WINSTON & STRAWN LLP

GLOBAL PRIVACY AND DATA SECURITY

Mastering Contracts: Navigating Privacy Requirements and Negotiations for Organizational Protection

August 15, 2023

SPEAKERS

ALESSANDRA SWANSON
Partner and Co-Chair,
Global Privacy & Data Security Practice
Chicago

MARY KATHERINE KULBACK
Partner
Global Privacy & Data Security Practice
Chicago

KEVIN SIMPSON
Partner
Global Privacy & Data Security Practice
Los Angeles // Chicago

WINSTON & STRAWN LLP

Overview

Agenda

- The Privacy Awakening: The Regulatory Landscape and How This Impacts Commercial Contracting
- Critical Issues to Address in Data-Related Commercial Contracts
- How to Think About Managing Privacy-Related Risks

Our Goal For Today's Presentation

- Privacy is a rapidly evolving field and there will rarely be clear-cut answers to the complicated legal questions your organization will face.
- Emerging technologies such as AI are creating value with respect to data that should be captured and new issues to be considered in contracts.
- Our objective for today is to provide you with meaningful context about the current state of privacy and a primer on how to navigate associated risks in commercial contracts.

WINSTON & STRAWN LLP

THE PRIVACY AWAKENING

The Regulatory Landscape and How This Impacts Commercial Contracting

Current State of U.S. Privacy Law

- Prior to 2018, apart from regulated industries like health care and financial services, there were no comprehensive privacy laws regulating personal information in the United States.
- Today, with California leading the way, there are five states with complicated and sometimes conflicting regimes that have radically shifted how businesses must manage their consumer, employee, and customer personal information.

Current State of U.S. Privacy Law

- Regulators have responded to increasing consumer concern related to the use and disclosure of personal information by introducing and passing significant legislation, such as CCPA, VCDPA, etc.
- Plaintiffs' attorneys have seized upon this focus on privacy by pursuing claims under laws that received almost no interest prior to 2015, including BIPA and CIPA.

As the potential liabilities increase, an organization's first line of defense is through protections in commercial contracts.

- Aggressive Plaintiffs' Bar
- Uncapped Statutory Damages
- Strict Liability and Tough to Dismiss at Pleading Stage
- Bet-the-Business Class Action Damages Calculations
- Vague and Ambiguous Statutes
- Rapidly-Developing Case Law
- Ever-Changing Regulatory Landscape

WINSTON & STRAWN LLP

Critical Issues to Address in Data-Related Commercial Contracts

Four Buckets of Concern

- Provisions required by law
  - CCPA and similar state laws have specific requirements that are required to be in commercial contracts to avoid the exchange of personal data from constituting a “sale.”
- Establishing data ownership and usage rights vis-à-vis the contracting parties
- Protections for the privacy and security of data that constitutes personal information in particular
  - This includes rights and restrictions related to the use of personal information, safeguards to protect data, and notification in the event of unauthorized use or disclosure of data.
- Allocation of risk regarding all categories of data

Provisions Required by Law

- California has a long list of requirements that must be included in contracts involving the exchange of personal information, including by arguably increasing the obligation on a data controller to audit its data processors.
- Colorado, Connecticut, Virginia and Utah have their own requirements, which include explicit audit rights and the right to object to subprocessors.
- With more laws on deck that will go into effect in 2024 and 2025, these provisions must be efficiently integrated into written agreements.

Establishing Data Ownership and Usage Rights Vis-à-vis the Contracting Parties

- When personal information is being processed by a third party, valuable IP may be created.
- Define relevant categories of data and clarify who owns that data and other associated IP (*e.g.*, tools, work product) or risk losing out on valuable business assets.
- Craft, with precision, a party's rights and restrictions regarding use of data owned by or provided on or behalf of the other party in order to protect your assets and mitigate risk. Think of intended uses down the line as technology improves and also consider subcontractors and third parties.
- Don't forget about assignment / change of control provisions and rights to data after a contract terminates / expires.

How Privacy Laws Translate into Litigation Risk

- CCPA, TCPA, and BIPA all include significant statutory fines.
- Security breaches can also create liability through costs associated with investigation, notification, regulatory inquiries, and class action lawsuits.
- Vendor contracts in the TCPA and BIPA space generally push all privacy obligations on the company utilizing the technology and have strong indemnification terms.

