



M&A Insights: Tariff Due Diligence, DOJ's New Data Security Program, Privilege Ownership and Advance Notice Bylaw Updates

June 24, 2025

GIBSON DUNN

MCLE Information

The information in this presentation has been prepared for general informational purposes only. It is not provided in the course of an attorney-client relationship and is not intended to create, and receipt does not constitute, an attorney-client relationship or legal advice or to substitute for obtaining legal advice from an attorney licensed in the appropriate jurisdiction.

- This presentation has been approved for **0.5 general credit (This may change once you get approval from CLE)**.
- Participants must submit the form by **July 1, 2025** in order to receive CLE credit.

CLE Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_bjdBC1NRlbJCXEG

Most participants should anticipate receiving their certificate of attendance in 4-6 weeks following the webcast.

All questions regarding MCLE Information should be directed to CLE@gibsondunn.com.

Today's Panelists



Christopher T. Timura

Christopher T. Timura is a partner in the Washington D.C. office of Gibson, Dunn & Crutcher LLP and a member of the firm's International Trade, White Collar Defense and Investigations, and ESG Practice Groups. Chris helps clients solve problems that arise at the intersection of U.S. national security, foreign policy, and international trade regulation. His clients span sectors and range from start-ups to Global 500 companies. He is regularly ranked in Chambers Global and U.S.A. guides for his work and is a regular speaker and writer on the policy drivers, trends, and impacts of evolving international trade policy and regulation.



Stephenie Gosnell Handler

Stephenie Gosnell Handler is a partner in Gibson Dunn's Washington, D.C. office, where she is a member of the International Trade and Privacy, Cybersecurity, and Data Innovation practices. She advises clients on complex legal, regulatory, and compliance issues relating to international trade, cybersecurity, and technology matters. Stephenie's legal advice is deeply informed by her operational cybersecurity and in-house legal experience at McKinsey & Company, and also by her active duty service in the U.S. Marine Corps. Stephenie is regularly recognized for her excellence in the field, most recently being named to *Financier Worldwide Magazine's* Power Players: Foreign Investment & National Security 2025 – Distinguished Advisers report.



Michelle M. Gourley

Michelle M. Gourley is a Partner in the Orange County office of Gibson, Dunn & Crutcher and is a member of the firm's Mergers and Acquisitions and Private Equity Practice Groups. Ms. Gourley is a corporate transactional lawyer whose experience includes advising both strategic companies and private equity clients (including their portfolio companies) in connection with public and private merger transactions, stock and asset sales, joint ventures, strategic partnerships, and other complex corporate transactions. Ms. Gourley works with clients across a wide range of industries, and has extensive experience working with life sciences companies (pharma and medical device) and media, technology and entertainment companies.



Mark H. Mixon, Jr.

Mark H. Mixon, Jr. is Of Counsel in the New York office of Gibson, Dunn & Crutcher and is a member of the firm's Litigation and Securities Litigation Practice Groups. Mark is a general corporate and commercial litigator who represents individual and corporate clients in complex, high-stakes business and corporate governance disputes, including commercial breach of contract actions, corporate-control litigation, disputes related to directors' and controlling stockholders' fiduciary duties, stockholder derivative and securities litigation, M&A-related litigation, and antitrust and competition matters.



Robert B. Little

Robert B. Little is a partner in Gibson, Dunn & Crutcher's Dallas office. He is a Global Co-Chair of the Mergers and Acquisitions Practice Group and a member of the firm's Executive Committee. Rob is consistently recognized for his leadership and strategic work with clients, having been named among the nation's top M&A lawyers by Chambers USA every year for more than a decade. Rob's practice focuses on corporate transactions, including mergers and acquisitions, securities offerings, joint ventures, investments in public and private entities, and commercial transactions. He also advises business organizations regarding matters such as securities law disclosure, corporate governance, and fiduciary obligations.

Agenda

01 **Tariff-Related Due Diligence in M&A Transactions**

02 **DOJ's Regulations on Bulk Sensitive Personal Data and US Government Data**

03 **Assigning Ownership of Privilege in M&A Transactions**

04 **New Developments in Case Law Governing Advance Notice Bylaws**

Tariff-Related Due Diligence in M&A Transactions

01

Tariff-related due diligence in M&A transactions: Contractual Review

For both buyers and sellers in an M&A deal, it's critical to evaluate how tariffs affect the target's **supply chain, compliance posture, and contract structure**. Failure to do so may expose the acquirer to **unexpected costs, regulatory risk, or price renegotiation** post-signing.

