

February 6, 2025

**IPO and Public Company Readiness:
Advance Planning for 2025 and 2026 IPOs**

Privacy and Cybersecurity Considerations

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 **1.0 General credit**
- Participants must submit the form by **Thursday, February 13th** in order to receive CLE credit

[CLE Form Link](#)

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 Speakers



Stephenie Gosnell Handler

Partner | Privacy, Cybersecurity, and
Data Innovation, International Trade

Washington, D.C.

GIBSON DUNN



Harrison Tucker

Partner | Capital Markets, Securities
Regulation and Corporate
Governance

Houston



Sarah Scharf

Associate | Technology Transactions,
Privacy, Cybersecurity and Data
Innovation

Los Angeles

Introduction

01

About this Webcast Series

IPO & Public Company Readiness: Advance Planning for 2025 & 2026

| Date and Time | Program | Registration Link |
|---------------------------------|---|-------------------------------|
| Tuesday, October 15, 2024 | Navigating Executive Compensation and Employee Benefits | Replay |
| Tuesday, November 12, 2024 | Corporate Governance and ESG Considerations | Replay |
| Wednesday, January 15, 2025 | Regulatory Considerations for Public Companies and Their Key Stakeholders | Replay |
| Wednesday, February 6, 2025 | Cybersecurity and Privacy Considerations | Today's Programming |
| Wednesday, February 19, 2025 | Considerations for Private Equity Sponsor-Backed Portfolio Company IPOs | Event Details |
| Wednesday, March 26, 2025 | Structuring and Tax Issues | Event Details |
| Wednesday, April 16, 2025 | Risk Management and Financial Systems | Event Details |
| Wednesday, May 14, 2025 | Key Developments in the UK and Middle East | Event Details |
| Wednesday, June 11, 2025 | Navigating Liability Exposure for Companies and Boards | Event Details |



Agenda

01 Introduction

02 Risk Landscape

03 Key IPO Considerations

04 Calibrating Approach: Context Matters

05 Assessing Privacy and Cybersecurity Maturity

06 Privacy and Cybersecurity Risk Mitigation Pre- and Post-IPO

07 Privacy and Cybersecurity Risk Characterization

Risk Landscape

02

Privacy and Cybersecurity: Risk Exposure

Damage to Business

- Lost Customers/Revenue
- Damage to Reputation/Brand
- Diverted Management and Board Focus
- Direct Response Costs
- Operational Disruptions

Litigation/Regulatory Risks

- Regulatory Investigations (e.g., SEC, FTC, State AGs)
- Class Actions (e.g., BIPA, wiretapping/session replay cookies, tort liability, state consumer protection statutes, fiduciary duties)
- Derivative/Shareholder Actions

Impact to Public Company/Stock Price

- Loss of Investor Confidence
- Negative Financial Impact
- Failure to Meet Guidance

Key IPO Considerations

03

Key IPO Considerations

Disclosure

- Registration statement/prospectus must appropriately disclose material cybersecurity risks with specificity

Underwriters Due Diligence

- Underwriters seeking to establish due diligence defense by conducting reasonable diligence, with increased scrutiny on privacy and cybersecurity issues

Public Attention

- Publicity around IPO/being a public company may attract a higher level of attack/scrutiny

Post-IPO Reporting Obligations

- Consider post-IPO reporting obligations under SEC's new cyber rules and evolving privacy regulations

Compliance and Risk Oversight

- Issuers must put in place compliance and risk oversight policies in accordance with public company practices

Overview of SEC Cybersecurity Disclosure Rules



The SEC's new Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules—adopted by the Commission in July 2023—impose three new reporting obligations on registrants (including public issuers):

Incident Disclosures: Disclose cybersecurity incidents on Form 8-K within four days of determining the incident likely has a material impact (or presents a material risk).

Governance: Disclose cybersecurity governance, oversight, and management.

Risk Factors: Disclose cybersecurity-related risk factors on Form 10-K in Item 1A.

Key Provisions of the Cybersecurity Rules:

Material Incident Disclosure under Item 1.05 on Form 8-K

Cybersecurity Incident:

An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing therein.

