Strafford

Presenting a live 90-minute webinar with interactive Q&A

Big Data Use and Licensing Agreements: Key Contractual Provisions

TUESDAY, JULY 31, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Melissa Krasnow, Partner, **VLP Law Group**, Minneapolis

Michael R. Overly, Partner, **Foley & Lardner**, Los Angeles

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-961-8499** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

Big Data Use and Licensing Agreements

Michael Overly, Esq., CISA, CISSP, COP, CIPP, ISSMP, CRISC
Melissa Krasnow, Esq., CIPP/US

Overview

- What is Big Data?
- Components of Big Data
- Big Data Ecosystem
- How Industry Uses Big Data
- What is Personal Information?
- Anonymization and De-identification
- Privacy and Data Security Promises
- Privacy Policy Disclosure Requirements

Licensing/Contractual Issues

- Do We Own What We Think We Own?
- Getting the Rights
- Example Language
- The Devil is in Aggregating
- Information Security
- Breach Notification and Data Security

Licensing/Contractual Issues

- Licensing
- Warranties
- Indemnities
- Potential Indemnities
- Confidentiality
- Audit Rights
- Limitation of Liability
- Term and Termination

Overview

What is Big Data?

Big Data consists of extensive datasets—primarily in the characteristics of volume, variety, velocity, and/or variability—that require a scalable architecture for efficient storage, manipulation, and analysis.

Source: https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1r1.pdf

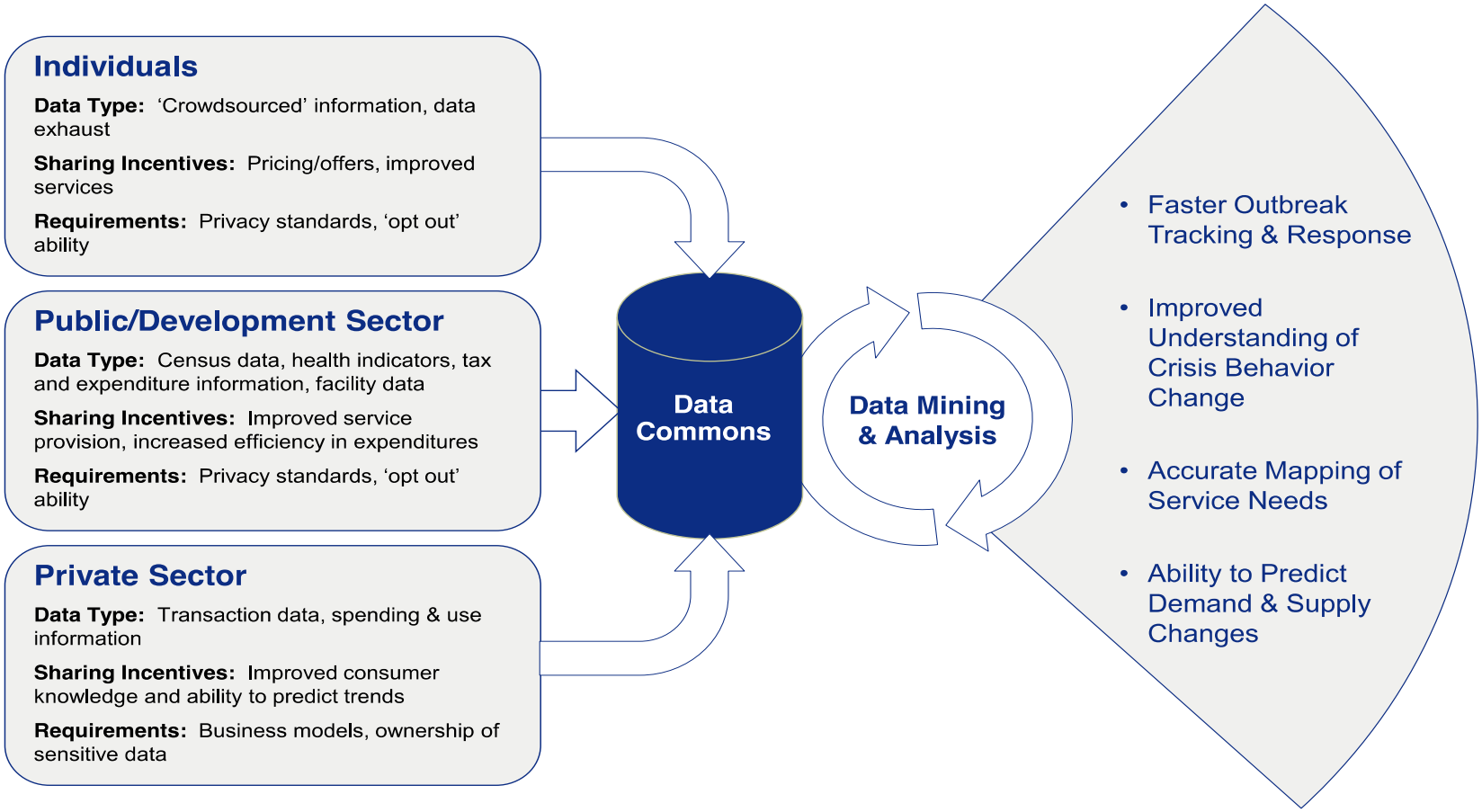
What is Big Data?