Tariff-related provisions have often been under-negotiated in commercial contracts. Given the evolving enforcement landscape, it is now critical to review the target's agreements to understand how tariff obligations are allocated. Key considerations include:

- **Tariff Sharing Clauses**: Tariff-sharing clauses allocate responsibility for import duties between contracting parties. Many agreements lack clear provisions, creating uncertainty when tariffs significantly affect pricing. Diligence should confirm whether such clauses exist, how risk is allocated, and whether the language is sufficiently clear to avoid disputes post-closing.
- **Force Majeure Clauses**: Force majeure clauses may excuse performance due to government actions. Diligence should evaluate whether these clauses exist, and whether they are broad and/or express enough to cover tariff disruptions under relevant state laws.
- **Other Contractual Provisions**: Other relevant contractual clauses include price adjustment clause and indemnities clause (that may relate to regulatory liability allocation), among others.

Tariff-related due diligence in M&A transactions: Trade Compliance

Rising tariffs and heightened enforcement make it essential to assess a target's trade compliance posture as part of due diligence. In particular, companies should investigate any indicators of tariff evasion. Key areas for review include:

- **Country of Origin (COO) Determination**: COO substantially affects tariff exposure of goods. For example, products COO China in general are subject to higher tariffs than, *e.g.*, products COO Vietnam. U.S. Customs of Border and Protection (CBP) is expected to tighten scrutiny, making it critical that COO determinations are well-supported and compliant with legal standards.
- **HTSUS Classification**: Product classifications under the Harmonized Tariff Schedule should be reviewed for accuracy and legal defensibility, as misclassification can lead to underpaid duties and enforcement risk.
- **Transfer Pricing**: Due diligence should include evaluating whether intercompany pricing aligns with customs valuation rules and assess any adjustments that may signal efforts to reduce declared dutiable value.

Tariff-related due diligence in M&A transactions: Liabilities and Risks

Tariff evasion and trade non-compliance may expose a target to significant enforcement risks and liabilities, which should be closely examined during due diligence:

- **CBP Enforcement**: For misclassification, false COO declaration, and undervaluation, CBP may retroactively assess duties owed and demand payments accordingly.
- **False Claims Act (FCA) risks**: The more serious enforcement risk arises under FCA, which the Department of Justice (DOJ) has pledged to use more aggressively to police customs and tariff compliance. In this context, FCA liability can stem from **fraudulent** misclassification, undervaluation, or false country-of-origin declarations. If a violation is found, the government may impose treble damages, significantly increasing the financial exposure beyond ordinary CBP penalties.

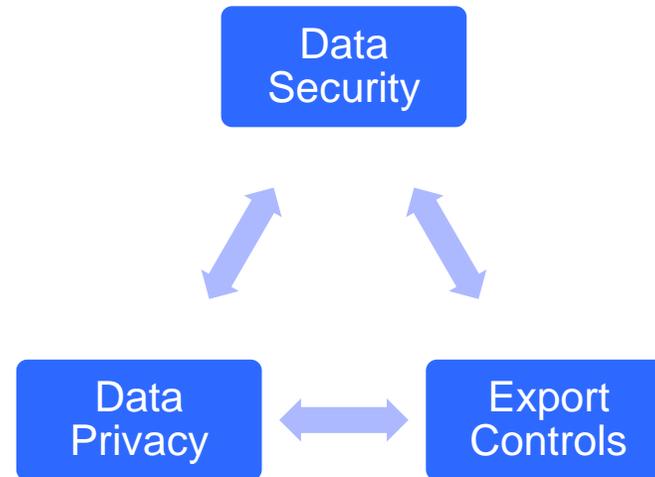
DOJ's Regulations on Bulk Sensitive Personal Data and US Government Data

02

Setting the Stage: DSP = National Security Restrictions on Data Access

Data Security vs Export Controls vs Data Privacy

- Despite its name, the DSP is not solely focused on data security. The Rule is focused on access to data by countries and individuals viewed by the US Government to pose a national security risk. In other words, the Rule is about data as a national security matter as opposed to a traditional privacy view of data protection.
- The Rule is an amalgamation of export controls, data privacy, and data security, with security being the smallest consideration of the three.
- Orienting around the data localization and access requirements—in other words, more of an export controls perspective as opposed to strictly data security perspective—enables a more clear understanding of the Rule itself.



