September 2021

ECONOMIC ESPIONAGE & THEFT OF INTELLECTUAL PROPERTY

GIBSON DUNN

Today's Presenters

Zainab N. Ahmad
New York
zahmad@gibsondunn.com
TEL:+1 212.351.2609

David P. Burns
Washington, D.C.
dburns@gibsondunn.com
TEL:+1 202.887.3786

Robert K. Hur
Washington, D.C.
rhur@gibsondunn.com
TEL:+1 202.887.3674

H. Mark Lyon
Palo Alto
mlyon@gibsondunn.com
TEL:+1 650.849.5307

Alexander H. Southwell
New York
asouthwell@gibsondunn.com
TEL:+1 212.351.3981

The Global Scale of Intellectual Property Theft

- **The U.S. Department of Commerce** estimates that IP-intensive industries support at least 45 million U.S. jobs and contribute more than $6 trillion dollars or over 38% of U.S. GDP.

- **Yet, intellectual property is subject to a tremendous level of theft:** the Department of Commerce estimates the domestic value of stolen intellectual property to be at **least $200 billion annually,** with other sources suggesting losses could be **closer $600 billion.**

- DOJ's Task Force on Intellectual Property recognizes the "rise in intellectual property crime in the United States and abroad" as a significant economic and public safety threat.

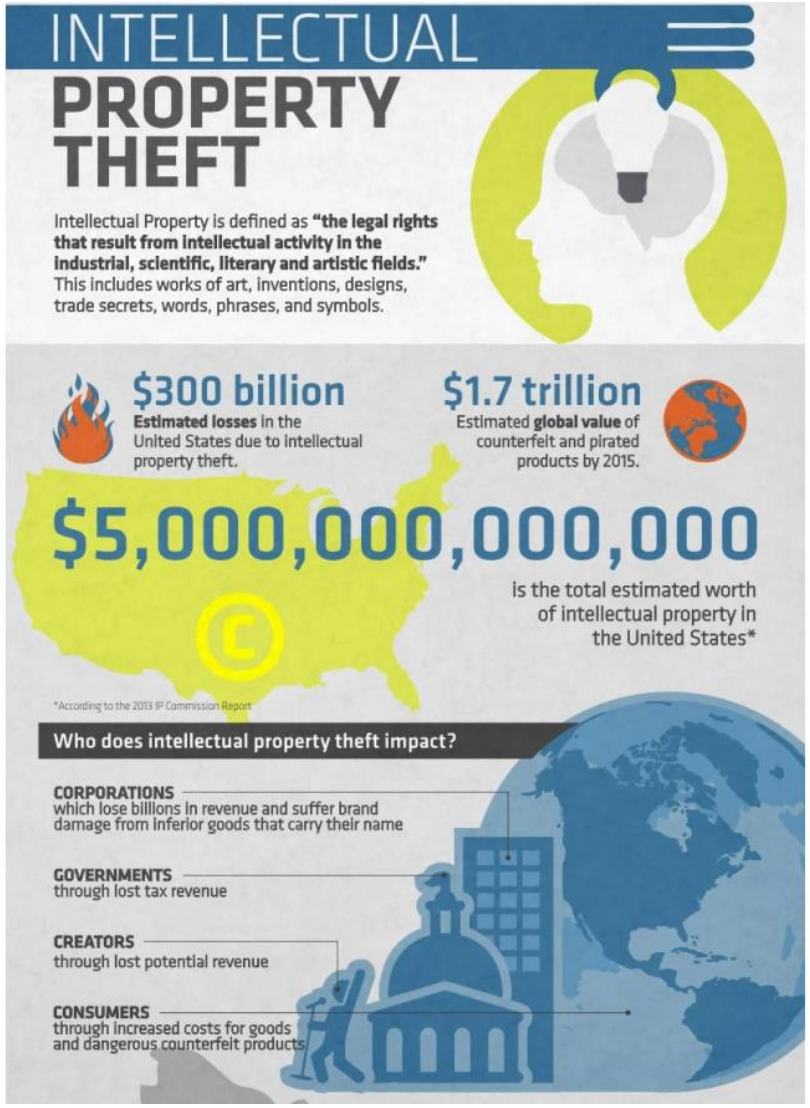

Image Source: *i-Sight.*

U.S. Patent and Trademark Office, INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: 2016 UPDATE; IP Commission, FOREIGN SOURCES RESPONSIBLE FOR MOST IP THEFT, 2017; U.S. Department of Justice, Intellectual property Task Force.

Economic Espionage and Theft of Intellectual Property: Criminal Penalties

- **18 U.S.C. § 1831 ("Economic Espionage Act")** Prohibits the theft of trade secrets, "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."
- **18 U.S.C. § 1832 ("Theft of Trade Secrets")** offers similar prohibitions more generally regarding theft of trade secrets for "the economic benefit of anyone other than the owner."