Protections for the Privacy and Security of Personal Information to Manage Litigation Risk

- Rights and restrictions related to the use of personal information
  - State laws have become more specific about enumerating data use purposes within the contract.

- Safeguards to protect personal information
  - These can vary from high-level requirements to specific data security exhibits.
- Notification in the event of unauthorized use or disclosure of data
  - Contracts should specify notification timelines (if possible) and actions service providers should take following an incident.

Safeguards to Protect Personal Information

- How to incorporate safeguards into the contract
  - Security exhibits
  - Vendor documentation
  - References to reasonable safeguards
- Critical safeguards to address
  - Access controls
  - Network monitoring and endpoint detection
  - Encryption
  - Security audits
  - Destruction and deletion of data
  - Role of cyberinsurance

Notification in the Event of Unauthorized Use or Disclosure of Data

- What constitutes a breach
  - Actual vs. suspected incidents
  - State law requirements (unauthorized access or acquisition)
  - Triggering security incidents (ransomware or phishing events)
- Timing requirements
  - What is market vs. what is feasible
- Obligations of vendor in the event of a breach
  - Mitigation, investigation, notification, remediation and associated liability

Allocation of Risk Considerations

- The rep and warranty, indemnification, and limitation of liability provisions all need to be read together to ensure appropriate and harmonious coverage.
- Indemnification terms
  - Often a contract will have an indemnity that was intended to address IP infringement and does not address unique data-related issues, so review the indemnity in light of your exposure under the facts.
  - Most indemnities are limited to third-party claims, which would not cover costs incurred through security breach (notification, credit monitoring, investigation, legal, regulatory inquiries).
- Limitations of liability
  - Carve-outs from the limitation of liability and the emergence of super caps.

WINSTON & STRAWN LLP

How to Think About Managing Privacy-Related Risks

Privacy Risk is Interrelated Across The Spectrum

COUNSELING ⟷ CLASS ACTION LITIGATION ⟷ REMEDIATION

Understand Universe of Risk

- Assess current contractual obligations
- Develop system for oversight of vendors
- Internal understanding of privacy requirements
- Data security infrastructure
- Insurance

Negotiation Strategies - Customer

- On the customer side
  - Think strategically about goals
    - Ensuring that there are specific contractual promises about privacy and security
    - Enumerating appropriate data use provisions and restrictions
    - Appropriate allocation of liability
  - Consider compensating controls
    - Vendors are unlikely to meet every specific security requirement your organization may have in place, but there are very often compromises that can be made.

Negotiation Strategies - Vendor

- On the vendor side
  - First and foremost, ensure that you can meet the obligations to which you agree.
  - Consider cyber insurance levels and ensure that any significant promises made in customer contracts can be met through current coverage levels.
  - Understand what is “market” for risk allocation terms and confirm that the organization can take on this level of risk.
  - Create reasonable contracts that address customer legal requirements and market “asks.”

WINSTON & STRAWN LLP

Presenter Bios

ALESSANDRA SWANSON

Co-Chair, Global Privacy & Data Security and Regulated Personal Information Practices
Chicago
+1 (312) 558-7435
ASwanson@winston.com

Alessandra is a co-chair of Winston's Global Privacy & Data Security and Regulated Personal Information practices and counsels clients on significant matters related to the collection, processing, and protection of personal information.

Alessandra is a former federal privacy regulator and primarily focuses her practice in the areas of regulated personal information, privacy and data security counseling, security breach response and regulatory defense, corporate advisory services and outsourcing, and large-scale commercial contracting. Prior to joining Winston, Alessandra spent five years with the U.S. Department of Health and Human Services – Office for Civil Rights, where she was involved in a number of high-profile privacy investigations and settlements.

Alessandra has counseled some of the country's most well-known health care companies, brands, retailers, media companies, and e-commerce platforms regarding their compliance with privacy and data security laws. She has helped clients develop privacy compliance programs, employee training, and security incident response plans; undertake information security assessments; implement privacy-by-design processes; create internal and consumer-facing privacy disclosures; assess software platforms and new technologies for privacy and security issues; and leverage new technologies to reach consumers.