Data Security Program – Summary Overview

What is the DSP?

- **US persons** are not allowed to give bulk US Sensitive Personal Data or US Government Data to Covered Persons or “countries of concern” in a covered transaction:
 - China (including Hong Kong and Macau)
 - Russia
 - Iran
 - North Korea
 - Cuba
 - Venezuela
- Four transactions trigger DSP:
 - Data Brokerage
 - Vendor Agreements
 - Employment Agreements
 - Investment Agreements

Why the DSP?

- The DSP is intended to address national security threats.
- Foreign “countries of concern” have sought to collect Americans’ personal and government data for espionage, blackmail, AI training, etc.
- The DSP aims to prevent such exploitation by prohibiting or restricting certain data transactions that could give adversaries access to the protected data.

Who Does it Effect?

- All **US persons** (including companies, residents, and citizens) must comply with the DSP regulations.
- **Multinational companies** with US entities also fall under the classification of “US Persons” and must also comply.
- Violations can lead to civil or criminal **penalties**.

When Does it Start?

- DOJ’s final rule (28 C.F.R. 202) was issued pursuant to Executive Order 14117 (February 28, 2024). It came into effect April 8, 2025.
- Core prohibitions and restrictions took effect **April 8, 2025**.
- DOJ has provided a 90-day **leniency period** that will expire **July 8, 2025**, for those companies making a **good-faith efforts** at compliance.
- While most requirements are effective now, remaining requirements under the rule will take effect on October 6, 2025.

“Today, the Justice Department took significant steps to move forward with implementing a critical program to prevent China, Russia, Iran, and other foreign adversaries from using commercial activities to access and exploit U.S. government-related data and Americans’ sensitive personal data to ... undermine our national security.”

- DOJ Press Release, April 11, 2025

Data Security Program – Purpose and Key Components

The DSP applies when a “covered data transaction” takes place with “covered data” allowing access by “countries of concern” or “covered persons.”

- The regulations are **complex** and require **careful analysis** to assess compliance requirements.
- In addition to the regulations, as a sign of its focus, DOJ issued a Compliance Guide, 100 FAQs, an Implementation and Enforcement Policy.
- At the core, the regulations applies to transactions fulfilling the following **elements**:

Covered data transaction:

A transaction that involves any **access** by a **country of concern** or **covered person** to any **government-related data** or **bulk US sensitive personal data**

and that also involves:

- (1) **data brokerage**;
- (2) a **vendor agreement**;
- (3) an **employment agreement**, or
- (4) an **investment agreement**.

China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, Venezuela

Foreign person that is an entity 50% or more owned by countries of concern; organized, chartered, or has its principal place of business in a country of concern; is an individual primarily residing in a country of concern; or is an employee or contractor of a country of concern or other covered person.

Geolocation data in a restricted geofenced region or sensitive personal data of current or former government employees

A set of sensitive personal data including personal identifiers, geolocation data, biometric identifiers, human ‘omic data, personal health data, personal financial data, etc.

Covered Data Transaction

The DSP applies when a “covered data transaction” takes place with “covered data” allowing access by “countries of concern” or “covered persons.”

When do you have a “covered data transaction”?

- The rule identifies **four types of transactions** that, if they involve access by a country of concern/covered person to covered data, fall under the DSP.

Data Brokerage Transactions

Definition:

The **sale, license, or transfer of data** as a commodity from one party to another, where the recipient **did not collect the data directly** from the individuals.

Vendor Agreements

Definition:

Contracts where a US person **hires or uses a vendor or service provider** that is a covered person who accesses covered data. A “vendor agreement” involves providing data access to a counterparty as part of a service or product arrangement.

Employment Agreements

Definition:

Hiring or contracting individuals (**employees or contractors**) who are **covered persons** into roles where they could access **covered data**.

Investment Agreements

Definition:

Any arrangement where a country of concern or covered person acquires an ownership interest in a US business that maintains covered data.