Economic Espionage

- *Corporations*: Greater of—
  - USD 10 million fine *or*
  - Three times the Value of the Trade Secret including expenses for research and design and other costs of reproducing the trade secret.
- *Individuals*:
  - Up to 15 years imprisonment, *and/or*
  - USD 5 million fine.

Trade Secret Theft

- *Corporations*:
  - USD 5 million fine *or*
  - Three times the value of the stolen trade secret, including expenses for research and design and other costs of reproducing the trade secret.
- *Individuals*:
  - Up to 10 years imprisonment *and* a fine.

The China Counterintelligence Threat

- The Chinese Government is engaging not only in traditional espionage, but also in a whole range of efforts to misappropriate trade secrets from private industry in the U.S. (and in other Western countries) for commercial and military application.
- The effort is on an unimaginable scale.
  - "Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history."
  - "All 56 FBI Field Offices have open China-related CI investigations. "
  - "There is a new China-related counterintelligence threat every 10 hours."
  - "Over the past decade, economic espionage cases with a link to China grew by 1300%."

– FBI Director Wray Remarks at the Hudson Institute, July 7, 2020

- The threat is multi-faceted, and includes:
  - Traditional Spying
  - Cyber Intrusions
  - Co-opting Insiders
  - Non-traditional Collectors

*"China is engaging in a global campaign to **'rob, replicate, and replace'** non-Chinese companies in the global marketplace ."*

– AAG John C. Demers, July 21, 2020

“Made in China 2025” – A Roadmap to Theft

- In 2015, China’s State Council released the “Made in China 2025” initiative, a ten-year plan for targeting ten advanced technology manufacturing industries.

