Privacy Update

GDPR, California, and the Future of Privacy

LECLAIRRYAN

Legal Strategies. Business Solutions.

Peter Day & Matthew Moisan

Privacy Update

- Introduction
- Overview of Changes in Europe
- Overview of Changes in California
- Overview of Changes in the ROTW

*

Privacy Update | Introduction

- Speakers
  - Peter Day is a partner in LeClairRyan's San Francisco office. Peter focuses on privacy, data security, compliance, and white collar crime
  - Matthew Moisan is a partner in LeClairRyan's New York office. Matthew represents companies in all stages of development, with a particular focus on representing emerging growth companies

*

Privacy Update | Introduction

- 2018 witnessed significant changes in the privacy and information security landscape
- Several themes emerged:
  - The need to understand data flows, and build business processes that can capture and control data
  - Cross-border compliance issues are increasing
  - Increased regulatory scrutiny
  - Incident response remains challenging

*

Privacy Update | *European Union*

Overview of a few key provisions of the GDPR

Fines

Applicable to both controllers and processors, fines can be significant with the maximum penalty being up to € 20 million or 4% of global turnover.

Jurisdiction

GDPR significantly expands scope of EU data protection law to include processing by entities entirely outside the EU.

Consent

Must be explicitly provided and based on clear, easily understood disclosures; consent must also be easily withdrawn by data subjects.

Access & Portability

Consumers must be given access to personal data and the right to take their data to another controller or processor, free of charge, in electronic form.

Breach Notification

Controllers and processors must give notice to competent authority within 72 hours; breaches include violation of data subject rights.

Privacy by Design

Data protection must be factored into the engineering and design of any system collecting, processing, or sharing personal data.

Erasure

Consumers can petition to have controllers or processors erase personal data, cease sharing the data, including use by downstream processors.

Data Protection Officers

In certain cases, entities may be required to appoint a data protection officer responsible for ensuring compliance with the GDPR.

*

Privacy Update | *European Union*

GDPR | Fines

- Article 83 of the GDPR has two species of administrative fines:
  - *Section 3 fines* → applicable to certain processing obligations, max out at € 10 million or 2 % of global turnover
  - *Section 5 fines* → applicable to violations of data subject rights, max out € 20 million or 4% of global turnover
- Important to note fines are maximal—Data Protection Authorities must weigh several factors before imposing fines; these factors are principally aimed at determining whether controller or processor respects data subject rights

*

Privacy Update | *European Union*

GDPR | Jurisdiction

- Article 2 set out the purpose of the GDPR, and makes clear it applies broadly to processing of personal data by “automated means”

- Article 3 sets out three basis for GDPR jurisdiction:

    1. *Art. 3(1)* → Controllers or Processors established in the EU
    2. *Art. 3(2)* → Controllers or Processors not established in the EU

- For Controllers or Processors not established in the EU, the GDPR applies if:

    A. *Art. 3(2)(a)* → Offering goods and services in the Union
    B. *Art. 3(2)(b)* → “Monitoring” data subjecting behavior

*

Privacy Update | *European Union*

GDPR | Consent

- Under Article 4(11) of the GDPR, “consent” is only effective where it is a “freely given, specific, informed, and unambiguous indication of the data subject’s wishes.” Such an indication must signified through a “statement or clear affirmation.”

- Article 7 expands on this, and requires:

    1. Controllers or processors to make requests for consent very clear, in “plain language” and in a fashion that is separate from other disclosures, specifically questioning where contracts require sharing personal data for performance consent is considered to be freely given

    1. Free withdrawal of consent

*

Privacy Update | *European Union*

GDPR | Access & Portability

- Article 15 of the GDPR grants data subjects two rights:

    1. *Art. 15(1)* → gives data subjects the right to "obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed."

    1. *Article 15(3)* → requires controller to "provide a copy of the personal data undergoing processing [i.e. that which was identified in Art. 15(1)] . . . in a commonly used electronic form."

*

Privacy Update | *European Union*

GDPR | Breach Notification

- The GDPR introduces breach notification requirements in cases involving a "personal data breach." Art. 4(11) defines personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised [sic] disclosure of, or access to, personal data transmitted, stored or otherwise processed."

- Two key forms of notice:

    1. *Art. 33* → requires controllers to notify supervisory authorities within 72 hours of a personal data breach

    1. *Art. 34* → requires controllers to notify data subjects if the data breach "is likely to result in a high risk to the rights and freedoms of natural persons . . .without undue delay."

*

Privacy Update | *European Union*

GDPR | Privacy by Design

- The GDPR enshrines privacy by design concepts. As Article 25 requires controllers to "implement appropriate technical and organisational [sic] measures" to ensure that systems processing personal data are designed to "meet the requirements of the [GDPR] and protect the rights of data subjects."

