provide data services can be financially beneficial to a company (e.g., by removing the company's need to finance and facilitate data collection itself).
- Also introduces greater risk.



VENABLE LLP

22

Data and "Personal Information"

- "Personal information" is often subject to regulation by various policies worldwide due to concerns surrounding use and disclosure of that information.
  - E.g., CCPA definition is broad (similar to that in GDPR).
  - Federal definitions also vary (since there are multiple federal privacy laws, e.g., COPPA, HIPAA).
- "Personal information" = information that could "reasonably be used to identify a data subject including, for example, name, age, address, email address, photograph, SSN, or a combination of these."
- When engaging in an agreement, a company should (1) ensure compliance with the applicable data protection laws, and (2) ensure that it, and the company with which it engages, maintain a high standard of security of any personal information.

VENABLE LLP

23

Privacy Laws

COPPA (Children's Online Privacy Protection Act)	Graham-Leach-Bliley (GLC) Act	Health Insurance Portability and Accountability Act of 1996
General Data Protection Regulation (GDPR)	Fair Credit Reporting Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act
Driver's Privacy Protection Act of 1994 (DPPA)	Federal Trade Commission Act (Section 5)	California Consumer Privacy Act (CCPA)
	Other U.S. federal and state laws	

VENABLE LLP

24

Ensuring Compliance with Data Protection Laws

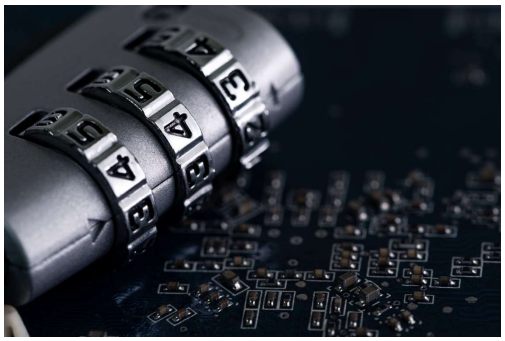
- Complete a security risk assessment.
- Determine what personal information *your* company collects and from whom. Different laws will apply, depending on this finding.
- Examine the means that your organization uses to collect personal information (e.g., online forms, purchasing from other entities, publicly available sources, etc.).
- Examine your organization's use of the personal information (e.g., for business development, for licensing out to other organizations, etc.).
- Examine your organization's storage and destruction practices for personal information (where, what steps, who has access, systems in place?).

VENABLE LLP

25

Setting Privacy Standards for Vendors

- Checklist for vendor engagement:
  - Perform due diligence on a vendor before any engagement.
  - Develop standard contract terms that support the organization's privacy and security programs.
  - Engage in regular oversight of the vendor and ensure that contract terms are enforced.
  - Incorporate your company's other policies into its terms that apply to the vendor (e.g., information security policies, privacy policies).



VENABLE LLP

26

Implementing a Privacy Policy

- A privacy policy is a policy statement for a company's website and its visitors.
- To be enforceable, the policy should be conspicuous on the site, and the user should be prompted to consent to it.
- There are applicable laws and standards if the policy applies to children (under COPPA).

VENABLE LLP

27

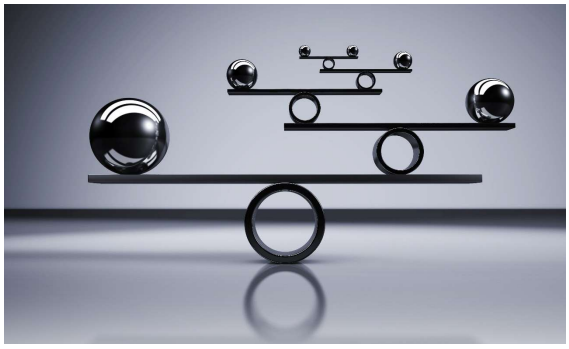
Managing Privacy Risks

Sources of Risk at Work

- Work devices (or employee personal devices)
- Employee emails
- Physical files

Insurance for Data Privacy

- Insurance policies re: cyber liability, cyber risk, etc., are designed to cover losses to an insured, including losses that have resulted from damages caused by a computer or network-based incident.



VENABLE LLP

28

Personal Information and Advertising

- Personal information, as a type of "data," is often used to inform targeted advertising.
- "Advertising identifiers" technology enables advertisers to "tag" and track a consumer's online activities to provide more personalized ads and services.
- FTC suggests that entities with consumer-facing relationships be transparent about their data collection and use practices and maintain reasonable security.
- In contracts with customers, this can appear in the form of transparency in the agreement about how the customer's data is used.

VENABLE LLP

29

Best Privacy Practices When Engaging a New Vendor

- Perform vendor due diligence before any engagement re: data.
- Develop standard contract terms that uphold the company's privacy and information security standards.
- Regularly audit vendors and ensure that the contract is enforced in the event of breach (this can be enumerated in the contract).

VENABLE LLP

30

VENABLE LLP

31