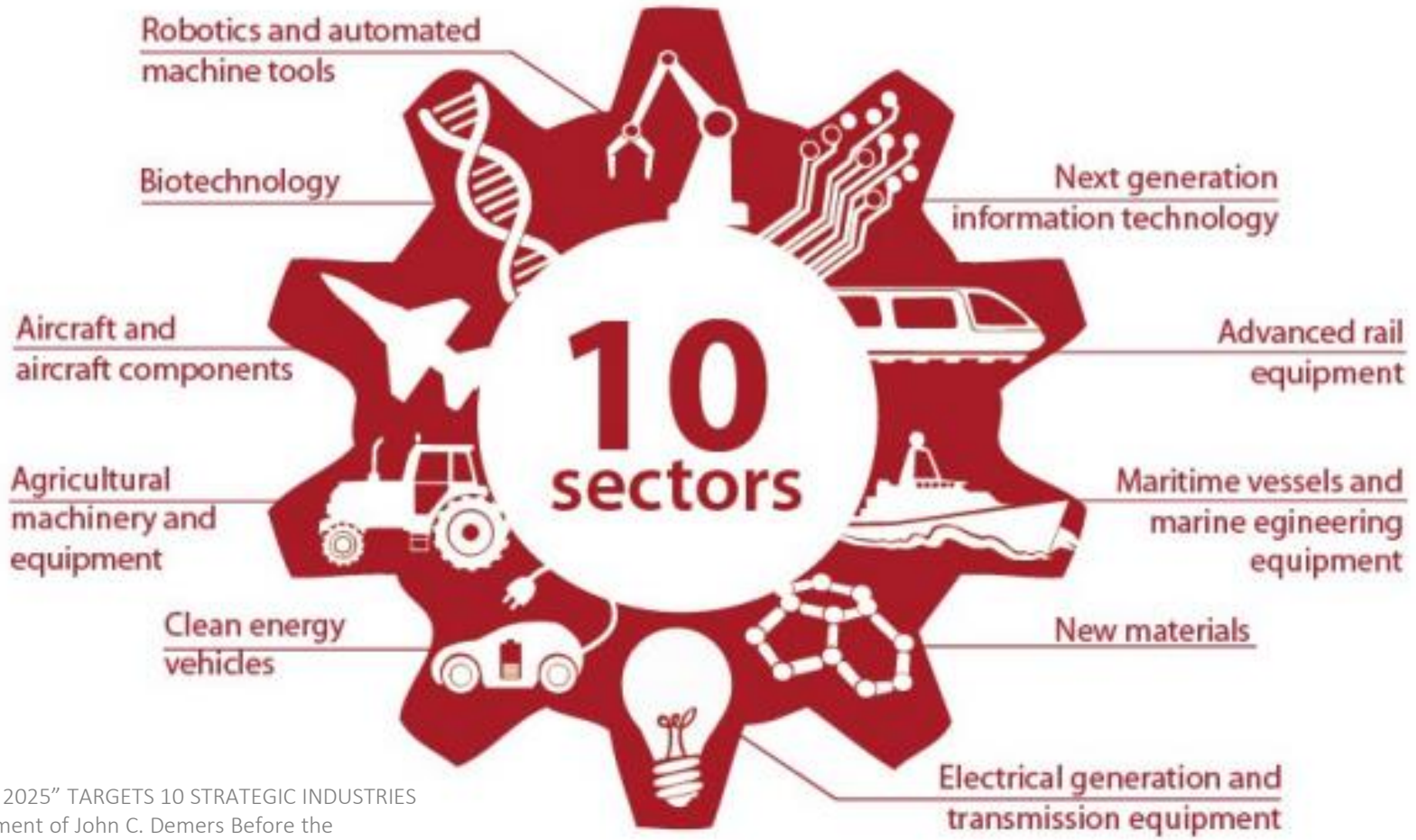

Image Source: “MADE IN CHINA 2025” TARGETS 10 STRATEGIC INDUSTRIES FOR DEVELOPMENT (NSD)Statement of John C. Demers Before the Committee on the Judiciary, United States Senate. December 12, 2018

DOJ's China Initiative

Launched in 2018, DOJ's China Initiative identified a series of goals and enforcement priorities related to countering threats posed by the Chinese government across a range of sectors:

- Prioritize investigations of economic espionage and trade secret theft
- Develop an enforcement strategy for non-traditional collectors, such as exploitation of universities and colleges
- Counter malicious cyber activity, such as the theft of personally identifiable information
- Counter malign foreign influence, including via FARA violations
- Counter foreign intelligence activities
- Conduct foreign investment reviews and bolster telecommunications security
- Conduct education and outreach

DOJ's China Initiative

The China Initiative has achieved significant success, but at the same time suffered from several prosecutorial setbacks and criticism that its focus on non-traditional collectors has unfairly targeted individuals of Chinese heritage. Even with these issues, the China Initiative—even if rebranded—is likely to continue in some form, given the range of threats posed by the Chinese government.

Notable China Initiative prosecution setbacks include:

- Anming Hu, an engineering professor at the University of Tennessee working on NASA projects, was indicted in February 2020 on charges of wire fraud and making false statements related to his alleged failure to disclose ties to a Chinese state-run university. After initially declaring a mistrial because the Jury failed to reach a verdict, the judge acquitted Hu of all counts.

- In July 2021, DOJ dropped charges against Dr. Qing Wang, a researcher at the Cleveland Clinic, who was charged with wire fraud and false statements related to Chinese grant funding.

> "We will counter Chinese espionage and cyber and everything else but we won't forget the civil rights and civil liberties of the people in this country."
>
> - Attorney General Merrick Garland, June 2021

- Also in July 2021, DOJ dismissed its case against Dr. Juan Tang, a cancer researcher at University of California – Davis, for allegedly lying about previous service in the Chinese People's Liberation Army. Similar cases were dropped against Chinese researchers at other universities.

Economic Espionage and Theft of Intellectual Property

Recent prosecutions under the Economic Espionage Act show a substantial focus on theft of intellectual property by Chinese actors.

- **Chi Lung Winsman Ng:** In February 2021, Chinese businessman Chi Lung Winsman Ng was indicted for conspiring to steal trade secrets from General Electric involving the company's silicon carbide semiconductor technology.

- **Hao Zhang:** In September 2020, Hao Zhang was sentenced to 18 months in prison and nearly half a million dollars in restitution for stealing trade secrets relating to acoustic wave filters used in mobile phones and other devices for consumer and military applications.

- **Hongjin Tan:** In February 2020, Hongjin Tan was sentenced to 24 months in prison for stealing more than $1 billion worth of proprietary information from his employer, a U.S. petroleum company.

"About 80 percent of all economic espionage prosecutions brought by [DOJ] allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases." *– DOJ, Information About the Department of Justice's China Initiative*

- **Shan Shi:** In February 2020, the head of a Houston-based company that was the subsidiary of a Chinese company was sentenced to 16 months in prison for conspiracy to steal trade secrets for pledging to "digest [and] absorb" foam manufacturing technology in the United States.

- **Haitao Xiang:** In November 2019, Haitao Xiang was indicted for trade secrets offenses for the theft of certain farming software from his employer, Monsanto. Xiang was arrested at the airport en route to China with a copy of the company's proprietary algorithm on his person.

Economic Espionage and Theft of Intellectual Property

Recent prosecutions

- Emblematic of this trend is the United Microelectronics Corporation ("UMC") case, in which the Taiwan-based semiconductor foundry pleaded guilty to criminal trade secret thefts and was sentenced to a $60 million fine.

- As part of the deal, UMC agreed to cooperate with the government in the investigation and ultimate prosecution of its co-defendant, Fujian Jinhua Integrated Circuit Co., Ltd., a Chinese state-owned enterprise. The case centered on a conspiracy to steal the trade secrets of American semiconductor company Micron Technology for the benefit of the Chinese government.