- Recital 78 adds that controllers embrace principles of data protection by "design and . . . by default." Recital 78 also provides several examples:

    1. Data minimization
    2. Enhanced data subject control
    3. Transparency

*

Privacy Update | *European Union*

GDPR | Erasure

- Article 17 of the GDPR grants data subjects the right “to obtain from the controller the erasure of personal data concerning him or her without undue delay . . . .”

- The scope of this right is fleshed out in Recital 65 of the GDPR, which provides that data subjects shall have the right to erasure where the data is no longer necessary to the original purpose justifying collection or where:

    - Consent has been withdrawn
    - Processing is objected to
    - Processing fails to comply with the GDPR

*

Privacy Update | *European Union*

GDPR | Data Protection Officers

- Although not required in all cases, appointment of a Data Protection Officer is among the key features of the GDPR.
- Article 37 requires appointment of a Data Protection Officer where:
  1. The processing is done by a public authority
  2. The processing requires “regular and systematic” monitoring of data subjects
  3. The processing involves access to sensitive personal data (as defined in Article 9) or criminal conviction data
- A Data Protection Officer must have “expert knowledge” in data protection law.
- Data Protection Officer is responsible for: (i) advising a controller or processor of obligations under the GDPR; (ii) monitoring compliance and training staff; (iii) advising on data privacy impact assessments; (iv) cooperating with supervisory authorities; and (v) acting as a contact for supervisory authorities.

*

Privacy Update | *European Union*

- Since taking effect in May 2018, we have seen:
  - A September 2018 UK enforcement action against Canadian data analytics firm AggregateIQ
  - July 2018 securities class action against Facebook related to GDPR charges
  - September 2018 securities class against Nielsen related to GDPR compliance charges

*

Privacy Update | *European Union*

- Thoughts and recommendations:
  - Carefully consider expsoure—the GDPR is much broader than ePrivacy Directive
  - Begin data mapping—companies and institutions should strongly consider broading insight into data
  - Treat GDPR as a cost, and one that may substantially increase
  - Understand that it is still in its infancy—much remains to be seen about how it will be enforced

Privacy Update | *European Union*

- There is more than just GDPR coming out of Europe
  - *ePrivacy Regulation* → a proposed regulation governing electronic communication that would repeal and expand an existing Directive such that any business providing any form of electronic communication could be scope. Fines are similar to those under GDPR.
  - *NIS Directive* → the Directive on Security of Network and Information Systems went into effect on August 2016, and gave member states 21 months (i.e. June 2018) that set out minimum information security standards for certain critical businesses

*

Privacy Update | *California*

The California Consumer Protection Act

(effective Jan. 1, 2020)

Right to Know

Both a general and specific policy that details what types of personal information are being collected, and what it is being used for.

Right to Opt Out

Allows consumers to opt-out from businesses selling personal information to third parties.

Right of Erasure

With some exceptions, the CCPA permits California consumers to demand deletion of personal data

Right to Equal Service

Consumers who exercise privacy rights must be treated the same as consumers who do exercise their rights.

Right to Access

Consumers have the right to access a copy of the personal data a business has collected

*

Privacy Update | *California*

CCPA | Jurisdiction

- The Act applies to “personal information” which it very broadly defines as “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.”

- As currently drafted, the Act applies to “Covered Businesses”-- organizations that conduct business in California and meets one of the following three conditions:

    1. *Section 1798.140(c)(1)(A)* → has annual gross revenues in excess of $25 million
    2. *Section 1798.140(c)(1)(B)* → alone or in combination collects personal information on 50,000 or more California consumers annually
    3. *Section 1798.140(c)(1)(C)* → derives 50 percent or more of its annual revenue from selling consumers’ personal information

*

Privacy Update | *California*

CCPA | Right to Know

- At or before the time of collection, Covered Businesses must disclose what Personal Information it will collect, and:

    1. The purpose for which such information will be used
    2. The categories of personal information actually collected over the preceding 12 month period; and
    3. The categories of personal information sold or disclosed for business purposes in the preceding 12 month period

- If a Covered Business receives a verifiable consumer request, the Business must also disclose: (1) the categories of the requesting consumer's personal information were actually collected and/or (2) sold during the prior 12 month period.

