Navigating the Risks in the Cyber and Emerging Technology Compliance Landscape

Jennie Wang VonCannon, Crowell & Moring

Evan Wolff, Crowell & Moring

Jay Shah, Honeywell International Inc.

Crowell

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Agenda

Enforcement Efforts

- DOJ Civil-Cyber Fraud Initiative
- SEC Cyber Disclosure Rules

CMMC

Generative AI 101

Utilizing AI in Providing Products & Services to the Federal Government

DOJ Civil-Cyber Fraud Initiative

DOJ Civil-Cyber-Fraud Initiative

In October 2021, DOJ announced the Civil Cyber-Fraud Initiative

- Will utilize False Claims Act to pursue cybersecurity related noncompliance by government contractors and grant recipients.

Three cybersecurity failures that are prime for enforcement:

Failure to meet specific contract terms → Misrepresentation of security controls and practices → Failure to timely report suspected breaches

Potential Theories of Liability for Cybersecurity Noncompliance

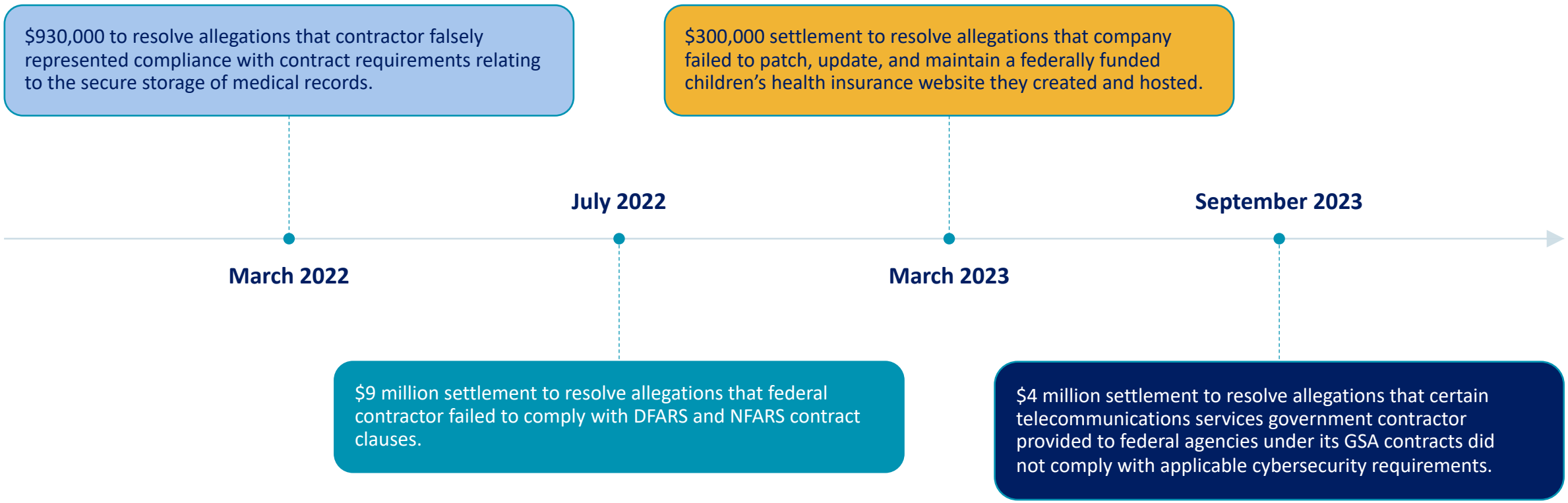
Fraudulent Inducement / Promissory Fraud

Liability attaches to **each claim** submitted to the government under a contract, when the contract was originally obtained through **false statements** or **fraudulent conduct**.

False Certification

- **Express** certification
- **Implicit** certification

False Claims Act Cyber-Related Settlements



Potential False Claims Act Liability under CMMC

Affirmations

"A senior official from the prime contractor and any applicable subcontractor will be ***required to affirm continuing compliance with the specified security requirements*** after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS."