- In relation to the case, Deputy Attorney General Jeffrey Rosen stated: "UMC stole the trade secrets of an American leader in computer memory to enable China to achieve a strategic priority: self sufficiency in computer memory production without spending its own time or money to earn it. This prosecution is an example of [DOJ's] successful efforts to defend American companies from those who try to cheat and steal their technology."

Image Source: Maurice Tsai/Bloomberg

The Role of Chinese Intelligence Services in Trade Secret Theft

- **Li Xiaoyo and Dong Jiazhi:** In July 2020, DOJ unsealed charges against two Chinese hackers working with the Chinese Ministry of State Security ("MSS") for engaging in a sweeping global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19-related treatment, testing, and vaccines. The targeted industries included high tech manufacturing; medical device, civil, and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense.

- **Yanjun Xu:** In October 2018, an MSS operative was arrested in Belgium and extradited to the United States in connection with charges of conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies. Xu allegedly identified experts who worked for leading aviation companies and recruited them to travel to China often under the guise of asking them to deliver a university presentation.

- **Zha Ron, Chai Meng and JSSD Intelligence Officers:** In October 2018, Chinese intelligence officers and other co-conspirators working for the Jiangsu Province Ministry of State Security ("JSSD")—a provincial foreign intelligence arm of the MSS—were charged with conspiring to defraud the United States in violation of 18 U.S. Code § 1030 for their role in conducting repeated cyber intrusions into private companies' systems in the United States and abroad.
  - From around January 2010 to May 2015, JSSD intelligence officers, a team of JSSD supported hackers, and JSSD-recruited insiders engaged in multiple hacks targeting a French aerospace manufacturer and other companies in Arizona, Massachusetts and Oregon.
  - The co-conspirators targeted intellectual property, confidential business information and technology associated with the turbofan engine—a commercial aircraft engine used by U.S. and European airlines.

Cyber Intrusion

Recent prosecutions

Recent actions under Section 1030 demonstrate DOJ's willingness to use the statute to prosecute hacks that affect both the U.S. government and private businesses, including where the subject intrusions overlap with economic espionage and trade secrets theft. For example:

Image Source: Alex Wong/Getty Images

- **APT 41 Indictments:** In September 2020, DOJ announced charges against five China-based computer hackers for intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profits, universities, think tanks, foreign governments and pro-democracy activities in Hong Kong.

- **North Korean Cyberattacks:** In February 2021, indictments were unsealed against three North Korean computer programmers who conducted a series of cyberattacks aimed at stealing $1.3 billion in money and cryptocurrency from financial institutions and companies.

The DTSA: A Federal, Private Civil Cause of Action

- Trade secret misappropriation claims were previously brought in one of **three** ways:
  - By **private plaintiffs** under relevant **state** laws
  - By the **government** for **civil** or **criminal** enforcement under the Economic Espionage Act of 1996 ("EEA")
- The DTSA adds a **fourth** avenue: a federal, **private civil** cause of action

Image Source: Al Drago/Reuters

- "An **owner** of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service **used in, or intended for use in, interstate or foreign commerce**."
  - Owner: whoever has "rightful legal or equitable title to, or **license in**, the trade secret"
    - *Phyllis Schlafly Revocable Tr. v. Cori*, 16-cv-01631 (E.D. Mo. Nov. 9, 2016) (motion to dismiss granted and TRO denied because it was unclear whether plaintiff "owned" the alleged trade secrets).
  - Purely **intrastate** products and services not covered
- No preemption (18 U.S.C. § 1838)
  - Can bring both state and federal trade secrets claims in federal court
  - Exception: whistleblower immunity

The Impetus Behind the DTSA

- "[I]ncreased digitization of critical data and increased global trade."
- Federal agencies unable to investigate every case of trade secret theft.
- Pre-DTSA federal criminal laws "not suited to mak[e] whole the victims of misappropriation." *- H.R. Rep. No. 114-529, at 2, 4 (2016).*
- Belief state Trade Secret laws were inadequate:
  - Costly compliance with each individual state's laws
  - Trade secret theft often not confined to a single state, making it difficult for:
    1. Efficient discovery
    2. Preserving evidence; and
    3. "[K]eep[ing] a trade secret thief from boarding a plane and taking the secret beyond the reach of American law." *- H.R. Rep. No. 114-529, at 2, 4 (2016).*
- Lack of predictability and uniformity

Image Source: Jim Wilson/New York Times

Economic Espionage and Theft of Intellectual Property

- Under the **Justice Manual**, the Economic Espionage Act "is not intended to criminalize every theft of trade secrets for which civil remedies may exist under state law" and requires special advisory approval by the National Security Division ("NSD") AAG.
- When considering to initiate a prosecution under **Sections 1831 or 1832**, the Justice Manual requires consideration of:
  - Scope of criminal activity, including evidence of involvement by a foreign government, foreign agent, or foreign instrumentality
  - Degree of economic injury to the trade secret owner
- Additional considerations include:
  - Type of trade secret misappropriated
  - Effectiveness of available civil remedies
  - Potential deterrent value of the prosecution

Why Get Law Enforcement Involved?