DOJ Expectations: Compliance Program

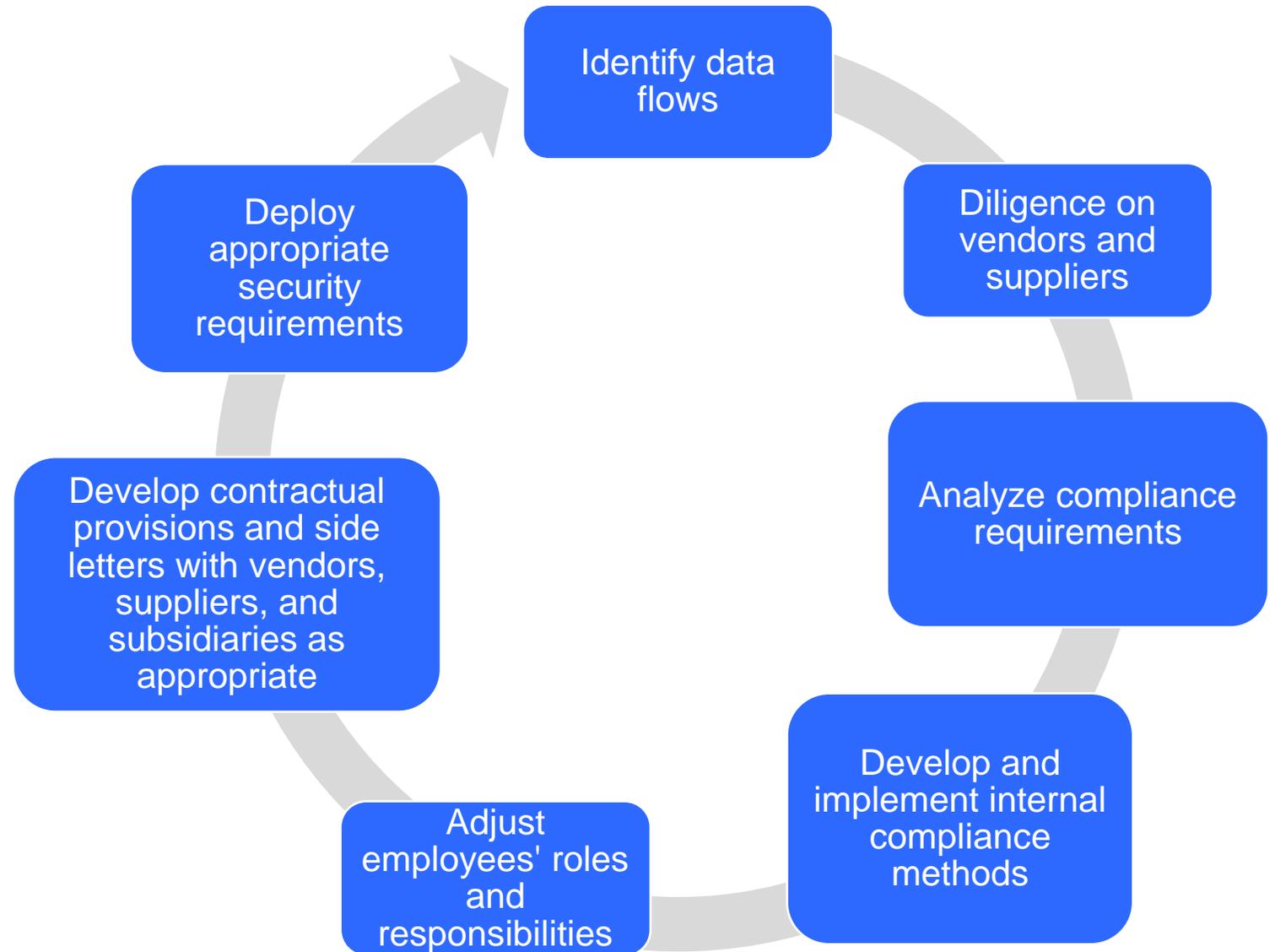
“A company is generally expected to **“know their data”**, including the kind or volume of data processed or handled; how the company uses the data; whether the US company engaged in data transactions; and how such data is marketed, particularly with respect to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community.”

DOJ Compliance Guide at 12 n18.

