Morgan Lewis

TECHNOLOGY MAY-RATHON

Big Data, Privacy and Competition Law: The Transatlantic Debate

PRESENTERS: Reece Hirsch, Christina Renner, Brian Rocca

May 10, 2019

BIG DATA, PRIVACY AND COMPETITION LAW: THE TRANSATLANTIC DEBATE

W. REECE HIRSCH

SAN FRANCISCO

CO-LEADER, PRIVACY AND CYBERSECURITY PRACTICE

CHRISTINA RENNER

BRUSSELS

ANTITRUST PRACTICE GROUP

BRIAN C. ROCCA

SAN FRANCISCO

LEADER, WEST COAST ANTITRUST PRACTICE

Agenda

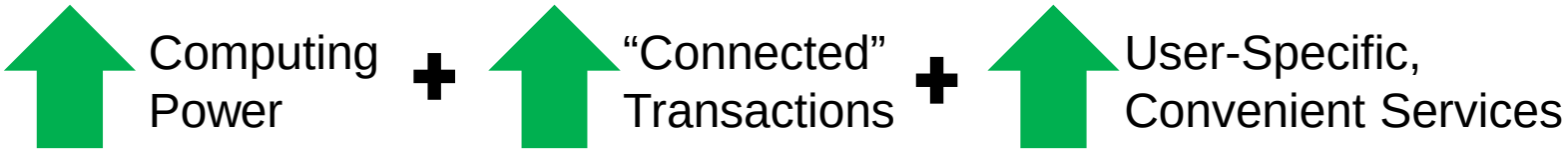
- The Context
- The Competition Law Debate
- The Privacy Law Solution?

SECTION 01

THE CONTEXT

The Context

- Data is easier than ever to collect, analyze and store, so more and more companies are using it to help provide goods and services.



The Context

- Data is easier than ever to collect, analyze and store, so more and more companies are using it to help provide goods and services.

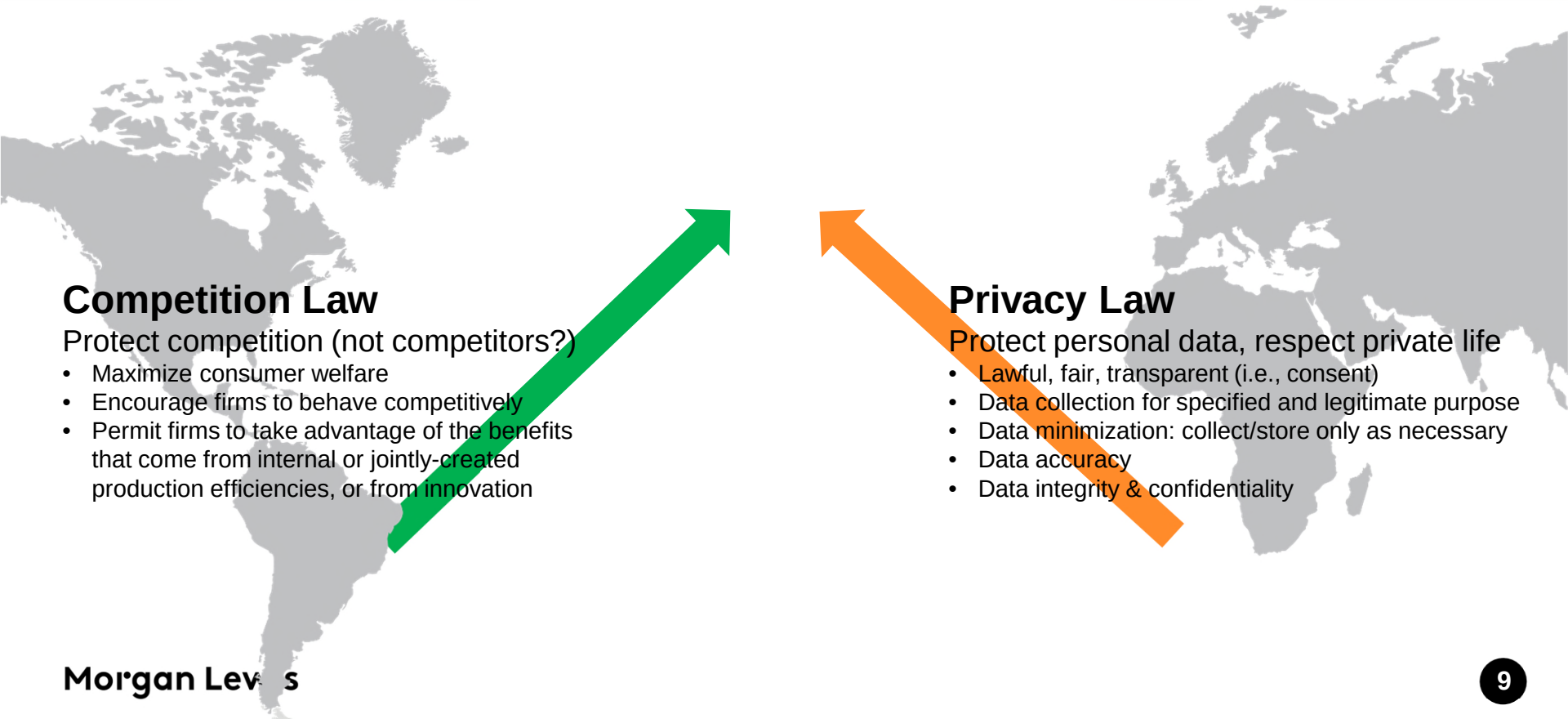
Computing Power + "Connected" Transactions + User-Specific, Convenient Services