- Investigative process
- Search warrants and other investigative mechanisms are likely stronger.
- The Penalties are more severe (including incarceration) and not exclusive.
- Law Enforcement involvement can provide a deterrent effect or stop misappropriation at less legal expense to company.

What Considerations Warrant Excluding Law Enforcement?

- Less Control over Litigation and Potential Settlements.
- Involving Law Enforcement Results in limits on Confidentiality.
  - These limits include constitutional Sixth Amendment considerations, Criminal Discovery and Brady Obligations
  - There is an enhanced risk of disclosure of trade secrets or other confidential company information
- Assessment of the financial and impact on the company and employees.
- Involving Law Enforcement can also involve a substantial time investment.
- Consideration of a potential Public Relations Impact.

Steps to Take Before Contacting Law Enforcement

1. Preserve documents

2. Identify key documents and witnesses

   - These will include documents and facts supporting the case for theft

   - These should also include negative documents and facts

3. Assemble the story

   - What happened?

   - Why should law enforcement get involved?

   - The narrative should be clear about negative facts and elements

Image Source: Joshua Roberts/Reuters

Reaching Out to Law Enforcement

- It is best to do so if there are established relationships
- In person meetings are recommended as being most effective
- It is important tell the story while remaining up-front about the negatives, in order to build and retain trust
- The conversation should not dwell on technical issues regarding the technology
- Be vigilant and refrain from disclosing privileged information

Image Source: Leah Millis/REUTERS

What Happens Next?

There is still a need for legal advice and monitoring throughout the process:

- Initial investigation period
- Indictment
- Warrants, subpoenas and discovery
- Plea negotiations
- Trial
- Potential impact on civil matter

Image Source: Toru Hanai/Reuters

Zainab Ahmad

200 Park Avenue, New York
NY 10166-0193

Tel +1 212.351.2609
zahmad@gibsondunn.com

Zainab Ahmad is a partner in the New York office of Gibson, Dunn & Crutcher and a member of the firm's White Collar Defense and Investigations and Privacy, Cybersecurity and Consumer Protection Practice Groups. Ms. Ahmad served as Senior Assistant Special Counsel in Special Counsel Robert S. Mueller's Office following a successful career as a prosecutor and trial lawyer at the Department of Justice in both Washington, D.C., and the Eastern District of New York. As former Deputy Chief of the National Security and Cybercrime section at the U.S. Attorney's Office in the Eastern District of New York, Ms. Ahmad supervised a unit of over 20 attorneys, investigators, and staff prosecuting sensitive counterterrorism, counterespionage and cybercrime cases. Ms. Ahmad's practice focuses on white collar defense and investigations, as well as regulatory and civil litigation challenges, such as matters involving corruption, anti-money laundering, sanctions and FCPA issues. She also advises clients on cybercrime and intellectual property issues, including handling investigations, enforcement defense, and litigation. She has extensive experience with a wide range of federal, state, and international cybersecurity laws, regulations, and standards.

Prior to joining Gibson Dunn, Ms. Ahmad was a prosecutor with the U.S. Department of Justice for 11 years. She most recently served as a Senior Assistant Special Counsel in Special Counsel Robert S. Mueller's Office from 2017 to 2019. Prior, she served as an Assistant U.S. Attorney at the U.S. Attorney's Office in the Eastern District of New York, where her roles included Deputy Chief of the National Security and Cybercrime section. During her tenure, she prosecuted and supervised some of the most complex international terrorism investigations in the United States, focusing on al-Qaeda, ISIS and attacks against U.S. military personnel and U.S. diplomats abroad. In pursuit of these extraterritorial national security investigations, she worked closely with the FBI, U.S. intelligence community, Department of State and Department of Defense, and she frequently traveled to Europe, the Middle East and Africa to negotiate with foreign law enforcement officials and regulators for access to evidence and testimony, and to collaborate with foreign counterparts regarding mutual legal assistance requests and extradition assurances. Her work was chronicled in a The New Yorker feature article, "Taking Down Terrorists in Court."

During her career, Ms. Ahmad was seconded twice to Washington, D.C., serving in 2016 as Counselor for Transnational Organized Crime and International Affairs and in 2017 as Acting Deputy Assistant Attorney General in Washington, D.C., where she was responsible for supervising about 70 prosecutors in three sections: Organized Crime & Gangs, Human Rights and Special Prosecutions, and Capital Cases, including the filter team handling the "Panama Papers"-related investigations.