How should companies focus to ensure compliance:

- **Review your data and data flows.**
Know your data. Understand (i) the nature, volume, geographic location and cybersecurity measures pertaining to covered data and (ii) where you are sending your data—and who has access.
- **Assess impact of the regulatory prohibitions and restrictions.**
Conduct legal analysis of covered data transactions to assess whether such transactions are prohibited or restricted and whether exemptions may apply.
- **Develop and implement a tailored compliance program.**
A comprehensive risk assessment may facilitate the development of a compliance approach tailored to the nature and scope of covered data transactions.
- **Establish the tone from the top—and resource the compliance team.**
DOJ is clear that a strong program will have senior management support and buy-in and set forth specific responsibilities for senior leadership.
 - U.S. companies should appoint an individual responsible for building and maintaining the compliance program.
 - Compliance managers should have organizational senior-level authority, sufficient technical expertise, and appropriate personnel, technical, and other resources to ensure proper implementation of the Data Compliance Program.
 - An officer, executive, or other employee responsible for compliance should sign an annual certification of (1) the company’s Data Compliance Program implementation and due diligence efforts; (2) the company’s implementation of any applicable security requirements; and (3) the completeness and accuracy of recordkeeping documenting the company’s due diligence, as supported by an audit.
- **Expect this landscape to evolve.**
Many open questions remain concerning the implementation of the Rule.

What Compliance Looks Like



Top Considerations for M&A

- **Enhanced due diligence into exposure**
 - New areas of due diligence must be built into diligence workflows when appropriate.
 - Map and review data flows: enhanced due diligence to understand the data assets of the target company and ensure compliance with DSP.
 - Evaluate current data, cataloging and classification systems, and existing protections.
 - Analyze vendor and third-party data-sharing relationships and agreements to ensure they align with the DSP, especially regarding data transfers to third parties.
- **Deal structuring**
 - The DSP may impact how deals are structured, particularly with regards to the transfer of sensitive data and the involvement of entities in countries of concern.
 - Negotiate DSP-related clauses: purchase agreements should include clauses related to security controls, breach notification timelines, indemnities for cyber incidents, etc.
 - Contracts may need to include specific clauses addressing data security, onward transfers, and compliance with the DSP.
- **Post M&A integration**
 - Integration plans must include unified auditing systems capable of monitoring DSP compliance across both legacy and acquired operations.
 - The DSP requires training programs. These must be extended or created to cover newly integrated staff.
- **Potential for regulatory scrutiny**
 - There is a potential for DOJ scrutiny on M&A deals involving entities handling sensitive data, particularly if there are countries of concern involved.

Assigning Ownership of Privilege in M&A Transactions

03

Key Case Law

Great Hill Equity Partners IV, LP v. SIG Growth Equity Fund I, LLP, 80 A.3d 155 (Del. Ch. 2013)

- **Holding:** Where privilege was not explicitly carved out of a merger transaction, Seller's privilege passed to Buyer as a matter of law.
- **Rationale:** Delaware merger statute (§ 259 of the DGCL) says "all property, rights, privileges, powers and franchises, and all and every other interest shall be ... the property of the surviving or resulting corporation." The plain terms of the statute required the outcome. Court noted parties can **contract around** this default rule.

Shareholder Representative Servs. LLC v. RSI Holdco, 2019 WL 2290916 (Del. Ch. May 29, 2019)

- **Holding:** Where the merger agreement carved out Seller's privilege from the assets transferred, privilege remained with Seller, and Seller did not waive privilege (even though privileged communications in email form remained in computers that were transferred in the sale).
- **Rationale:** Merger agreement carve out + "no use" provision defeated Buyer's argument. Court rejected argument that Seller waived privilege by failing to remove the privileged communications from the computers before giving them to the Buyer.

DLO Enterprises, Inc. v. Innovative Chem. Prods. Grp., LLC, 2020 WL 2844497 (Del. Ch. June 1, 2020)

- **Holding:** "In the asset purchase context, the **seller will retain pre-closing privilege** ... unless the buyer clearly bargains for waiver."
- **Rationale:** The law distinguishes between mergers and asset purchases. [In an asset sale, "[t]he **seller still exists**, holding any assets that were not purchased, together with related privileges."

Key Language in Transaction Agreements

What is the scope of the communications that should be subject to the retained privilege?

- All communications with counsel occurring pre-closing
- Only communications directly related to the transaction
- Everything in between (i.e., communications not related to the transaction at first that later become part of the transaction)

Who *owns* the target company privilege?

- Stockholder group and/or the Stockholder Representative
- Buyer
- Surviving Corporation (in a merger)

Who *controls* the target company privilege?

- Stockholder group and/or the Stockholder Representative
- Buyer
- Surviving Corporation (in a merger)

Key Language in Transaction Agreements

Who has access to the privileged communications?