- **What is an incident?**
 - The Cybersecurity Rules broadened the definition of “cyber incident” to include “a series of related unauthorized incidents.”
- **What must be disclosed?**
 - Companies should include the material aspects of the **scope, nature, and timing of the incident**, including the reasonably likely material impact to the company's operations and financial position.
 - Disclosure need not contain technical details regarding the nature of the breach, especially not those that would impede the company's response.
- **What is the timing for disclosure?**
 - Companies should make a materiality determination “without unreasonable delay.”
 - Companies should file a Form 8-K announcing the incident within **four days** of determining that the incident is material.
- **Updating disclosures.**
 - If a company discloses a cybersecurity incident and subsequently gains additional information that should be disclosed, it should file an amendment to its 8-K within four days of gaining the required information.

Assessing Materiality for Cybersecurity Incidents: Considering Quantitative and Qualitative Factors

A cybersecurity incident is **material** if “[t]here is a substantial likelihood that a *reasonable shareholder* would *consider it important* in making an investment decision or if it would have “*significantly altered the ‘total mix’ of information* made available.”

The materiality of a cybersecurity incident is a **facts and circumstances determination**, that should consider a **range of qualitative and quantitative factors** informed by the law, facts, professional judgment, and advice of outside counsel.

Illustrative Qualitative Factors:

- Potential harm to a company’s reputation
- Potential harm to vendor or customer relationships
- Potential harm to a company’s competitiveness
- The possibility of litigation or regulatory action
- The nature of the incident (e.g., access vs extraction)

Illustrative Quantitative Factors:

- The amount of data impacted
- Extent of impact to quarterly results financial results or results of operations
- Extent of current or ongoing business interruptions
- Lost revenue
- Remediation costs
- Regulatory fines
- Increased cybersecurity costs
- Lost assets
- Ransom payments
- Potential liabilities to third parties

Overall Disclosure Trends under the New Cybersecurity Rules

There have been ~95 filings made by ~65 companies.

- After **Director Gerding issued a statement in May 2024** clarifying companies should only disclose under Item 1.05 when an incident is determined to be material, there has been a decrease in companies making initial disclosures under Item 1.05.
- **Companies are making multiple disclosures:** an initial disclosure under Item 8.01 before materiality has been determined, followed by an amended 8.01 updating the disclosure, or an Item 1.05 disclosure if materiality has been determined.
- **Recent comment letters and SEC guidance indicate that disclosures that discuss materiality at a high level may not be detailed enough.**
 - The SEC has requested that companies that have disclosed material impact describe all material impacts in future or amended 8-K filings.
 - The SEC has questioned whether companies applied materiality standards under U.S. securities law.
 - The SEC has directly asked for more information from companies.
 - The SEC has made clear that companies should consider both quantitative and qualitative factors in assessing materiality.
- **Delayed Reporting:** Delayed reporting is permitted only under narrow circumstances if the U.S. Attorney General informs the SEC that disclosure would pose a substantial risk to national security or public safety.
 - DOJ has stated that it has delayed disclosure “on a number of occasions” since the rules went into effect.
 - As expected, this exemption is narrow and granted sparingly.
 - There is also a delay available for companies subject to the FCC’s reporting requirements.

Key Provisions of the Cybersecurity Rules: Form 10-K Cybersecurity Disclosures

- Under the new Item 106 of Reg S-K, companies must **discuss their management and oversight of cybersecurity risks in a new section in the Form 10-K**, which is new “Item 1C. Cybersecurity.”
 - This would be right after the Risk Factors section, which is Item 1A, and the Unresolved Staff Comments section, which is Item 1B, in Part I of Form 10-K.
- This includes a requirement to describe their **processes for identifying and managing risks from cyber threats**.
- This has two components:
 - **Risk Management**
 - **Strategy and Governance**

Form 10-K Item 106 Disclosures: Risk Management and Strategy

- **Risk Management and Strategy:** Describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats. Disclosure should address, as applicable:
 - how the processes fit into the company's overall risk management approach;
 - whether the company uses assessors, consultants, auditors, or other third parties in connection with such processes; and
 - whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
- Companies must also describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition, and if so, how.