- Creation, storage, processing and analysis of datasets that exceed capabilities of standard database software tools
- Includes transactional data, location-based data, health information, financial information, etc.
- Uses:
  - Mined to increase efficiency, identify trends, predict outcomes
  - Leveraged to drive behavior, develop sophisticated decision-making algorithms, customize products/user experiences, create/improve products
- US Govt. investing hundreds of millions in research programs for Big Data computing

Components of Big Data

- Collection
- Distribution
- Processing
  - Infrastructure (hardware)
  - Analytics (software, SME expertise)
  - Storage (data centers, incl. "super data centers")
- Implementation
  - Strategy for collection/analysis
  - Leveraging Big Data

Big Data Ecosystem



How Industry Uses Big Data

Big Data application domains include healthcare, drug discovery, insurance, finance, retail, and many others from both the private and public sectors. Among the scenarios within these application domains are health exchanges, clinical trials, mergers and acquisitions, device telemetry, targeted marketing, and international anti-piracy. Security technology domains include identity, authorization, audit, network and device security, and federation across trust boundaries…. Source: https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-4r1.pdf

How Industry Uses Big Data

- **Xerox** used Big Data to create algorithm that makes hiring decisions for its 48,700 call-center jobs
- **Google** uses Big Data to power is search engine and advertising business
- **Walmart** and **Target** use Big Data to tailor inventory at stores and customize advertising
- **UPS** uses Big Data to optimize shipping routes

How Industry Uses Big Data

- **Law firms** use Big Data to set rates and predict costs
- **NGOs** use Big Data to predict disease outbreaks
- **Politicians** use Big Data to predict voter turnout, voting trends

What is Personal Information?

The definition of personal information continues to expand.

Personal data means any information that relates to an identified or identifiable living individual. Article 4(1) of the EU General Data Protection Regulation.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN%5d

What is Personal Information?

Personal information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. California Consumer Privacy Act of 2018.

Source: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Anonymization and De-identification

If personal information is involved, certain laws can apply unless such information is anonymized or de-identified.

Increasingly, laws are defining anonymization and de-identification.

Anonymization and De-identification

[Anonymous information means]….information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Recital (26) of the EU General Data Protection Regulation.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN%5d

Anonymization and De-identification

Deidentified means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

Anonymization and De-identification

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information. California Consumer Privacy Act of 2018.

Source: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Anonymization and De-identification

When a company states that it maintains de-identified or anonymous data, the [FTC] has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.

Anonymization and De-identification

This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

Source: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Anonymization and De-identification

There are no widely accepted standards for testing the effectiveness of a de-identification process or gauging the utility lost as a result of de-identification. Given the growing interest in de-identification, there is a clear need for standards and assessment techniques that can measurably address the breadth of data and risks….

Source:
https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

Privacy and Data Security Promises

Section 5 of the Federal Trade Commission Act….prohibits unfair or deceptive acts or practices….Companies engaging in big data analytics should consider whether they are violating any material promises to consumers—whether that promise is to refrain from sharing data with third parties, to provide consumers with choices about sharing, or to safeguard consumers' personal information—or whether they have failed to disclose material information to consumers.

Privacy and Data Security Promises

In addition, companies that maintain big data on consumers should take care to reasonably secure consumers' data. Further, at a minimum, companies must not sell their big data analytics products to customers if they know or have reason to know that those customers will use the products for fraudulent or discriminatory purposes.

Source: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

Privacy Policy Disclosure Requirements

California, Delaware and Nevada privacy policy law disclosure requirements include:

Categories of personal information collected and categories of third parties with whom such personal information may be shared

See: https://www.irmi.com/articles/expert-commentary/nevada-passes-new-privacy-notice-law

Privacy Policy Disclosure Requirements

EU General Data Protection Regulation privacy notice disclosure requirements include:

Categories of personal data, source from which personal data originate, and if applicable, whether it came from publicly accessible sources, and recipients or categories of recipients of the personal data, if any. Articles 13 and 14 of the EU General Data Protection Regulation.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN%5d

Privacy Policy Disclosure Requirements

California Consumer Privacy Act of 2018 privacy policy disclosure requirements include:

A list of the categories of personal information that the business has collected about consumers, sold about consumers and disclosed about consumers for a business purpose in the preceding 12 months. California Consumer Privacy Act of 2018.

Source: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Licensing/Contractual Issues

Do We Own What We Think We Own?

- Step One: Clearing rights
- Right to collect
- Right to distribute
- All elements of the database

Do We Own What We Think We Own?

- What type of data is in play?
  - Personal
  - Business
  - Unclear

Getting the Rights

- Obtaining rights from your own customers
  - Vendor oriented provision
  - Customer oriented provision
- Separately license data from third party providers (data licensors)

Example Language (Vendor)

Company grants Provider a non-exclusive, perpetual, irrevocable, fully-paid-up, royalty free license to use, copy, distribute, and otherwise exploit statistical and other aggregated data derived from Company's and its End Users' use of Services (the "**Aggregated Data**") for Provider's business purposes, including the provision of products and services to Provider's customers; provided the Aggregated Data is combined with similar data from Provider's other customers and does not include (directly or by inference) any information identifying Company or any identifiable individual. The Aggregated Data will not be considered Company's Confidential Information.