DATA FOOTPRINT

Data is Everywhere

- Data is central to the digital economy
  - Access to data helps drive important innovations (medical diagnoses, language translation, public safety, digital platforms/communities, etc.)
- Data is omnipresent and readily available; it is not like a limited natural resource
  - Very difficult for one firm to prevent others from obtaining data
  - Users access multiple online services, engage in transactions on different platforms
- Users can share similar data with many firms – users don't really "lose" their info
- Thus, different firms often have near-simultaneous access to data

Intersection Between Competition and Privacy Laws



Competition Law

Protect competition (not competitors?)

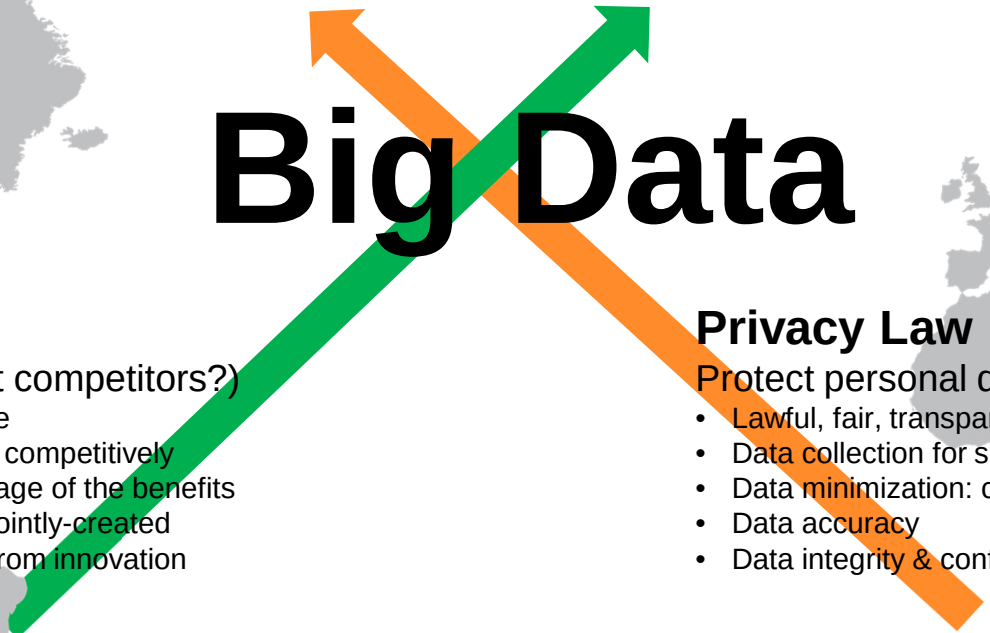
- Maximize consumer welfare
- Encourage firms to behave competitively
- Permit firms to take advantage of the benefits that come from internal or jointly-created production efficiencies, or from innovation

Privacy Law

Protect personal data, respect private life

- Lawful, fair, transparent (i.e., consent)
- Data collection for specified and legitimate purpose
- Data minimization: collect/store only as necessary
- Data accuracy
- Data integrity & confidentiality

Intersection Between Competition and Privacy Laws



Competition Law

Protect competition (not competitors?)