Drawing on her experience, Ms. Ahmad has played an active role in the advancement of global cybercrime laws and regulations. She previously represented DOJ at meetings of the World Economic Forum's Cybercrime Workshop and participated in development of WEF's Guidance on Public-Private Information Sharing Against Cybercrime. She also organized and led a Cybercrime Roundtable with former FBI Director James Comey and General Counsel and C-suite executives from various industries, including banking, media, health care and pharmaceutical companies, to discuss improved public-private partnership in combatting cybercrime.

Ms. Ahmad received her law degree in 2005 from the Columbia University School of Law, where she received the Hamilton Fellowship (full scholarship for academic excellence), was a James Kent Scholar and a Harlan Fiske Stone Scholar, and served as the Senior Editor of the Columbia Law Review. She served as a law clerk for Judge Jack B. Weinstein of the U.S. District Court for the Eastern District of New York from 2006 to 2007 and for Judge Reena Raggi of the U.S. Court of Appeals for the Second Circuit from 2007 to 2008.

David P. Burns

1050 Connecticut Avenue
N.W., Washington, DC 20036-5306

Tel +1 212.887.3786
dburns@gibsondunn.com

David P. Burns is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher. His practice focuses on white-collar criminal defense, internal investigations, national security, and regulatory enforcement matters. Mr. Burns represents corporations and executives in federal, state, and regulatory investigations involving securities and commodities fraud, sanctions and export controls, theft of trade secrets and economic espionage, the Foreign Agents Registration Act, accounting fraud, the Foreign Corrupt Practices Act, international and domestic cartel enforcement, health care fraud, government contracting fraud, and the False Claims Act. He is the co-chair the firm's National Security Practice Group, and a member of the White Collar and Investigations and Crisis Management practice groups.

Prior to re-joining the firm, Mr. Burns served in senior positions in both the Criminal Division and National Security Division of the U.S. Department of Justice. Most recently, he served as Acting Assistant Attorney General of the Criminal Division, where he led more than 600 federal prosecutors who conducted investigations and prosecutions involving securities fraud, health care fraud, Foreign Corrupt Practices Act violations, public corruption, cybercrime, intellectual property theft, money laundering, Bank Secrecy Act violations, child exploitation, international narcotics trafficking, human rights violations, organized and transnational crime, gang violence, and other crimes, as well as matters involving international affairs and sensitive law enforcement techniques. Prior to joining the Criminal Division, Mr. Burns served as the Principal Deputy Assistant Attorney General of the National Security Division from September 2018 to December 2020. In that role, he supervised the Division's investigations and prosecutions, including counterterrorism, counterintelligence, economic espionage, cyber hacking, FARA, disclosure of classified information, and sanctions and export controls matters. He also spent five years as an Assistant United States Attorney in the Southern District of New York, Criminal Division, from 2000 to 2005.

Mr. Burns has been recognized by Chambers USA – America's Leading Business Lawyers as a leading White Collar attorney in the District of Columbia and Who's Who Legal and Global Investigations Review (GIR) recognized him as a leading investigations lawyer, deemed "excellent" for his work across "federal, state, and regulatory investigations." Who's Who Legal also recognized Mr. Burns as a leading lawyer in the area of Business Crime Defense.

Mr. Burns graduated in 1995 from Columbia Law School, where he was a Harlan Fiske Stone Scholar and an Articles Editor of the Columbia Business Law Review. He received his Bachelor of Arts degree in economics from Boston College in 1991.

Robert K. Hur

1050 Connecticut Avenue
N.W., Washington, DC 20036-5306

Tel +1 202.887.3674
rhur@gibsondunn.com

Robert K. Hur is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher, and Co-Chair of the Firm's Crisis Management Practice Group. A seasoned trial lawyer and advocate, he brings decades of experience in government and in private practice, including service in senior leadership positions with the U.S. Department of Justice, to guide companies and individuals facing white-collar criminal matters, regulatory proceedings and enforcement actions, internal investigations, and related civil litigation. He is also a member of the firm's White Collar Defense and Investigations Practice Group and the National Security Practice Group.

Prior to joining Gibson Dunn, Mr. Hur served as the 48th United States Attorney for the District of Maryland. Presidentially appointed and unanimously confirmed by the United States Senate, he served from 2018 to 2021 as the chief federal law enforcement officer in Maryland, setting strategic priorities for and supervising one of the largest and busiest U.S. Attorney's Offices in the nation. During his tenure as United States Attorney, the Office handled numerous high-profile matters including those involving national security, cybercrime, public corruption, and financial fraud. In pursuit of sophisticated and impactful cases, Mr. Hur partnered closely with other enforcement agencies including the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Department of Health and Human Services Office of Inspector General, and the Maryland Attorney General's Office. He also hired dozens of attorneys from diverse backgrounds to bring the Office to its maximum staffing level and as a member of the Attorney General's Advisory Committee, counseled the Attorney General on matters of policy, procedure, and management.