Form 10-K Item 106 Disclosures: Governance

- Companies must describe the board's oversight of risks from cybersecurity threats, including the applicable committee, if any.
- Companies must also describe management's role in assessing and managing material risks from cybersecurity threats, as well as its role in implementing cybersecurity policies, procedures, and strategies. Disclosure should address, as applicable:
 - whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as is necessary to fully describe the nature of the expertise;
 - the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
 - whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Calibrating Approach: Context Matters

04

Consider the Context & Risk

Consider the Sector

- Is the sector's market an attractive target for criminal or nation state threat actors? The subject of regulatory focus?
- Are there regulatory rules or guidance from self-regulatory bodies regarding cybersecurity or privacy? If not, likely first foray into cyber regulations (SEC)?
- Does the company hold significant amounts of proprietary data? Consumer data?

Consider the Externalities

- How dependent is the company on its supply chain? Resilience in suppliers?
- Does the company rely on emerging technologies (e.g., AI)?

Consider the Data

- What is the nature and extent of data collected and used? Data-centric v. non-data focused?
- Engage with individual customers? Youth customers?
 - Include personal data? Sensitive personal data?

Consider the Jurisdiction

- Worldwide business activities? Subsidiaries? Employee locations?
- Potentially applicable laws and their consequences inform approach
 - E.g., EU/UK GDPR (with penalties up to 4% of worldwide turnover)

Assessing Privacy and Cybersecurity Maturity

05

Pre-IPO Privacy and Cybersecurity Maturity Assessment

General:

- Digging into company's privacy and cybersecurity maturity pre-IPO is essential to manage risk and inform disclosures

Privacy:

- Privacy maturity is variable and depends on context and industry (e.g., data brokers versus widget manufacturer)
 - E.g., privacy "mature" but biometrics company → higher risk
 - E.g., privacy "immature" but widget manufacturer → lower risk
- Privacy IPO risk management is not just about "fixing" privacy gaps, but informing disclosures

Cybersecurity:

- While cybersecurity IPO risk management is also context-dependent, it is tied to "reasonableness" and sector-specific regulatory expectations as well as SEC requirements

Privacy Maturity Considerations

Personal Data Inventory and Mapping

- What types of personal data do we process?
- What types of personal data do we store? Where? Is it encrypted?
- Does it include sensitive personal data? Youth personal data?

Nature of Processing

- For what purposes do we process personal data?
- Do we sell/share personal data?
- What are the sources of personal data?

Assess Geographic Scope

- Where do we process personal data?
- Where is data stored?
- Does the company transfer or receive any data or information across borders?

Existing Privacy Compliance

- What privacy regulations is company consider itself subject to? What are the company's related compliance activities to date?
- Has the company received any regulatory inquiries and/or privacy complaints?
- What public-facing privacy commitments have already been made?
- Does the company maintain a public-facing privacy policy?
- Does the company have contractual privacy obligations with its vendors?

Cybersecurity Maturity Considerations

Existing Cyber Infrastructure

- Standards for what is deemed “reasonable” in the cybersecurity arena continue to evolve.
- What administrative, technical, and organizational measures have been taken to ensure IT and data security?
- Has a formal program has been established in writing? Do company’s policies, procedures, and corporate governance adhere to industry security standards or certifications (e.g., ISO, NIST, SOC2)?
 - Do they demonstrate that the company takes cybersecurity seriously? Are they commensurate with the risk?
- Have outside advisors have been consulted? Have any third-party audits been conducted?
- Do we have an incident response plan? Do we follow it? Test it?

Prior Security Incidents

- Security incidents are common; it is likely that any company of sufficient size will have experienced at least some minor incidents.
- If the company has been breached or suffered a service disruption before, how quickly did company discover the intrusion?
- How did company respond, including securing the breach, remediation efforts, notice to consumers, etc.?
- Were the company’s disclosures adequate?
- Subject of a regulatory inquiry?

Third-Party Risk

- What functions does the target outsource? Do vendors or partners have access to Company data or systems?
- Does the company evaluate such third parties’ security infrastructure and policies?