*

Privacy Update | *California*

CCPA | Right to Opt Out

- The Act permits consumers to opt out of the sale of their Personal Information
- Covered business must provide a “clear and conspicuous link” entitled “Do Not Sell My Personal Information.” This link must be posted to a Covered Business national or California specific website
- Absent and affirmative opt out, and assuming the consumer is not a minor, the consumer’s personal information may be shared

*

Privacy Update | *California*

CCPA | Right to Erasure

The Act allows consumers to request deletion of their Personal Information from business servers and service providers. Covered Businesses are obligated to honor deletion requests unless it is necessary to save Personal Information to:

- Complete a transaction involving the Personal Information
- Maintain cybersecurity
- Debug or repair errors
- Exercise legally provided rights
- Comply with California law
- Engage in scientific research
- Comply with legal obligations
- Perform internal processing in line with purpose of collection

*

Privacy Update | *California*

CCPA | Right to Equal Treatment

- The Act grants a right to equal service. This right prohibits discrimination against consumers who exercise their rights under the Act
- Covered Business are generally prohibited from:
    - Charging higher rates (including discounts or benefits)
    - Providing a different level of service
- However the Act recognizes that were the level of service is contingent on the personal information supplied, Covered Businesses may offer a different level of service
- Additionally, Covered Business may offer financial inducements to consumers to provide Personal Information

*

Privacy Update | *California*

CCPA | Right to Access

- The Act also gives consumers the right to access a copy of “the specific pieces of personal information that [a business] has collected about that consumer.”

- The personal information can be delivered either by mail or by electronic service.

*

Privacy Update | *California*

- While the aforementioned rights form the core of the CCPA, there are several other significant provisions:

  - **Section 1798.155—Civil Penalties**—Any business failing to cure a violation of the CCPA upon 30 days notice is subject to a $2,500 fine. Intentional violations are subject to civil penalties up to $7,500 per violation, in addition to the $2,500 fine for failing to cure the violation.
  - **Section 1798.150—Private Right of Action**—Any consumer whose nonencrypted or nonredacted Personal Information is subject to unauthorized access or acquisition "as a result of the business' violation of the duty to implement and maintain reasonable security procedures" may seek to recover statutory damages of between $100 and $700 per violation.
  - **Section 1798.120—Minors**—Act generally prohibits sale of personal information about a child if covered entity knows the child is under the age of 16. Business must obtain consent from child if between 13 and 16, and parent opt-in if the child is under 13.

*

Privacy Update | *California*

- The CCPA represents a significant expansion of domestic privacy law, and has been compared to the GDPR.
- We disagree with this contention.

  - The GDPR and CCPA share some general features
  - However, the CCPA

    - Is not an omnibus law, separate statutes cover breach notification and supervision
    - The act requires companies to focus on specific types of data in a more mechanistic fashion than the GDPR
    - The opt-in and opt-out functions of data sales could make compliance with both laws very challenging for multi-national companies

- Important to note that the CCPA may and likely will change before going into effect in January 1, 2020

*

Privacy Update | *California*

- Regardless of whether the CCPA changes, we recommend taking several compliance steps:

  - Determining applicability
  - Planning for updates to consumer facing privacy notices
  - Planning for business processes suitable to handle a large volume of consumer privacy related requests
  - Planning for data mapping and data segregation
  - Consider employee training programs

*

Privacy Update | *Rest of the World*

*

Privacy Update | *Rest of the World*

- **Russia**—Data Localization Law
- **China**—Cyber Security Law of 2017
- **India**—Draft on Data Privacy Law
- **Canada**—Breach Reporting Guidance
- **Japan**—Protection of Personal Information

*

Thank you

Peter Day
Peter.Day@leclairryan.com
415.913.4898

Matthew Moisan
Matthew.Moisan@leclairryan.com

CALIFORNIA | CONNECTICUT | DELAWARE | FLORIDA | ILLINOIS | MARYLAND | MASSACHUSETTS | MICHIGAN
NEW JERSEY | NEW YORK | PENNSYLVANIA | RHODE ISLAND | TEXAS | VIRGINIA | WASHINGTON, D.C.
WWW.LECLAIRRYAN.COM

With 300+ attorneys in a full range of practices, LeClairRyan is an entrepreneurial firm providing business counsel and client representation in matters of corporate law and litigation.

Disclaimer

- This slide show provides general information and is not legal advice and should not be used or taken as legal advice for specific situations. You should consult legal counsel before taking any action or making any decisions concerning the matters in this show. This communication does not create an attorney-client relationship between LeClairRyan PLLC("LeClairRyan"), and the recipient.
-

As used herein, "LeClairRyan" refers to LeClairRyan PLLC, a Virginia professional limited liability company; LeClairRyan, LLP, a Delaware limited liability partnership; and LeClairRyan, A Professional Corporation, a Michigan domestic professional service corporation. Joseph P. Paranac, Jr. is the attorney in charge of LeClairRyan's Newark, NJ office.