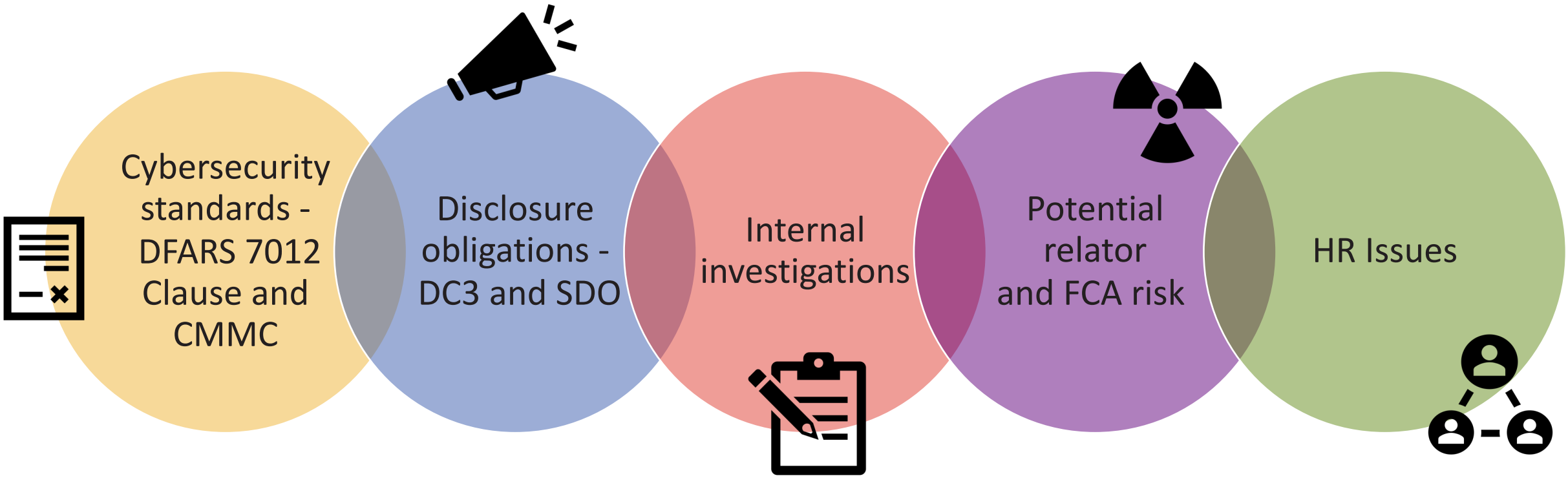
Potential predicates for investigation/liability:

- CMMC status revocation
- Inaccurate Self-Assessments
- Failure to provide C3PAO or Government with accurate information for Certification Assessments
- Failure to closeout POA&Ms in 180 days

Scenario

- CLO Company (CLO Co.) has multiple contracts with DoD to make complex weapon systems.
  - They recently hired a new CISO who reviewed their current System Security Plan and found multiple areas of deficiency
  - They brought in outside counsel to conduct a privileged investigation
  - For the past several years, CLO Co. has been conducting pen tests as a part of their security program; these have been conducted by the previous CISO, who left on uncertain terms
  - In preparation for their CMMC audit, they engaged a C3PAO to conduct an assessment of their controls and found that they have many undocumented POA&Ms
  - They have received a CID from DOJ

Issues


Cybersecurity standards - DFARS 7012 Clause and CMMC
Disclosure obligations - DC3 and SDO
Internal investigations
Potential relator and FCA risk
HR Issues

SEC Cybersecurity Disclosure Rules

SEC Cybersecurity Disclosure Rules

Finalized July 2023; went into effect (for most) December 2023

Applies to public companies that are subject to SEC reporting requirements

Focused on cybersecurity risk management, strategy, governance, and incidents

Required Disclosures:

- Cybersecurity Incidents within Four Days of Materiality Determination
- "Processes," But Not Cybersecurity Procedures