Key Watchouts

Privacy

- Lack of awareness of applicability of privacy laws (e.g., CCPA/CPRA) and requirements and limitation of exemptions (e.g., B2B/employment); sector-specific obligations
- Insufficient processes to respond to consumer requests, required contract provisions, disclosure requirements
- Processing of sensitive data (e.g., health data, biometrics, youth) + lack of consent/disclosure and/or processing of data from high-risk jurisdictions without adequate privacy maturity (e.g., EU, UK)
- Varying levels of online policy development: no policy, outdated policy, only online policy, or online policies do not match data collection and processing practices
- Lack of retention schedules and/or insufficient attention to data minimization

Cybersecurity

- Lack of awareness of applicability and requirements of sector-specific security laws (e.g., HIPAA, GLBA, DFARS, COPPA, BIPA, CAN-SPAM, TCPA, FCRA, etc.)
- Insufficient safeguards to protect personal/proprietary information and network
- Lack of security policies or mere placeholder policies; insufficient incident preparedness, business continuity/disaster recovery plans, and vendor management
- Incident history, issues with response times, security policies not addressing notification requirements (including deadlines)
- Past or ongoing claims/investigations

Privacy and Cybersecurity Risk Mitigation Pre- and Post-IPO

06

Privacy Risk Management

Gap Analysis

- Prepare legal assessment of applicable privacy regulations
- Conduct gap analysis of regulatory compliance measures

Update Internal and External Policies, As Needed

- Update privacy policy and related disclosures
- Establish processes for data subject requests

Establish Owners

- Assign designated owners of privacy compliance measures

Data Hygiene

- Establish data hygiene practices, including data minimization and data retention policies
- Purge data that is no longer necessary to business

Form 10-K Disclosures: Privacy Considerations

- Given the dynamic global regulatory and legal environment, companies will need to stay on top of evolving regulatory obligations and legal landscape to continually update their risk factors and related disclosures
 - Not a “one and done” exercise; the rapid proliferation of data protection laws globally requires ongoing monitoring
- Moreover, as a company grows and expands into new markets, engages overseas vendors, hires employees in new countries, or transfers data cross borders, new privacy regimes may come into play

Task List: Key Action Items Pre-IPO

- ✓ Legal assessment of applicable privacy and cybersecurity regulations
- ✓ Gap analysis of regulatory compliance measures
- ✓ Designated owners of privacy and cybersecurity compliance measures
- ✓ Tailored and tested IRP that incorporates legal function
- ✓ Preparation of a Materiality Assessment Protocol or Framework (MAP or MAF)
- ✓ Ensure that cybersecurity processes and governance align with SEC expectations
- ✓ Publication and/or update of public facing privacy policy

Impact of the SEC Cybersecurity Rules: Practical Application

Key Areas of Focus

Key Areas of Focus:

1. Ensuring that cybersecurity incident response playbooks facilitate appropriate escalation and reporting.
2. Revisiting cybersecurity processes and governance to align with the expectations expressed in the SEC's final rules.
3. Drafting and balancing of competing interests for Form 10-K cybersecurity disclosures.
4. Preparing for an incident: effective cybersecurity incident response and materiality assessments will require advance planning.
5. Responding to a cybersecurity incident.
6. Making a disclosure on Form 8-K in connection with a cybersecurity incident.
7. Preparing for an SEC investigation.

Impact of the Adopted Rule: Practical Application

Review Cybersecurity Incident Response Playbook, Materiality Assessment Framework, Escalation Protocols

1. Ensure that cybersecurity incident response playbooks will facilitate appropriate escalation and reporting:

- Disclosure controls and procedures should provide for effective communication between the relevant internal teams.
- Companies should ensure that disclosure controls and procedures reflect the relevant materiality considerations, including inputs to consider potential reputational harm and damage to customer and vendor relationships.
- Consideration should be given to documenting the materiality analysis and the reasonableness of the time that it takes to assess materiality.
 - Given the accelerated timeline for disclosure of cybersecurity incidents on Form 8-K within four business days of determining the incident is material, Companies should evaluate current evaluation and response procedures to ensure that a materiality determination can be made, and that a timely disclosure can be filed.

Practical Tip: Many IRPs are still primarily tailored to technical response—the 2023 cyber rules are requiring a substantive rethink for a number of public companies.

Impact of the Adopted Rule on Companies: Practical Application

Assess Processes for Managing Cybersecurity Risk

2. Companies may wish to revisit their cybersecurity processes and governance to align with the expectations expressed in the SEC's final rules:

- To avoid disclosing processes that lack features addressed in the final rule or that appear less robust than peers, companies should assess processes that will be disclosed.
- Specifically, companies should be aware of the need to describe engagement of third parties in connection with the risk management process, any processes to oversee and identify risks associated with use of third-party service providers, and the delegation of responsibility for cybersecurity risks between the board and management.