- Maximize consumer welfare
- Encourage firms to behave competitively
- Permit firms to take advantage of the benefits that come from internal or jointly-created production efficiencies, or from innovation

Privacy Law

Protect personal data, respect private life

- Lawful, fair, transparent (i.e., consent)
- Data collection for specified and legitimate purpose
- Data minimization: collect/store only as necessary
- Data accuracy
- Data integrity & confidentiality

Which direction does your scale tilt?

Which direction does your scale tilt?

Which direction does your scale tilt?

SECTION 02

THE COMPETITION LAW DEBATE

Different Approaches to Competition Law

- United States Enforcement - <u>Agencies</u>
  - Department of Justice, Antitrust Division
  - Federal Trade Commission
  - State Attorneys General
  - Industry-specific regulators (SEC for financial services, etc.)
  - Private litigation (e.g., class actions)

- European Enforcement - <u>Agencies</u>
  - European Commission, Directorate General for Competition
  - Member State Competition Authorities
  - Private litigation (more recent development)

Different Approaches to Competition Law

- United States Enforcement - Approach
  - Focused more on litigation
  - Guided by consumer welfare based on sophisticated economic analysis
  - Protects competition, not competitors

- European Enforcement - Approach
  - Focused more on regulatory enforcement, somewhat more bureaucratic
  - Guided by fairness and protecting the "structure" of the market
  - Places value on integration of member states into single common market
  - Protects competition and competitors

A U.S. PERSPECTIVE

"My view is that privacy and antitrust law each addresses different harms and vindicates different rights. Just because something is a privacy problem, doesn't make it an antitrust problem."

FTC Commissioner Noah Phillips

Interview, *Law360* (May 8, 2019)

"We must remember that big platforms were once themselves start-ups, and be cautious in any enforcement decision to not undermine the very innovation incentives that competition aims to protect."

Asst. Attorney General Makan Delrahim

Remarks (October 17, 2018)

Should privacy concerns be relevant to antitrust law?

- Competition and privacy policies have separate objectives that may be in tension
- Competition law should be focused on ensuring the market works for consumers

Lower Prices

Innovation

Greater output

- Improvements in data collection and expansion of online business models may result in more competition, not less competition

2018: Federal Trade Commission

Federal Trade Commission Announces
Hearings on Competition and Consumer Protection in the 21st Century

The intersection between privacy, big data, and competition:

(a) data as a dimension of competition and/or as an impediment to market entry

(b) competition on privacy and data security attributes (between, e.g., app developers)

(c) whether consumers prefer free/ad-supported products to products offering similar services or capabilities but that are neither free nor ad-supported

(d) the costs/benefits of privacy regs, including the effect of such regulations on innovation

(e) the costs/benefits of varying (often conflicting) state, federal and international privacy laws

(f) competition and consumer protection implications of use and location tracking

2019: FTC Technology Task Force

FTC announced "the creation of a task force dedicated to monitoring competition in the U.S. technology markets, investigating any potential anticompetitive conduct in those markets, and taking enforcement actions when warranted."

-Feb 26, 2019

Should privacy concerns be relevant to antitrust law?

- Under U.S. law, main focus of competition enforcement is economic efficiency
- Potential cost to privacy restrictions: limitation on data uses (reduced output), reduced revenue, and reduced innovation/quality
- Consumers, perhaps generically, value privacy, but still relentlessly share info
- Consumers value free and convenient services

Bottom Line Viewpoint: Why can't privacy concerns be addressed instead through data policies/terms and existing privacy regulations?

Should privacy concerns be relevant to antitrust law?