- Stockholders
- Stockholder Representative
- Buyer
- Surviving Corporation (in a merger)

Buyer's ability to assert target company privilege against third parties

Buyer's ability to waive target company privilege against third parties

- Consent requirement

Other Clauses

- Buyer's ability to disclose privileged communications if legally required
- Buyer's ability to request privileged communications
- Savings clause

Litigation After Closing

Let's assume:

- Purchase agreement assigns the privilege to the seller
- The privileged communications remain on the company's servers (now owned by the buyer) and have not been segregated in any way
- A third party has sued the company and seller's privileged communications are potentially relevant

Ethical Duties Under California Law

The *State Fund* Rule:

- When a lawyer who receives materials that obviously appear to be subject to an attorney-client privilege or otherwise clearly appear to be confidential and privileged and where it is reasonably apparent that the materials were provided or made available through inadvertence, **the lawyer receiving such materials should refrain from examining the materials any more than is essential to ascertain if the materials are privileged, and shall immediately notify the sender that he or she possesses material that appears to be privileged.** The parties may then proceed to resolve the situation by agreement or may resort to the court for guidance with the benefit of protective orders and other judicial intervention as may be justified.

State Compensation Insurance Fund v. WPS Inc., 70 Cal. App. 4th 644, 656-57(1999).

Ethical Duties Under California Law (continued)

Unlike federal rules, *State Fund* duties apply outside of discovery.

California courts applying *State Fund* have explicitly held that materials will be deemed as provided through “inadvertence” when the privilege holder did not intend to disclose them, and unlike the Federal Rules, an attorney's *State Fund* duties are not limited to documents produced through discovery.

- *Doe v. Fitzgerald*, No. CV2010713MWFRAOX, 2022 WL 4596557, at *6 (C.D. Cal. Sept. 21, 2022).

Compare with FRCP 26(b)(5)(B):

- If information *produced in discovery* is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has

Ethical Duties Under California Law (continued)

Will California honor the privilege assignment under Delaware law?

- California has “strong policy considerations favoring the enforcement of freely negotiated choice-of-law clauses.” *Kaul v. Mentor Graphics Corp.*, 2016 WL 6249024, at *6 (N.D. Cal. Oct. 26, 2016), aff’d 730 F. App’x 437 (9th Cir. 2018).
- One federal court—*Sentinel Offender Servs., LLC v. G4S Secure Sols., Inc.*, No. SACV14298JLSJPRX, 2015 WL 13546228 (C.D. Cal. Sept. 3, 2015) — has followed *Great Hill* and enforced a contractual provision assigning privilege to the seller. *Id.* at *2-3.
- It did so even though it recognized that in California, “when one company acquires or takes control of another, attorney-client privilege passes to the purchaser.” *Id.* at *2.

Ethical Duties Under California Law (continued)

So, what do you do?

- Segregate
 - But who does it?
- Inform appropriate person on seller side
 - Who is that?
- Review
 - But who does it?
- Assert the privilege
 - But who does it?

Practical Tips for Managing Privileged Communications

- Consider segregating pre-closing deal-related communications (creating a pre-closing wall)
 - At the outset of the transaction
 - At the closing or near the closing of the transaction
- Consider discussing post-closing use of pre-closing deal-related communications with employees continuing with the surviving corporation (i.e., a continuing general counsel)
- If there are multiple selling stockholders, but no stockholder representative is designated under the purchase agreement, consider appointing one stockholder (or a third party) to serve as the stockholder representative for privilege related issues that may arise post-closing

New Developments in Case Law Governing Advance Notice Bylaws

04

Advance Notice Bylaws

Recent Cases:

Siegel v. Morse, 2025 WL 1101624 (Del. Ch. Apr. 14, 2025) (Cook, V.C.)

Assad v. Chambers, 2025 WL 1554609 (Del. Ch. June 2, 2025) (Cook, V.C.)

- Facial challenges disavowed after *Kellner II*, 320 A.3d 239 (Del. 2024); as-applied challenges not ripe.

Vejseli v. Duffy, 2025 WL 1452842 (Del. Ch. May 21, 2025) (David, V.C.)

- As-applied challenge failed where board fairly rejected non-complying nomination notice.

Advance Notice Bylaws

Agenda:

1. The proper **procedure** and **subject** of bylaws are well established.
2. A stockholder's ability to challenge the **clear-day** adoption or amendment of bylaws is limited by **burden** and **ripeness**.
3. The **cloudy-day** adoption or application of advance notice bylaws is subject to *Unocal* and *Blasius* **enhanced scrutiny**.