Consider incorporating AI utilization and technological developments in the assessment of cybersecurity risk.

Impact of the Adopted Rule on Companies: Practical Application

Careful Drafting of Disclosures and Coordination of New Form 10-K Disclosures with Existing Disclosures

3. Cybersecurity disclosures for Form 10-K will require careful drafting and balancing of competing interests:

- While some of the information now required to be disclosed has historically been disclosed to regulatory agencies and affected customers, the need to publicly disclose the information will subject such information to much greater scrutiny and potential liability as a result of possible regulatory enforcement or litigation.
- These disclosures will require careful drafting to balance the obligation to timely disclose material information (without material omission) while avoiding the unintentional exposure of weaknesses in a company's cybersecurity profile that could be further exploited by malicious actors.

Ongoing Considerations: Review existing disclosures when drafting new discussions for Form 10-K to maintain consistency with past public statements regarding cybersecurity governance and processes and to assess how those disclosures may be enhanced or revised going forward.

Impact of the Adopted Rule on Companies: Practical Application

**Materiality
determinations do not
happen in a vacuum:
preparation is key.**

4. Preparing for an incident – effective cybersecurity incident response and materiality assessments will require advance planning:

- Create and maintain **documented incident response policies and procedures**, including an incident response plan (IRP), playbooks, contact lists, escalation procedures, and preferred vendor lists.
- Ensure **roles and responsibilities are clearly defined** (e.g., cybersecurity incident response team, incident response leader, legal, outside counsel, digital forensics firm, crisis communications firm, disclosure committee, etc.).
- Develop a **materiality assessment framework** that sets forth procedures to support the assessment of whether a cybersecurity incident is material.
- Regularly conduct **tabletop exercises to test response** and proactively make improvements to policies and procedures, as necessary. Note, it is critical that internal policies employed during an incident are drafted to be user-friendly.

Impact of the Adopted Rule on Companies: Practical Application

Action internal policies and procedures to help ensure a more cohesive and organized crisis response process.

5. Responding to a cybersecurity incident:

- Ensure that discussions about the cybersecurity incident and its materiality are **conducted under privilege and kept confidential**.
 - All communications regarding materiality should include a member of the Company's legal team and outside counsel. Written communications should be marked with "Privileged and Confidential—Prepared at the Direction of Counsel" headers.
 - Engagement of and communications with incident response vendors must be undertaken at the direction of and involve outside counsel.
- Establish an **out-of-band communications method** to be deployed if needed.
- Ensure **investigative activities are documented** by outside counsel and the Company's legal team.
- The materiality determination made by the disclosure committee should be documented by legal in a manner that demonstrates that the **determination was made in accordance with the materiality assessment framework**.
- Ensure that the **materiality assessment itself is conducted under legal privilege**; a non-privileged summary may be maintained for audit purposes.
- Conduct post-incident lessons learned exercises to enhance incident response preparedness materials.

Impact of the Adopted Rule on Companies: Practical Application

Be accurate and be prepared for the SEC to request more information.

6. Making a disclosure on Form 8-K in connection with a cybersecurity incident:

- **Exercise caution** not only in drafting initial 8-K disclosures, cybersecurity risk factors, and the new Item 106, but **also in any public statements regarding the company's cybersecurity practices.**
- **Confirm that assertions made or controls discussed do in fact presently apply to the full environment disclosed.** Any such disclosures or statements should be reviewed by both legal and cybersecurity leadership to confirm accuracy.
- **Materiality assessment procedures should consider whether the incident is part of a series of related incidents that are immaterial individually, but when viewed in the aggregate have a more significant impact.**
- Disclosures of incidents on Form 8-K should be consistent with the full set of facts known at the time.
 - Disclosures should make clear if there is a known connection to prior attacks.
 - Disclosures about alignment with recognized industry cybersecurity standards should be accurate and note any control gaps or other limitations.
- Be prepared to provide sufficient detail about the material impacts and materiality assessment process.

Impact of the Adopted Rule on Companies: Practical Application

Preparing for an SEC Investigation

7. Preparing for an SEC Investigation:

What might an SEC investigation reasonably focus on?