- Potential dangers in using competition law as a "law of everything"
- In fact, using antitrust law might actually undermine privacy protection as…
  - competition enforcers seek to "level the playing field" by artificially forcing data-sharing
  - competition enforcers create onerous new "privacy" requirements that make market entry more complex or legal compliance more costly (particularly for smaller firms)

Traditional Analysis Applied to "Big Data"

- Elements of monopolization: market power + exclusionary conduct
  - Indirect evidence of market power: market share + barriers to entry/expansion
- Big Data mischaracterized as "barrier to entry"?
  - Data can be shared with more than one firm (the "$100 comparison")
  - Data is widely available and cheap to collect/store
  - Data becomes stale relatively quickly (so mass amounts of old data may not be helpful)
  - Data is rarely the "product" – but, rather, just one potential input (go find other inputs!)
- Use of Big Data as "exclusionary conduct"?
  - Antitrust law rarely requires *helping* a competitor

Takeaway Points – U.S. Law

- Focus of competition enforcement should remain on economic efficiency
- Conduct that is unlawful under traditional antitrust law can be remedied
- Focus should be on the conduct itself and its effect on consumer welfare, not on how much data a company holds
- A helpful sanity check: If the conduct involved some other input (besides data), would competition law care about it?

THE EUROPEAN DEBATE

"***Data is the new currency***."

Margrethe Vestager,

EU Commissioner for Competition

An Evolving European Perspective

1. Use of data by hybrid platforms: Crossing the line?
2. Vertical data integration: Leveraging upstream power on downstream markets
3. Data aggregation (part 1): Is this an antitrust issue?
4. Data aggregation (part 2): Remedies proposed against "data market power"
5. Merger control: The spectre of innovation buy-out

An Evolving European Perspective

1. Use of data by hybrid platforms: Crossing the line?
2. Vertical data integration: Leveraging upstream power on downstream markets
3. Data aggregation (part 1): Is this an antitrust issue?
4. Data aggregation (part 2): Remedies proposed against "data market power"
5. Merger control: The spectre of innovation buy-out

What if there is no natural monopoly?

- Issue: Use of data from one platform business for the other platform business, to the alleged detriment of rivals only active on one side of the business.
- "Old wine in new bottles": a theory of harm from the times of the utilities…
- ….but not quite: Is there a conflict of interest?

An Evolving European Perspective

1. Use of data by hybrid platforms: Crossing the line?
2. Vertical data integration: Leveraging upstream power on downstream markets
3. Data aggregation (part 1): Is this an antitrust issue?
4. Data aggregation (part 2): Remedies proposed against "data market power"
5. Merger control: The spectre of innovation buy-out

What if there is no essential facility?

- Issue: Extending the position of the platform into new markets by allegedly giving preferential treatment of the platform to own services in those markets
- Acting as "player and referee"
- When is the platform or service "essential to compete"?

An Evolving European Perspective

1. Use of data by hybrid platforms: Crossing the line?
2. Vertical data integration: Leveraging upstream power on downstream markets
3. Data aggregation (part 1): Is this an antitrust issue?
4. Data aggregation (part 2): Remedies proposed against "data market power"
5. Merger control: The spectre of innovation buy-out

Blurring the borders between antitrust and consumer/privacy protection

- Issue: Alleged aggregation of personal data w/o prior consent by the consumer
- EU Commission: "*private businesses, public responsibilities*"
- German FCO: violation of data protection rules is the benchmark for a non-price abuse of a dominant position

An Evolving European Perspective

1. Use of data by hybrid platforms: Crossing the line?
2. Vertical data integration: Leveraging upstream power on downstream markets
3. Data aggregation (part 1): Is this an antitrust issue?
4. Data aggregation (part 2): Remedies proposed against "data market power"
5. Merger control: The spectre of innovation buy-out

Behavioural remedies currently the preferred option

- Limiting data collection on grounds of antitrust or privacy
- Imposing access to data (against remuneration)
- Imposing portability of data for customers
- Imposing interoperability between different platforms and data bases

An Evolving European Perspective

1. Use of data by hybrid platforms: Crossing the line?
2. Vertical data integration: Leveraging upstream power on downstream markets
3. Data aggregation (part 1): Is this an antitrust issue?
4. Data aggregation (part 2): Remedies proposed against "data market power"
5. Merger control: The spectre of innovation buy-out

European merger regimes in full (r)evolution

- Mergers between physical and digital sides of the business get special attention
- Value thresholds capture start-up acquisitions
- Fear of "killer acquisitions" could provoke fundamental shift in merger control

SECTION 03

THE PRIVACY LAW SOLUTION?