National Security Delay Exception may have limited impact

- Applies only if the U.S. Attorney General notifies the SEC in writing that the disclosure poses a substantial risk to national security or public safety

New Disclosure Requirements – Form 8K

When there is a **"cybersecurity incident"** that the company determines is **"material"** the company must:

- Disclose the material aspects of the nature, scope, and timing of the incident
- Disclose the material impact or reasonably likely material impact on the company of the incident, including such impact on the financial condition and company operations

The materiality determination must be made **"without unreasonable delay"**

New Disclosure Requirements – Form 10K

Company must describe its **cyber risk management and strategy**. This must include the company's

- Processes for the assessment, identification, and management of material cyber risks
- Whether any cyber risks have materially affected or are reasonably likely to affect business strategy, finances, or operations

Company must describe **governance regarding cyber risks**. This must include the company's

- Board oversight of cyber risks, and reporting to the board
- Management's control in assessment and managing material cyber risks
- Management's cyber expertise and experience
- Processes for preventing, monitoring, detecting, and mitigating incidents

Scenario

- GC Corp. is the victim of a cyber incident, which is based on a series of social engineering and phishing campaigns that results in a threat actor getting credentials and causing unknown data loss:
  - After a few days, GC Corp is notified by the local FBI office regarding potential threat actor activity; they request information from GC Corp
  - As a part of the incident response, GC Corp hires a forensic vendor who initially identifies the threat actor as a PRC-based organization
  - GC Corp has an incident playbook but could not find it for the first few days of the incident

SEC Report Analysis

Timing

Nature of Incident

Financial Impact

Coordination with law enforcement

Threat actor and related factors

Decision-making process – who decides?

Use of third parties

External factors

Generative AI 101

Generative AI Key Terms

ChatGPT is a "chatbot" application...

Built on **GPT-3.5, which is a type of...**

Large Language Model (LLM) developed by...

OpenAI, a developer creating various forms of...

Generative AI (GAI or GenAI)

TL;DR:
LLMs are highly skilled "sente nce finishers"

GAI is AI that can create new content

Large Language Models (LLMs) are just one type of GAI

GPT is one type of LLM and the underlying framework of...

The application ChatGPT

Generative AI's Limitations and Risks

Garbage In, Garbage Out

- Bias
- Hallucinations / Inaccuracy
- Oversimplification

Data Security

- Legal Questions
- Waiver of Privilege
- Confidentiality

Lack of Transparency

AI & IP Concerns

Key Questions

- Is AI-generated content copyrightable or patentable?
- What be used as inputs?
- Licensing schemes?
- Disclosure requirements?
- Recordkeeping requirements?
- Labelling requirements?
- Can AI unlearn?
- Attribution?
- Infringement?

Key Challenges

- Evolving and (potentially conflicting) agency instruction
- Lack of established case law
- Lack of understanding of emerging field
- Ensuring client advice aligns with evolving landscape
- Navigating IP, privacy, ethical, and reliability issues
- Lack of clear guidance

Privacy Concerns in an AI-Focused World

Data storage, usage, and access concerns

- Need for transparency
- Need for regulation

AI's ability to infer personal and sensitive data

Deepfakes

Rights of Publicity

Notable Proposed Legislation and Regulations for 2024

The Biden Administration's Approach to AI

MAY 04, 2023

FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety

BRIEFING ROOM › STATEMENTS AND RELEASES

MAY 23, 2023

FACT SHEET: Biden-Harris Administration Takes New Steps to Advance Responsible Artificial Intelligence Research, Development, and Deployment

BRIEFING ROOM › STATEMENTS AND RELEASES

JULY 21, 2023

FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI

BRIEFING ROOM › STATEMENTS AND RELEASES

SEPTEMBER 12, 2023

FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI

BRIEFING ROOM › STATEMENTS AND RELEASES

BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE

AI.GOV

Examples of Existing Regulatory Frameworks Impacting AI

Housing and Urban Development (HUD)

Algorithmic Bias in Housing

Food and Drug Administration (FDA)