- There is no way to predict which cybersecurity incidents will become the focus of future SEC enforcement investigations. However, companies can reasonably expect that an SEC inquiry will follow either:
 - The disclosure of a cybersecurity incident, or
 - Non-disclosure of a cybersecurity incident the SEC believes may have impacted the company, such as after a publicly reported incident believed to impact a range of entities.
- The SEC will also likely focus on the procedures and documentation associated with materiality determinations.

What might the SEC request?

- Inputs and substance of materiality determinations;
- “Worksheets” or outputs of materiality determinations; and
- Information and work product from investigations conducted following an incident, even when such investigations occur at the direction of counsel.
- Information regarding whether and how the company’s “disclosure decision-makers” were provided with information regarding a cybersecurity incident.

Impact of the Adopted Rule on Companies: Practical Application

Preparing for an SEC Investigation

7. Preparing for an SEC Investigation (Continued):

How can companies best prepare?

- **Companies should create a process for integrating cybersecurity and disclosure functions.**
 - Companies should institute processes for: (1) determining which cybersecurity incidents need to be escalated to the company’s “disclosure decision-makers”; and (2) ensuring that the right information is provided in a timely manner.
 - The best defense remains implementing and adhering to a well-documented, tightly reasoned process grounded in actual legal standards.
- **When investigating a cybersecurity incident, companies should ensure processes are in place to protect privilege.**
 - Companies should institute thoughtful privilege protocols to determine what information is disclosed to whom.
 - When establishing engagements with incident response providers, such as forensic investigators, careful consideration should be given towards establishing and protecting appropriate privileges.

Privacy and Cybersecurity Risk Characterization

07

Best Practices

Preparing for rigorous privacy and cybersecurity diligence from underwriters, investors, and regulators during the IPO process

- Assemble final privacy and cybersecurity policies as revised
- Designate privacy and cybersecurity leader who will be on point for substantive responses
- Assemble post-mortem of any substantive data breach, with lessons learned and summary of response taken
- Assemble summary of any regulatory inquiry and/or third-party complaint regarding company's privacy or cybersecurity practices, including final resolution; if not yet resolved, ensure plan for response prepared

Privacy and cybersecurity disclosures will require careful drafting and balancing of competing interests

- The need to publicly disclose will subject responses to greater scrutiny and potential liability as a result of possible regulatory enforcement or litigation
- Must balance the obligation to timely disclose material information (without material omission) while avoiding the unintentional exposure of weaknesses in a company's privacy and cybersecurity profile that could be further exploited by malicious actors

Speaker Bios

08



1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.955.8510

shandler@gibsondunn.com

Stephenie Gosnell Handler

Partner / Washington, D.C.

Stephenie Gosnell Handler is a partner in Gibson Dunn’s Washington, D.C. office. She advises clients on complex legal, regulatory, and compliance issues relating to cybersecurity, data, and technology matters. Stephenie advises clients across the full lifecycle, from preparedness to response to investigations and enforcement actions. 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. In 2024, *Lawdragon* named Stephenie to their “500 Leading Global Cyber Lawyers” and “100 Leading AI and Legal Tech Advisors” list. Stephenie serves as Chair of the Future of Privacy Forum’s Privacy and Cybersecurity Expert Group, and has taught law school classes on managing privacy and cybersecurity risks.

Stephenie returned to Gibson Dunn as a partner of the Washington, D.C. office after serving as Director of Cybersecurity Strategy and Digital Acceleration at McKinsey & Company. In this role, she led development of the firm’s cybersecurity strategy and advised senior leadership on public policy and geopolitical trends relating to cybersecurity, technology, and data. Stephenie managed a team of experienced professionals responsible for the firm’s cybersecurity strategic initiatives, cybersecurity standards and certifications program, lifecycle governance initiatives, data analytics and optimization, and digital acceleration efforts across the cyber domain. She previously led McKinsey’s in-house cybersecurity legal team, where she advised on diverse global cybersecurity and technology matters, including strategic legal issues, data localization, regulatory compliance, risk management, governance, preparedness, and response. Stephenie frequently advised at the intersection of cybersecurity, technology, and data and export control and sanctions requirements.

Stephenie earned her J.D. from Stanford University in 2011. She earned her M.A. from Georgetown University and her B.S. from the U.S. Naval Academy, both in 2001.

Stephenie’s full biography can be viewed [here](#).