Services
Government Program Fraud, FCA, and Qui Tam Litigation
Health & Welfare Benefits
IP/IT Transactions & Licensing
Intellectual Property
Privacy & Data Security
Regulated Personal Information

Sectors
Consumer Products
Financial Services & Banking
HIPAA and HITECH
Health Care & Life Sciences
Health Care Litigation & Investigations
Health Care Privacy & Data Security
TNT

Bar Admissions
Illinois

Education
DePaul University, JD, 2009
Northwestern University, BA, 2005

MARY KATHERINE KULBACK

Partner, Global Privacy & Data Security and Regulated Personal Information Practices
Chicago
+1 (312) 558-6458
MKulback@winston.com

Mary Katherine is a partner in Winston's Global Privacy & Data Security and Regulated Personal Information Practices who focuses her practice on intellectual property, technology, privacy, and data security matters.

Services
Advertising & Consumer Protection
Brand Enforcement / Trademark Litigation
Copyright Infringement
Emerging Growth & Venture Capital
IP/IT Transactions & Licensing
Intellectual Property
Privacy & Data Security
Regulated Personal Information
Trademark Prosecution

Sectors
Consumer Products
Financial Services & Banking
Health Care & Life Sciences
Media & Entertainment
Sports
TNT

Bar Admissions
Illinois

Education
Chicago-Kent College of Law, JD 2013
University of Notre Dame, BA 2009

Mary Katherine assists her clients in building, commercializing, protecting, and enforcing their intangible assets by providing commercial contracting services, corporate advisory services, and IP/technology/data counseling. Mary Katherine regularly drafts and negotiates a wide variety of agreements involving intellectual property, technology, privacy, data security, and commercial issues, including assignments, licensing and cross-licensing agreements; development agreements; joint venture agreements; strategic alliance agreements; research, development, and cooperation agreements; manufacturing agreements; service agreements; supplier agreements; reseller agreements; software as a service (SaaS), cloud service agreements, and other sourcing and IT-related agreements; consulting agreements; e-commerce agreements, and confidentiality agreements.

Mary Katherine also advises on IP and technology matters associated with mergers, acquisitions, asset purchases, investments, and other strategic transactions and routinely represents buyers, sellers, investors, and investees. She provides strategic guidance on optimal structures for IP and IT transactions; negotiates and drafts IP provisions in purchase agreements and negotiates and draft licenses, assignments, transfers, and other agreements ancillary to the transactions; and evaluates intellectual property secret portfolios, companies' practices and agreements related to the development of IP and the protection of confidential and trade secret information, among other services. She also advises emerging and established companies on the development, protection, licensing, use, and commercialization of creative, intellectual, and other intangible properties such as patents, trademarks, data, trade secrets, and software.

KEVIN SIMPSON

Partner, Global Privacy & Data Security and Regulated Personal Information Practices
Los Angeles // Chicago
+1 (213) 615-1778
KPSimpson@winston.com

Kevin is an experienced litigator whose practice encompasses complex commercial disputes and class-action lawsuits. Kevin has deep experience defending companies in consumer privacy lawsuits and advising companies on compliance with federal and state privacy laws.

Services
Appellate & Critical Motions
Litigation
Privacy & Data Security
Regulated Personal Information
Bar Admissions
California
Illinois
Clerkships
USCA - Tenth Circuit for the Honorable Nancy L. Moritz
Education
University of Kansas, BA 2011
Washington University - Saint Louis, JD 2014

Kevin is a litigation partner in Winston & Strawn's Los Angeles office. His practice encompasses complex commercial disputes, class-action litigation, state-law tort claims, and internal investigations. He has experience defending and litigating complex cases at the trial and appellate levels in federal and state courts, through and including trial. While based out of Los Angeles, Kevin also has extensive experience with the Chicago legal market.

Kevin focuses on defending class actions brought under consumer-protection and privacy statutes, including the California Consumer Privacy Act, California Invasion of Privacy Act, Telephone Consumer Protection Act, Fair Credit Reporting Act, and Fair Debt Collection Practices Act, among others. He also counsels clients to help them achieve compliance with these statutes.

Before joining Winston, Kevin served as a law clerk for the Honorable Nancy L. Moritz of the U.S. Court of Appeals for the Tenth Circuit. Before clerking, he worked in private practice.

WINSTON
& STRAWN
LLP