The California Consumer Privacy Act of 2018

- On June 28, 2018, California enacted the California Consumer Privacy Act (CCPA)
  - A unique and comprehensive consumer privacy law
  - Unlike any other US privacy law
  - "GDPR-like" consumer privacy rights
  - New private right of action for security breaches and potential statutory damages

- IAPP estimates that the law will likely affect more than 500,000 US companies doing business in California
  - Including many small and midsized businesses

Factors Influencing the CCPA

- GDPR
  - CCPA is influenced by concepts such as GDPR's "right to be forgotten"
  - GDPR's heightened transparency requirements
  - Right of portability

- CCPA builds upon other unique California privacy laws
  - California Online Privacy Protection Act (CalOPPA)
  - The "Shine the Light" law
  - The "Reasonable Security" law

- Reflects recent concerns expressed in congressional hearings and the press regarding collection and use of personal information by social media and other tech companies

Reshaping the U.S. Privacy Landscape

- As with several other landmark laws, California is likely to be the "tail that wags the dog" with respect to U.S. privacy practices
- CCPA reflects:
  - A much more prescriptive approach to privacy regulation (as opposed to the FTC's general "notice and consent" framework under Section 5 of the FTC Act)
  - A desire to regulate social media and technology companies and address the robust consumer profiles that they are maintaining
  - Desire to empower consumer lawsuits re privacy / security to drive corporate conduct
    - Which may be expanded beyond security breach to all CCPA privacy violations if a proposed amendment bill is enacted

Businesses Subject to the CCPA

- A "business" subject to the CCPA must be a for-profit org or legal entity that
  - Does business in California
  - Collects consumers' personal info, either directly or through a third party on its behalf
    - "Collects" broadly defined to include "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."
  - Either alone, or jointly with others, determines the purposes and means of processing of consumers' personal information
    - Resembles GDPR's "data controller" concept

Additional Criteria for Businesses

- A business must also satisfy one of three thresholds:
  1) Annual gross revenue in excess of $25 million
  2) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination
  3) Derives 50% or more of annual revenue from selling consumers' personal information

- Applies to brick-and-mortar businesses, not just collection of personal information electronically or over the internet
- Does not apply to nonprofits

CCPA Does Not Apply To …

- Medical information and entities subject to HIPAA or the California Confidentiality of Medical Information Act (CMIA)
  - SB 1121 expands this exception and clarifies that it applies to HIPAA business associates
- Personal information subject to the Gramm-Leach Bliley Act (GLBA) or the California Financial Privacy Act
  - SB 1121 eliminated some ambiguities regarding this exception
- SB 1121 adds an exception for clinical trials data
  - But does the exception apply more broadly to all clinical research activities?

CCPA Definition of Personal Information

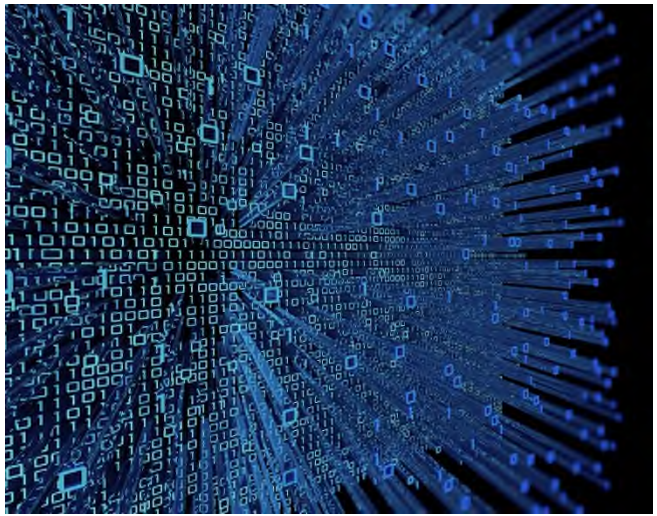
1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

New Statutory Rights

- Right to know the categories of info
- Right of access and data portability
- Right to be forgotten
- Right to opt out of the sale of personal info to third parties
- Right to equal service and price

Right to Know the Categories of Information

- A business is required to disclose
  - At or before the point of collection
  - In its website privacy policy or otherwise
  - The categories of personal info to be collected about a consumer
    - Including the categories of the consumer's personal info that were actually collected during the last 12 months
    - PI sold or disclosed for business purposes in the last 12 months
  - The purposes for which the info will be used



Verifiable Consumer Requests

- In addition to website privacy policy, CCPA requires each business to respond to "verifiable consumer requests" with individualized disclosures about the business's collection, sale, or disclosure of PI belonging to the specific consumer making the request

- "Verifiable consumer request" is a request by "a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State"
  - Consumer can make two requests in a 12-month period

Complying With Consumer Requests

- Business must offer two or more methods for making the requests
  - At a minimum: a toll-free phone number and a website address

- Does your business have the ability to produce this sort of highly granular report for each consumer?