EDUCATION

Stanford University
Juris Doctor

U.S. Naval Academy
Bachelor of Science

Georgetown University
Master of Arts



Harrison Tucker

Partner / Houston

811 Main Street, Suite 3000, Houston, TX 77002-6117

+1 346.718.6643

htucker@gibsondunn.com

Harrison Tucker is a partner in the Houston office of Gibson, Dunn & Crutcher, where he currently practices with the firm's Capital Markets and Securities Regulation and Corporate Governance practice groups. He regularly represents public and private businesses in a broad range of corporate and securities matters and issuers and investment banking firms in both equity and debt offerings, including Rule 144A offerings. His practice also includes general corporate concerns, including Exchange Act reporting, stock exchange compliance, corporate governance and beneficial ownership reporting matters. In addition, he works closely with the Gibson Dunn bankruptcy and restructuring team, advising on applicable securities laws issues.

Harrison received his J.D. from the University of Houston Law Center in 2008, where he was elected to the Order of the Coif and Order of Barons. While in law school, he served as a Member of the Houston Law Review. Prior to law school, he graduated from Texas A&M University in 2005, where he received his B.A. in history and was elected to Phi Beta Kappa.

Harrison maintains an active pro bono practice. For example, he has represented U.S. military veterans through the National Veterans Legal Service Program in seeking discharge upgrades and enhanced disability compensation. He is also active in the Houston Volunteers Lawyers program sponsored by the Houston Bar Association.

Harrison's full biography can be viewed [here](#).

EDUCATION

University of Houston
Juris Doctor

Texas A&M University
Bachelor of Arts

Sarah Scharf

Associate Attorney / Los Angeles

Sarah Scharf is an associate in the Los Angeles office of Gibson, Dunn & Crutcher. She is a key member of the firm's Technology Transactions and Privacy, Cybersecurity and Data Innovation practice groups. Sarah has extensive experience advising clients across a range of industries on privacy, cybersecurity, artificial intelligence (AI), information technology (IT), and intellectual property (IP) issues, and focuses on complex transactional representations, strategic product counseling, regulatory compliance counseling, and privacy and AI program development.

Sarah regularly advises clients on privacy, cybersecurity, and AI considerations, with particular expertise in compliance with the California Consumer Privacy Act (CCPA) and other comprehensive state privacy laws, the Gramm-Leach-Bliley Act (GLBA), and the European Union's General Data Protection Regulation (GDPR). Her experience includes drafting privacy policies, just-in-time notices, consents and acknowledgements, data processing addenda, risk assessments, consumer request procedures, and incident response plans, as well as AI, privacy and cybersecurity-related stock exchange disclosures. She also routinely counsels clients on the development, acquisition, licensing and exploitation of intellectual property, as well as commercial transactions. Additionally, Sarah advises public and private companies and financial sponsors on privacy, cybersecurity, AI, IT, and IP issues in connection with corporate transactions, including venture and private equity representations, mergers and acquisitions, carveouts, leveraged buy-outs, and distressed lending. Her experience includes conducting due diligence; drafting and negotiating privacy, cybersecurity, AI, IT, and IP-related representations, warranties, covenants and indemnities, complex transition services agreements, and transitional trademark licensing arrangements; counseling regarding privacy, cybersecurity, AI, IT, and IP-related risks and mitigation strategies; and implementing post-acquisition privacy compliance programs.

Prior to joining Gibson Dunn, Sarah clerked for Justice Daphne Barak-Erez of the Supreme Court of Israel. Sarah earned her J.D. and LL.M. in Comparative and International Law from Duke University School of Law in 2019. In 2016, Sarah graduated *magna cum laude* from Columbia University with a Bachelor of Arts degree in Political Science. Simultaneously, she earned a Bachelor of Arts degree in Jewish Gender and Women's Studies from the Jewish Theological Seminary, graduating *cum laude*.

Sarah is a Certified Information Privacy Professional—United States and Europe (CIPP/US/E).

Sarah's full biography can be viewed [here](#).



EDUCATION

Duke University
Juris Doctor

Duke University
Master of Laws (LL.M.)

Columbia University
Bachelor of Arts

Jewish Theological Seminary of America
Bachelor of Arts

The background features a series of white, wavy, concentric lines that create a sense of depth and movement. These lines are set against a smooth, light gray gradient that transitions from a slightly darker shade on the left to a lighter shade on the right. The overall effect is clean, modern, and minimalist.

GIBSON DUNN