Example Language (Customer)

Customer hereby grants Vendor a non-exclusive, "as-is," perpetual, royalty-free license to use Aggregated Data (defined below) for the purpose of improving its products and otherwise in connection with its business.

Example Language (Customer)

The foregoing shall not be construed as a representation or warranty by Customer that it has the rights, if any, to grant such license or to authorize such use. Vendor acknowledges and agrees that the Aggregated Data is provided by Customer as-is, without warranties of any kind. Customer hereby disclaims all warranties, express and implied, including the implied warranties of merchantability, fitness for a particular purpose, title/non-infringement, and quality of information with regard to the Aggregated Data.

Example Language (Customer)

"Aggregated Data" refers to Customer Data that (i) is combined with other similar data of other Vendor customers and de-identified in such a way as to comply with any applicable laws or regulations governing de-identification of such information; (ii) does not directly or by inference contain any information identifying or capable of being re-identified to Customer or any identifiable entity or individual; (iii) does not contain any Customer Confidential Information; and (iv) does not contain any Customer intellectual property.

The Devil is in Aggregating

- De-identification is **not** aggregation
- Know the standards, particularly those imposed by law (e.g., HIPAA).
- Entity v. individual de-identification
- Potential to re-identify

Information Security

- General obligations
- Legal/regulatory obligations
- Customer expectations
- Licensee expectations
- Important sales tool

Breach Notification and Data Security

50 states, plus the District of Columbia, Guam, Puerto Rico and Virgin Islands, have breach notification laws that require notification of a breach to affected individuals.

Certain states also have laws addressing security procedures, some of which may require a written information security program and/or third party contractual provisions.

Breach Notification and Data Security

The EU General Data Protection Regulation has breach notification and data security requirements.

The California Consumer Privacy Act of 2018 addresses certain types of breaches and data security.

Licensing

- Why do we need a license?
- Licensee
- Other authorized users
- Sublicensing
- Scope of license
- Combinations with other databases

Licensing

- Salting
- Exclusivity – Customer side
- Exclusivity – Vendor side
  - Example of the financial services company

Warranties

- Customer warranties?
  - Authority
- Vendor warranties
  - Rights (generally not; public sources)
  - Accuracy (generally not; public sources)

Indemnities

- What is an indemnity? Think third party claims
- Compare warranties
- Common law right to seek indemnity Why is a contractual indemnity so important?

Indemnities

- Interplay with limitation of liability
  - Exclude all
  - Selective exclusion
  - If cap, exclude attorney's fees and costs
- Danger of capping an indemnity obligation
  - Control of defense and settlement
  - Opt out

Indemnities

- What is the vendor's financial status?
- Is an indemnity even worthwhile?
- Guarantee from related entity
- Indemnity bond

Indemnities

- Key terms:
  - hold harmless, defend, and indemnify;
  - all types of damages and costs, including attorney's fees and expert costs
  - fines and sanctions
  - beware "final" awards only
- Who is indemnified?

Potential Indemnities

- Vendor side
  - Failure to aggregated/de-identify properly
  - Exploitation of any kind
- Customer
  - Rights to furnish data

Confidentiality

- Standard protections
- Trade secrets?
  - Beware fixed confidentiality periods
- Injunctive relief (consider adding breach of license as well)
- Relationship to limitation of liability

Audit Rights (Vendor Perspective)

- Essential to protecting rights
- Huge potential revenue stream
- Cost of audit
  - Cost shifting
- True up
- Contingent fee auditors
- Penalties

Audit Rights (Licensee Perspective)

- Huge potential revenue stream
- Cost of audit
  - Cost shifting
- True up
- Contingent fee auditors
- Alternatives: Confirmation of use.

Limitation of Liability

- Two parts to almost every limitation of liability:
  - Direct Damages
  - Consequential Damages
- Exclusions
  - Indemnities
  - Violation of license

Term and Termination

- What is the term?
- Is there renewal of the term?
- Which party can terminate and on what basis?
- What are the termination events (e.g., convenience)?
- Can termination occur only after a specific time period?
- How long is the notice period for termination and is there an opportunity for cure?
- Effect of termination and survival

Questions?

Michael R. Overly, Esq.
CISA, CISSP, COP, CIPP, ISSMP, CRISC
Partner, Foley & Lardner LLP
(213) 972-4533
moverly@foley.com

Melissa Krasnow, Esq.
CIPP/US
Partner, VLP Law Group LLP
(312) 350-1082
mkrasnow@vlplawgroup.com

Resources

A Brief Overview of the California Consumer Privacy Act of 2018

https://www.vlplawgroup.com/blog/brief-overview-california-consumer-privacy-act-2018/

https://www.vlplawgroup.com/attorneys/melissa-krasnow/

https://www.irmi.com/biographies/melissa-Krasnow