AI Medical Devices

Consumer Financial Protection Bureau (CFPB)

AI in Consumer Financial Products

Federal Trade Commission (FTC)

Advertising Claims

Consumer Product Safety Commission (CPSC)

Consumer Products

Department of Transportation (DOT)

Self-Driving Cars

U.S. Federal Proposed Legislation

Targeted Legislation / Popular Proposed Themes

Deepfakes

National Security

Consumer Protection

50+

AI-Related Bills Introduced In 118th Congress

Coordinating Federal Agencies' AI Use

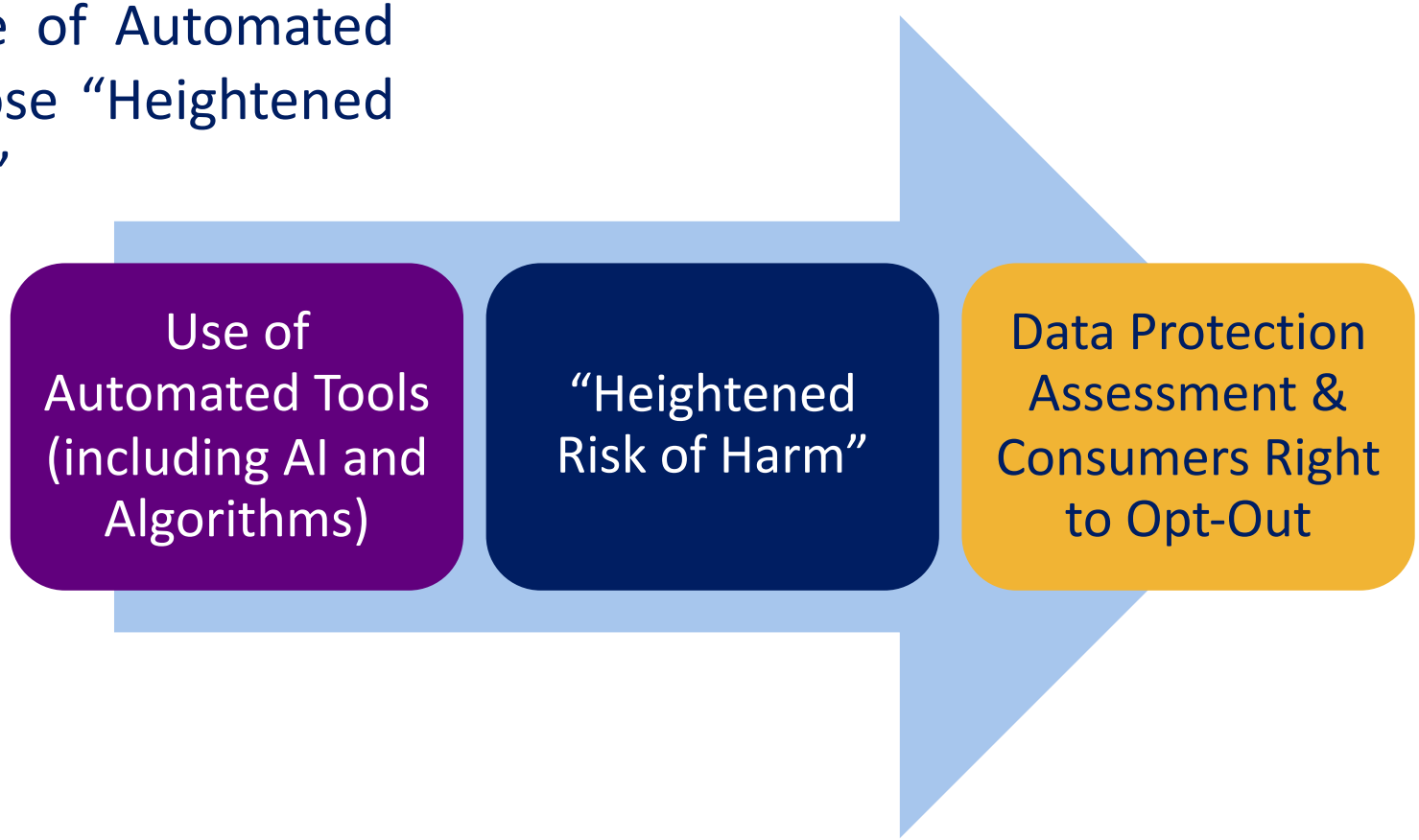
Disclosure

Workforce

AI R&D Leadership and Oversight

U.S. State Developments: The Status of State AI Laws in 2023-24

Existing State Privacy Laws Regulate Use of Automated Tools that Pose "Heightened Risk of Harm"



European Union – the Artificial Intelligence Act (AI Act)

Why

- Need for comprehensive AI regulation – safety of AI systems (especially in high-impact sectors)
- Geopolitical interest of the EU

Goals

- Improve functioning of the internal market
- Promote "human central and trustworthy AI"
- Ensure a high level of protection of health, safety, fundamental rights (including democracy, rule of law and environment)
- Support innovation (legal certainty and facilitating investment)
- Governance and effective enforcement

Approach

- Risk-based

Scenario

- XYZ Corp. is considering licensing an AI product designed to enhance HR procedures and assist in making key employment decisions
  - After an extensive search, XYZ Corp. identifies a promising AI software vendor, but compliance concerns arise
  - The legal and HR teams begin assessing the AI software against a backdrop of regulatory and ethical considerations
  - Negotiations reveal unexpected integration and transparency issues
  - Final preparations prompt questions about training and cultural fit

Key Takeaways re AI

Precautions and Risks

Some Solutions to GAI Risks – Contractual Limitations

Liability Limitations

Indemnifications

Warranties

Confidentiality

AI-specific provisions

Contract termination due to AI-related violation

Contact Information

Jennie Wang VonCannon

Partner, Crowell & Moring
jvoncannon@crowell.com
+1.213.310.7984