In response to a request, the business must disclose:

(1) categories of personal info collected about consumer

(2) categories of sources from which personal info collected

(3) commercial purpose for collecting or selling the PI

(4) categories of 3rd parties in receipt of the PI

(5) specific pieces of PI the business has collected

(6) categories of PI that were sold or disclosed for business purposes in the 12 months preceding the request

Right of Access and Data Portability

- CCPA gives each consumer the right to access a copy of the "specific pieces of information that the business has collected about that consumer"
  - To be delivered free of charge
  - Within 45 days
  - By mail or electronically
- Does not apply to PI that is collected for "single, one-time transactions"
- Implies an obligation for businesses to preserve these consumer records
- Information produced must be portable, to the extent "technically feasible"
- In a readily usable format
- "Technical feasibility" standard appears to be drawn from Art. 20 of GDPR, which also creates a right of portability

Right to be Forgotten

- Under the CCPA, consumers have the right to request that a business delete any PI collected about the consumers
  - Extends to PI held by a third-party service provider
- Exceptions where PI is necessary to:

(1)Complete a transaction, provide goods and services, or otherwise perform a contract with a consumer

(2)Detect security incidents

(3)Exercise free speech

(4)Enable internal uses that are reasonably aligned with consumer expectations

(5)Comply with a legal obligation

(6)Otherwise use the consumer's PI in a lawful manner that is compatible with the context in which the PI was provided

Right to be Forgotten Versus Preservation of Evidence

- The right to be forgotten may not be consistent with a company's need to preserve evidence for litigation

- CCPA will entail a review of a company's document retention policy
  - Policy will need to be revised to reconcile:
    - Need to preserve evidence for litigation
    - Honor CCPA's right to be forgotten
    - Avoid sanctions for spoliation of evidence

Right to Opt Out of Sale of Personal Information

- The CCPA provides consumers with the right to opt out of the sale of their personal information to third parties
  - Businesses that sell personal information to third parties must provide notice to consumers that
    - Their personal information may be sold
    - They have the right to opt out of the sale

- A business must post a "clear and conspicuous link" on its website's home page titled "Do Not Sell My Personal Information"
  - The page must also be linked in the business's privacy policy

Minors' Opt-in Right

- CCPA provides minors with a "right to opt in"
  - Businesses are prohibited from selling PI of consumers between the ages of 13 and 16 without first obtaining affirmative opt-in consent
    - From the consumers or
    - From the parent or guardian where a consumer is under the age of 13
  - CCPA age requirements are stricter than the federal Children's Online Privacy Protection Act (COPPA)
  - CCPA also differs from the Privacy Rights for California Minors in the Digital World law, which permits persons under age 18 to remove certain posted online content

What is a Sale?

- A "sale" is defined as
  - "selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating
  - orally, in writing, or by electronic or other means,
  - a consumer's personal information
  - by the business to another business or a third party
  - for monetary or other valuable consideration"

- Limited exceptions, including "intentional interaction" directed by a consumer and disclosure to a service provider
- Definition is extremely broad and needs to be clarified

Is Affiliate Sharing a Sale?

- When a business shares PI with an affiliate, would that constitute a sale requiring opt-in consent?
  - Arguably a "transfer" of PI to another business or third party
  - However, the definition of "business" includes another entity under the business's control that operates under the same brand
  - Under current definitions, the answer will depend on the facts and circumstances
    - Is the affiliate using the same brand?
    - Is monetary or "other valuable consideration" changing hands?
      - This is probably not a high bar under California contract law authorities

Right to Equal Service and Price

- CCPA grants consumers a "right to equal service and price"
  - Prohibits businesses from discriminating against consumers who exercise their rights under the CCPA
- A business is specifically prohibited from

(1)Denying goods or services to a consumer

(2)Charging a consumer a different price or rate for goods or services, including through the use of discounts or other benefits

(3)Imposing penalties

(4)Providing a consumer with a different level of quality or service

(5)Suggesting a consumer will receive a different price or rate or different level of quality of goods or services

Right to Equal Service and Price (cont.)