Before serving as United States Attorney, Mr. Hur served as the Principal Associate Deputy Attorney General with the Department of Justice in Washington, D.C. from 2017 to 2018. In the position of "PADAG," Mr. Hur was a member of the Department's senior leadership team and the principal counselor to Deputy Attorney General Rod J. Rosenstein, assisting him with oversight of all components of the Department including the National Security, Civil, Criminal, and Antitrust Divisions, all 93 U.S. Attorney's Offices, and the Federal Bureau of Investigation. He also liaised regularly on behalf of the Justice Department with the White House, Congressional committees, and federal intelligence, enforcement and regulatory agencies.

Mr. Hur is an accomplished trial lawyer, having tried fourteen cases as a federal prosecutor and in private practice. He was a member of the trial team that won a clean-sweep acquittal in 2016 for Vascular Solutions, Inc., a publicly traded medical device company, in a groundbreaking federal criminal trial involving off-label promotion charges. More recently, in 2020 as United States Attorney, he tried and won conviction in an international money-laundering trial that was the first in-person federal jury trial conducted in the Washington, D.C. region during the COVID-19 pandemic.

Mr. Hur serves as Chair of the Asian American Hate Crimes Workgroup, a statewide body formed by Governor Larry Hogan and charged with developing strategies, recommendations, and actions to address the rise in violence and discrimination targeting the Asian American community. He is an active member of the Alliance for Asian American Justice, a national pro bono initiative providing legal services to victims of anti-Asian hate, and previously served on the Board of Directors of the Asian Pacific American Bar Association of the District of Columbia (APABA-DC).

Mark Lyon

1881 Page Mill Road
Palo Alto, CA 94304-1211

Tel +1 650.849.5307
mlyon@gibsondunn.com

H. Mark Lyon is Chair of the firm's Artificial Intelligence and Automated Systems Practice Group, and brings nearly three decades of experience as a trial lawyer and trusted corporate legal advisor to companies in a wide range of technology areas.

As practice group chair, Mr. Lyon has extensive experience representing and advising clients on the legal, ethical, regulatory, and policy issues arising from emerging technologies like artificial intelligence. He regularly acts as a strategic advisor to clients in their development of AI-related products and services, their acquisition and sale of technology-related businesses, and in their development of appropriate legal and ethical policies and procedures pertaining to AI-focused business operations. In the rapidly advancing area of automated and autonomous vehicles, Mr. Lyon has guided clients through the numerous hurdles of federal and state regulations and requirements for vehicle testing and deployment, as well as advising and assisting clients in exercising their voice before key agencies and legislative bodies. As a member of the firm's Privacy, Cyber Security and Consumer Protection practice group, Mr. Lyon brings a global focus to help his clients develop, implement, and audit appropriate policies and procedures to comply with applicable data privacy and cyber security regulations. In addition, as a member of the firm's Intellectual Property practice, he assists clients in the acquisition, protection and enforcement of strategic intellectual property rights.

When litigation and other disputes arise, Mr. Lyon serves as lead trial and appellate counsel in patent, trade secret, copyright, trademark, privacy, products liability, bankruptcy, and other complex litigation matters. He has successfully led litigation teams in matters involving sophisticated technologies ranging from electronic devices, artificial intelligence and other computer software, wireless telecommunications, and semiconductor products to medical devices and pharmaceuticals. While Mr. Lyon has tried to verdict and won both jury and bench trials, a consistent hallmark has been the strategic use of targeted motion practice to achieve success prior to trial. Indeed, on multiple occasions, the Daily Journal has named Mr. Lyon as a top IP litigator for his handling of high-stakes, high-profile litigation matters.

As a result of his work in AI and AV, he was recently named a "Top Artificial Intelligence Lawyer" by the *Daily Journal* and a "California Trailblazer" by the *Recorder*. In addition, on multiple occasions, the *Daily Journal* has named Mr. Lyon a top IP litigator for his handling of high-stakes, high-profile litigation matters.

Through his career, Mr. Lyon has represented a long list of technology-focused clients, including a major Silicon Valley-based global consumer electronics manufacturer, Intel, Facebook, Oculus VR, Medtronic, St. Jude Medical, GCL-Poly Energy Holdings Limited, Sharp Corporation, VMware, Square, Red Hat, and Novell, just to name a few.

Mr. Lyon is a frequent author and lecturer on matters relating to technology, particularly those involving machine learning, artificial intelligence and automation, intellectual property, data privacy, and disputes before the U.S. International Trade Commission. In addition, Mr. Lyon is an active member of The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems as well as the Association for the Advancement of Artificial Intelligence. He is a former co-chair of the Patent Litigation Committee of the Federal Circuit Bar Association.