Advance Notice Bylaws

1. Procedure & Subject

2. Clear Day (Burden, Ripeness)

3. Cloudy Day (Enh. Scrutiny)

Procedure & Subject:

- “[T]he power to adopt, amend or repeal bylaws shall be in the **stockholders** entitled to vote. ... Notwithstanding the foregoing, any corporation **may**, in its certificate of incorporation, confer the power to adopt, amend or repeal bylaws upon the **directors.**” DGCL § 109(a).
- “The bylaws **may** contain any provision, not inconsistent with law or with the certificate of incorporation, relating to the **business of the corporation**, the **conduct of its affairs**, and its **rights or powers** or the rights or powers of its stockholders, directors, officers or employees.” DGCL § 109(b).

Advance Notice Bylaws

1. Procedure & Subject

2. Clear Day (Burden, Ripeness)

3. Cloudy Day (Enh. Scrutiny)

Procedure & Subject:

- “The bylaws of Delaware corporations have a [procedural, process-oriented nature](#).”
 - *Boilermakers Local 154 Ret. Fund v. Chevron Corp.*, 73 A.3d 934, 951 (Del. Ch. 2013) (upholding forum selection bylaw).
- “Advance notice bylaws assist the board’s [information-gathering](#) and [disclosure functions](#), allowing boards of directors to knowledgeably make recommendations about nominees and ensuring that stockholders cast [well-informed votes](#).”
 - *Kellner II*, 320 A.3d at 257-58 (cleaned up).

Advance Notice Bylaws

1. Procedure & Subject

2. Clear Day (Burden, Ripeness)

3. Cloudy Day (Enh. Scrutiny)

Challenges to Action on a Clear Day:

Siegel v. Morse, 2025 WL 1101624 (Del. Ch. Apr. 14, 2025) (Cook, V.C.)

Assad v. Chambers, 2025 WL 1554609 (Del. Ch. June 2, 2025) (Cook, V.C.)

- **Burden of Facial Challenge**: Under Delaware law, bylaws are [presumed to be valid](#) and interpreted in a manner consistent with the law. To successfully challenge facial validity, a stockholder must demonstrate that the bylaw cannot operate lawfully under [any set of circumstances](#). *Kellner II*, 320 A.3d at 358.
- **Ripeness of As-Applied Challenge**: Delaware law does not permit challenges to bylaws based on hypothetical abuses. Courts will only undertake an equitable review of bylaws if it has a “[genuine, extant controversy](#) involving the adoption, amendment, or application of bylaws.” *Kellner II*, 320 A.3d at 258; *Boilermakers*, 73 A.3d at 949.

Held:

- Challenge unripe where no stockholder seeks to run a proxy contest.
- Absent proxy threat, franchise isn’t “chilled” or impermissibly burdened.
- No “immediate and devastating” financial consequence like poison pill or proxy put.

Advance Notice Bylaws

1. Procedure & Subject

2. Clear Day (Burden, Ripeness)

3. Cloudy Day (Enh. Scrutiny)

Challenges to Action on a Cloudy Day:

A board's adoption or application of advance notice bylaws under the **cloud** of a proxy contest is subject to **enhanced scrutiny** under *Unocal* and *Blasius*.

Vejseli v. Duffy, 2025 WL 1452842 (Del. Ch. May 21, 2025) (David, V.C.)

- **Compliance with Bylaw**: “Were the bylaws clear and unambiguous, did the stockholder’s nomination comply with the bylaws, and did the company interfere with the plaintiff’s attempt to comply[?]”
 - Activists failed to disclose agreements with third parties financing the contest concerning the governance, management, and business of the company if they won.
- **Threat to Corporate Interest**: “The concealment of arrangements and understandings that go to the heart of a nomination effort risks undermining the essential disclosure function of advance notice bylaws. Rejecting a nomination notice for failing to disclose plans or proposals ... promotes the disclosure function of advance notice bylaws.”
- **Proportionate, Non-Preclusive Response**: “Enforcing the Advance Notice Bylaw is a reasonable means of ensuring that stockholders receive material information about director nominees. ... Plaintiffs could have complied with the Advance Notice Bylaw’s disclosure requirements, but they did not.”

GIBSON DUNN