Jennie Wang VonCannon is a Partner at Crowell & Moring in the firm's Chambers USA-ranked Privacy and Cybersecurity Group and the White Collar & Regulatory Enforcement Group. She is a technology trial lawyer and advisor with a proven track record of success in both the courtroom and the boardroom — with over two decades of experience and deep understanding of corporate defense in both criminal and civil contexts, cybersecurity, and intellectual property matters. She is a trained AI Governance Professional who can assist clients with creating or updating compliance programs regarding AI (both generative and otherwise). She served for over eleven years as a federal prosecutor, culminating in her selection to serve with distinction as the Deputy Chief of the Cyber and Intellectual Property Crimes Section of the National Security Division of the U.S. Attorney's Office for the Central District of California.

Evan Wolff

Partner, Crowell & Moring
ewolff@crowell.com
+1.202.624.2615

Evan Wolff is a Partner at Crowell & Moring, where he is co-chair of the firm's Chambers USA-ranked Privacy and Cybersecurity Group and a member of the Government Contracts Group. Evan has a national reputation for his deep technical background and understanding of complex cybersecurity legal and policy issues. Calling upon his experiences as a scientist, program manager, and lawyer, Evan takes an innovative approach to developing blended legal, technical, and governance mechanisms to prepare companies with rapid and comprehensive responses to rapidly evolving cybersecurity risks and threats.

Jay Shah

General Counsel of Securities, Corporate Finance, and Global Cybersecurity, Honeywell International
Jay.Shah2@Honeywell.com
+1.770.519.0802

Jay Shah is General Counsel of Securities, Corporate Finance and Global Cybersecurity at Honeywell International Inc. Prior to his current role, Jay was General Counsel of Honeywell's software and Industrial Internet of Things business that leverages the power of software, cloud, mobile, data & analytics and IIoT. He has over 17 years of top-tier law firm and in-house experience advising executive level management at both public and private companies and is a frequent speaker and has published numerous articles in leading legal publications, including The Corporate Counselor, Bloomberg Banking & Finance Law Reports and the ABA Journal.

crowell.com