Mr. Lyon obtained his J.D., *summa cum laude*, from Santa Clara University and holds a bachelor's degree in electrical engineering from Michigan State University. He is a member of Pi Mu Epsilon (a national mathematics honorary), Eta Kappa Nu (a national electrical engineering honorary), and Alpha Sigma Nu (a national Jesuit honorary). Prior to becoming a lawyer, Mr. Lyon worked for Lockheed Missiles & Space Systems, Inc., in the Space Systems and Astronautics Divisions, performing systems design and analysis for RF and laser satellite telecommunications and computer and laser networks.

Mr. Lyon is admitted to practice in California and Washington, D.C., as well as various district and appellate courts across the country, and has had particular success defending cases in the plaintiff-favorite Eastern District of Texas.

Alexander Southwell

200 Park Avenue
New York, NY 10166-0193

Tel +1 212.351.3981
asouthwell@gibsondunn.com

A partner in Gibson, Dunn & Crutcher's New York office, Alexander H. Southwell founded and co-chairs the Firm's Chambers-ranked Privacy, Cybersecurity, and Data Innovation Practice Group and is a member of the White Collar Defense and Investigation, Litigation, Crisis Management, and Artificial Intelligence and Automated Systems Practice Groups.

Mr. Southwell advises emerging companies to global enterprises across all market sectors that experienced data breaches or were victimized by cyber-crimes and he has deep expertise counseling on broad issues under the Computer Fraud and Abuse Act, the Economic Espionage Act, the Electronic Communications Privacy Act, and related federal and state computer fraud and consumer protection statutes. He also regularly counsels clients on compliance with the full range of US and international privacy and data protection laws and regulations, including online privacy, financial privacy, medical privacy, educational privacy, telecommunications and marketing, and workplace privacy, as well as product counseling and global regulatory strategies. He often leads the defense of regulatory investigations from the Federal Trade Commission, State Attorneys General, and other federal, state, and local regulators and criminal authorities. Mr. Southwell has particular expertise advising on FTC order compliance, selecting and working with Assessors, and handling FTC 6(b) studies. He additionally counsels companies on privacy and security risks related to data-driven product development, including in cutting-edge areas such as artificial intelligence, cloud deployment, and data innovation, and related to compliance with international, national, state, and local privacy and cybersecurity laws and regulations. Mr. Southwell also is regularly retained to lead privacy and data security class actions and litigations around the country.

In addition, Mr. Southwell handles a range of white-collar criminal and regulatory enforcement defense, internal investigation, and compliance matters, and regularly leads complex civil litigations. An experienced trial and appellate attorney, prior to joining Gibson Dunn, Mr. Southwell served as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York where he focused on cyber-crimes and intellectual property offenses, in addition to securities and commodities and other white collar frauds.

Mr. Southwell is ranked as one of the top five attorneys nationwide for Privacy & Data Security Litigation by *Chambers USA* and *Chambers Global* and is also ranked for White Collar Litigation by *Chambers*, which notes his "keen eye for attention to detail, client service and navigating a complex legal and regulatory landscape." A client notes: "Alex is tremendous. If you've got an issue that is a paramount crisis and going to break the company, Alex is who you should turn to. He is top notch, savvy and he understands what you need." Recognized as a "Leading Individual" in Gibson Dunn's ranking in the 2021 *Global Data Review* GDR 100 Elite, he was also named a *Law360* "MVP" in Privacy in both 2016 and 2015 – one of five "elite attorneys" recognized – for his "successes in high-stakes litigation." Additionally, Mr. Southwell was selected as a Cybersecurity and Data Privacy Trailblazer by *The National Law Journal,* and has been recognized as one of the top 30 Data Protection Lawyers in Euromoney Expert Guides' *Best of the Best USA*, and named as one of the 30 best and brightest data breach response lawyers in Cybersecurity Docket's "Incident Response 30." In addition, he is recognized as a "Litigation Star" by *Benchmark Litigation*, as a leading lawyer in the area of Criminal Defense: White Collar by *The Best Lawyers in America®,* and as one of the world's leading investigations lawyers by *Who's Who Legal: Investigations*.

Mr. Southwell serves on Gibson Dunn's Technology Committee and was appointed to the New York State Bar Association's Task Force on Autonomous Vehicles and the Law, as well as serving on the Board of Advisors of the Center on Law and Information Policy at Fordham Law School, one of the nation's leading academic centers contributing to the development of the law and policy in the area of information technology. Mr. Southwell has also been an Adjunct Professor of Law at Fordham University School of Law, teaching a seminar on cyber-crimes, covering computer misuse crimes, intellectual property offenses, the Fourth Amendment in cyber-space, computer evidence at trial, data breach and privacy issues, and information security, among other areas.

Most participants should anticipate receiving their certificate of attendance via email approximately one month following the webcast.

Virginia Bar Association members should anticipate receiving their certificate of attendance two months following the webcast.

Please direct all questions regarding MCLE to CLE@gibsondunn.com