- A business may charge a consumer who exercises rights a different rate or provide a different level of service so long as the difference is directly related to "value provided to the consumer by the customer's data"
  - How would that difference in value be quantified and supported?
- Businesses may offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of personal information
- Businesses must ensure that personnel responsible for handling consumer inquiries under the CCPA are informed of the requirements and how to direct consumers regarding granting those rights

Limitations on Disclosures to Third Parties and Service Providers

- CCPA allows businesses to share PI with third parties or service providers for business purposes
  - So long as there is a written contract prohibiting a service provider from
    - selling the PI or
    - "retaining, using, or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract"
- "Business purpose" is defined as "the use of PI for the business's or service provider's operational purposes, or other notified purposes, provided that the use of PI shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected"

CCPA-Compliant Service Provider Agreements

- A business that satisfies CCPA's contracting requirements will not be liable for the service provider's or third party's violation of the CCPA
  - Provided that the business did not have actual knowledge or reason to believe at the time that the PI was disclosed that the recipient intended to violate the CCPA
- A CCPA-compliant service provider agreement will not constitute a sale of PI triggering the CCPA's opt-out right
- CCPA contracting requirements are generally consistent with good privacy practices, but they create a new filter that must be applied to agreements
  - Does the agreement limit use of PI to the specific purpose of performing the specified services?
  - Is the use of PI reasonably necessary and proportionate to the operational purpose?
  - Is the purpose of the agreement a "business purpose"?

CCPA and Class Actions

- Impact of CCPA's statutory damages for security breach on class action litigation in California

- CCPA provides that any agreement or contract provision that seeks to waive or limit a consumer's rights under the CCPA
  - Including any "right to a remedy or means of enforcement," shall be deemed void and unenforceable
  - Could be interpreted to bar arbitration and class action waivers with respect to private actions under the CCPA

The CCPA's Progeny

- The CCPA will be amended further; the question is, how substantially?
- Will other state legislatures take the CCPA as a model?
  - Will CCPA catch on like CA's data breach notification law?
  - Or will it be a one-off experiment, like the Shine the Light law?
  - Bills pending in New York, New Jersey and New Mexico that appear to be influenced by the CCPA
- If other states adopt CCPA-like laws, the US privacy regulatory landscape could become extraordinarily complicated, driving interest in broad federal privacy legislation
- February 27: Senate Committee on Commerce, Science and Transportation convenes a hearing on policy principles for a federal privacy framework

INTERPRETING THE CCPA: OPEN QUESTIONS

Preparing for 2020

- While further details concerning the CCPA remain unresolved, the framework is in place
- Eight CCPA amendment bills are currently advancing through the California Legislature
- Businesses can use the time now to begin thinking about how they would comply with the CCPA under the current framework
  - For the sweeping CCPA, a year and a half is not that long (as we learned with GDPR)
- Companies that have recently prepared for GDPR compliance have seen the benefits of a head start
  - GDPR data-mapping and privacy assessment exercises will be useful
  - But CCPA is not simply CA's version of GDPR, and the requirements differ in many important respects

Initial CCPA Compliance Questions

- Does the CCPA apply to your business or do you fit into an exception?
- How many of the data elements included in CCPA's broad definition of personal information does your business collect?
  - Are additional data-tracking mechanisms needed?
- How would your business go about organizing consumer PI to
  - Provide required CCPA notices
    - Can build upon existing California privacy notices developed for CalOPPA and Shine the Light law
  - Provide opt-out and opt-in rights
  - Delete data to comply with the CCPA's right to be forgotten

Biography

W. Reece Hirsch
San Francisco
T +1. 415.442.1422
F +1.415.442.1001

W. Reece Hirsch counsels clients on healthcare regulatory and transactional matters and co-heads the firm's privacy and cybersecurity practice. Representing healthcare organizations such as hospitals, health plans, insurers, physician organizations, healthcare information technology companies, and pharmaceutical and biotech companies, Reece advises clients on issues such as privacy, fraud and abuse, and self-referral issues. This includes healthcare-specific data privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act.

Biography

Brian C. Rocca
San Francisco
T +1.415.442.1432
F +1.415.442.1001

Brian C. Rocca focuses on antitrust and complex litigation matters. He is managing partner of the firm's 135-lawyer San Francisco office and leader of the firm's Chambers-ranked California antitrust practice. Brian has worked on litigation, investigation, and counseling matters in many industries, with particular emphasis on technology and internet-based services. In 2017, Brian was named one of the "Top 40" lawyers in California under the age of 40 by the San Francisco and Los Angeles Daily Journal, and was named by Law360 as one of only five "Rising Star" competition lawyers globally.

Biography

Christina Renner

Brussels

T +32.2.507.7524

F +32.2.507.7555

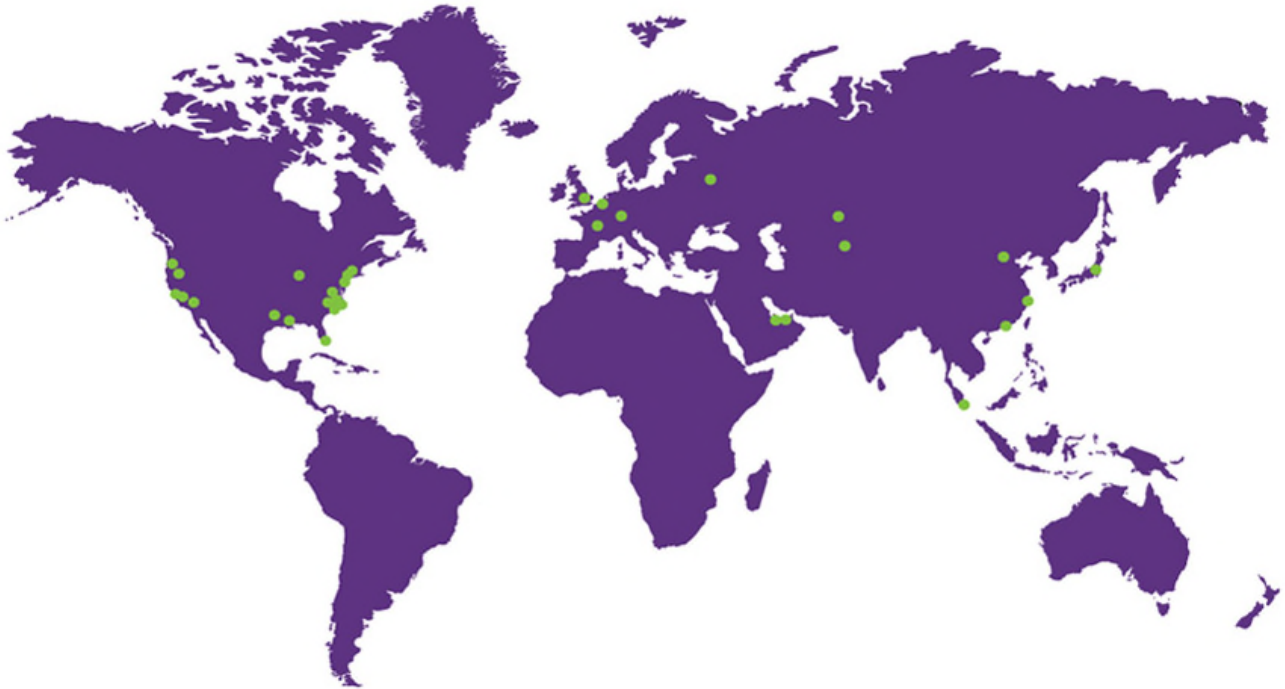
Christina Renner concentrates her practice on European Union and German merger control, competition, and antitrust law, with experience in cartels and general behavioral matters, abuse of dominance, and EU state aid laws. Christina regularly advises clients concerning mergers reviewed by the European Commission and the German Federal Cartel Office, as well as the French, Austrian, and Belgian competition authorities. She represents diverse international clients in antitrust investigations before the European Commission and other national competition authorities, including in litigation before European courts. Her work spans a variety of industries, including transportation, energy, life sciences, as well as retail and ecommerce. Christina is admitted in Brussels and Germany only.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU