TRUMP'S FIRST 100 DAYS: IMPLICATIONS FOR TECH

The second Trump administration has so far taken the United States – and the world – on a whirlwind journey. The volume and breadth of activity – including far-reaching tariff and trade measures, hundreds of Executive Orders and vast agency reorganizations and layoffs – are unprecedented. This briefing provides an overview of key tech-related developments during Trump's first 100 days and offers certain global perspectives and insights.

Tariffs on Technology Components

US tariffs are at their highest level in years, impacting almost all sectors and industries globally, with some specific sectoral exceptions. The "reciprocal tariffs" in effect since April 5, 2025, impose a 10% duty on imports from most countries, as well as significantly higher tariff duties on over 50 other countries. Although these higher tariffs are suspended while bilateral negotiations around potential trade concessions take place for certain countries, a combination of fentanyl-related and reciprocal tariffs results in a 145% tariff rate for Chinese imports.

With respect to tech, the reciprocal tariffs currently include exemptions for semiconductors, smartphones, some computers, various other electronic equipment, and certain critical minerals. However, the Trump administration has initiated investigations under Section 232 of the Trade Expansion Act into the effects of semiconductor and critical mineral imports on US national security, potentially laying the groundwork for additional targeted tariffs on these items. Both investigations are broad in scope. In addition to a range of semiconductors and their manufacturing equipment, the semiconductor investigation will include a review of derivative products that contain semiconductors. The investigation into critical minerals, including rare earth metals, will capture all derivative products that include critical minerals inputs, with significant implications for technology supply chains.

Technology products and services are likely to remain an area of focus in ongoing trade negotiations, although no tariffs have yet been imposed on tech services (e.g., cloud services). The Trump administration has expressed frustration with the impact of certain trading partners' tech-related privacy, content, and market regulations as well as digital services taxes on US technology companies. For example, the Executive Order Regulating Imports with a Reciprocal Tariff to Rectify Trade Practices that Contribute to Large and Persistent Annual United States Goods Trade Deficits, dated April 2, 2025, cited non-tariff barriers to "cross-border data flows and discriminatory practices affecting trade in digital products" as part of the justification for the national emergency on which the reciprocal tariffs are based.

The formal response of the European Union (EU) to US reciprocal tariffs has focused on the announcement of retaliatory tariffs on US goods, which have been suspended pending negotiations with the United States. However, there has been widespread speculation, including from senior EU policymakers, that if its trade negotiations with the United States are unsuccessful, future EU responses could potentially include measures impacting US digital services.

China has responded to the US tariffs with a 125% levy on American imports and licensing requirements for the export of seven medium and heavy rare earths necessary for the manufacturing of semiconductors, medical devices, aerospace and defense equipment. These licensing requirements can be applied as an outright export ban for rare earths that can hardly be replaced by suppliers from any other jurisdiction. It remains to be seen when the United States and China will begin negotiations.

The outcomes of the Section 232 investigations, as well as the ongoing and potential bilateral negotiations with trading partners, will impact the levels of duties applicable to tech-related imports, as well as potentially additional economic considerations affecting US and other technology companies. For instance, tech giants like Apple are looking to relocate production to avoid tariff uncertainty.

Trade and Export Controls as Tools in the Tech Competition

President Trump's Memorandum, America First Trade Policy, issued on his first day in office, calls for the Secretary of State and the Secretary of Commerce to make recommendations for boosting America's technological edge and to identify and eliminate loopholes in existing export controls – especially those enabling the transfer of strategic goods, software, services, and technology to key rivals and their proxies. The administration has called for enhanced enforcement and tightening of export controls, although it remains to be seen what further restrictions – which we expect to cover semiconductors and other critical technologies – will entail.

U.S. Department of Commerce Secretary Howard Lutnick has emphasized that threats from foreign adversaries require strong counterefforts, particularly where semiconductors and other important technologies are concerned, and that partnering with allies on export controls is critical.

Although President Trump removed several of the Biden administration's policies and orders, certain Biden-era export controls regulations remain in place, including those pertaining to advanced semiconductors and quantum technologies. Two regulations are worth highlighting:

- The Framework for Artificial Intelligence Diffusion, (AI Diffusion Framework), signed on January 13, 2025, by the Bureau of Industry and Security intends to maintain the US and select partners' leadership in advanced AI, mitigating the potential for chip smuggling, diversion of exports, and investment in AI compute facilities in countries deemed to pose national security risks. The AI Diffusion Framework establishes a global export control system that limits the export of advanced AI chips and closed-frontier AI model weights by dividing countries into three tiers. The United States and 18 key partner countries in Tier 1 face no export restrictions and unlimited access. For approximately 150 Tier 2, or "middle-tier" countries (including several EU Member States), the AI Diffusion Framework contains a complex set of export restrictions to protect US national security and economic interests. Tier 3 countries, already facing US arms embargoes, face continued severe export restrictions. The AI Diffusion Framework also introduces the Universal Validated End User and the National Validated End User Programs, which aim to ensure that AI technology is deployed responsibly, securely, and in a controlled manner, while still enabling companies to innovate and expand their operations.

With the May 15, 2025, compliance deadline approaching, foreign governments, tech companies, and Members of Congress have urged the Trump administration to reconsider certain restrictions, fearing that they could hinder AI development and investment. "The rule places burdensome constraints on U.S. companies that would be difficult to comply with and even harder for the Federal government to enforce," Republican senators wrote in an April 11, 2025 letter to Howard Lutnick. The White House officials are currently discussing the AI Diffusion Framework's implementation, with some suggesting eliminating the tiered system and computing power caps, and opting, instead, to rely on export licenses for most countries.

For more information about the AI Diffusion Framework, see our prior briefing.

- The Final Rule on Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (Data Rule), implemented President Biden's Executive Order 14117 and established "what are effectively export controls" by setting up a Data Security Program with the U.S. Department of Justice's (DOJ) National Security Division (NSD). The Data Rule regulates data transactions that provide "countries of concern" and covered persons with access to US bulk sensitive data or government-related data. The Data Rule prohibits certain highly sensitive transactions in their entirety and restricts others unless they meet security requirements set by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). It applies to US persons and non-US persons in certain scenarios, has nuanced definitions for in-scope data and defines "countries of concern" as China (inclusive of Macau SAR and Hong Kong SAR), Cuba, Iran, North Korea, Russia and Venezuela.

  The Data Rule came into effect on April 8, 2025, and on April 11, 2025, the DOJ issued explanatory guidance, which announced a grace period through July 8, 2025, during which the NSD will not prioritize civil enforcement for Data Rule violations against persons that engage in good faith efforts to comply with the Data Rule. The DOJ recognized that the rule is nuanced, and the grace period intends to "allow the private sector to focus its resources and efforts on promptly coming into compliance and to allow the NSD to prioritize its resources on facilitating compliance." The DOJ has stated that it will pursue penalties for egregious, wilful violations of the Data Rule.

For more information about the Data Rule, see our prior briefing.

An Uncertain Approach to Data Governance: Privacy and Cyber

In addition to the Data Rule, the first 100 days of Trump's second administration included several key developments relating to data governance:

- **Agencies in flux**. Federal data protection regulators experienced significant transition of leaders and downsizing of staff. The day President Trump took office, the U.S. Securities and Exchange Commission (SEC) former chair Gary Gensler stepped down. Shortly after, President Trump replaced the head of the Consumer Financial Protection Bureau (CFPB) and fired two of the remaining three commissioners at the Federal Trade Commission (FTC) (leaving just the chair for an agency normally led by a committee of five). Meanwhile the FTC, the CFPB, the SEC, and CISA have all experienced varying degrees of staff reductions. As these cuts occurred, new agency leadership has been putting in place approaches to regulation and enforcement that are markedly different from those of the previous administration. These changes have resulted in uncertainty and questions about these regulators' enforcement philosophies and priorities.

- **Key regulatory changes from 2024 remain**. With promises from President Trump to reverse most of President Biden's policies, many questioned the fate of significant regulatory changes that took effect at the near end of the previous administration – notably, FTC revisions to the Children's Online Privacy Protection Act (COPPA) rules and the Data Rule (discussed above). Thus far, these rules have proceeded largely untouched: the FTC announced on the eve of transition that it had finalized its proposed rule revisions on COPPA, publishing them in the Federal Register on April 22, 2025. Meanwhile, as noted above, the Data Rule's enforcement date of April 8, 2025 came and went without revocation or fanfare and several days afterwards, the DOJ issued explanatory guidance.
- **Cross-border data transfer framework threatened – but remains (for now)**. Days into the new administration, President Trump fired three Democratic members of the Privacy and Civil Liberties Oversight Board (PCLOB), jeopardizing the board's ability to continue its work. Many wondered what this action would mean for the recently established EU-US Data Privacy Framework (DPF) that helps facilitate compliant personal data transfers from the EU to the United States under the GDPR. EU regulators and advocates have raised questions about the continued viability of the DPF, given the changing regulatory landscape in the United States – but for now, both the United States and the EU continue to assert that the Privacy Framework satisfies GDPR data transfer obligations.

For more information about data transfer developments, see our prior briefing.

- **Continued support for federal privacy law and COPPA 2.0**. While much attention has been focused on executive action, in the background there remains hope for legislative action on the privacy front. Republican House representatives have launched a new working group aimed at developing a fresh proposal for a federal privacy law, while Senate members have restarted the discussion around a so-called COPPA 2.0 to strengthen children's and teens' privacy laws in the United States.

A Multilevel Effort to Lead on Artificial Intelligence

- **AI Executive Orders and memoranda.** One of President Trump's first actions after taking office was to rescind President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence and to issue the Removing Barriers to American Leadership in Artificial Intelligence Executive Order (Trump AI EO), which calls for a new action plan for AI to be developed by July 22, 2025. The Trump AI EO states: "It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security."

  It is still unclear what the new AI action plan will entail, but it will undoubtedly be impactful and likely, controversial. The administration issued a Request for Information on February 6, 2025, and received 10,068 responses from large tech companies, AI startups and other organizations, which are published on a dedicated webpage. Common response themes include calls for streamlined regulation and investment in infrastructure and innovation. OpenAI's and Google's arguments call for an expanded fair use defense under the US copyright laws, arguing that freedom to innovate is, among other things, a matter of national security. These comments drew a response from more than 400 entertainment industry members, urging the Trump administration not to jeopardize copyright protections for America's creative and knowledge industries just to train AI.

  On April 7, 2025, President Trump issued two revised memoranda calling for federal agencies to accelerate their use of AI through innovation, governance, and public trust as well as for federal agencies to maximize their use of AI in government.

  On April 29, 2025, several agencies issued a Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan, which will identify federal strategic priorities for AI R&D that may be less attractive for private-sector funding. Examples include AI research for accelerating fundamental scientific discovery and technological breakthroughs, AI research for national security and critical infrastructure, and advances in agentic and physically embodied AI with implications for US strategic competitiveness.

  Several Biden Executive Orders relevant to AI remain in effect and continue to be impactful. These include: (1) Advancing United States Leadership in Artificial Intelligence Infrastructure, signed on January 14, 2025, which aims to preserve US economic competitiveness in AI, emphasizing national security and use of clean energy technologies. The Executive Order outlines principles, criteria and timelines for the construction and operation of frontier AI infrastructure, including data centers, by private sector entities on federal land; and (2) Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity, signed on January 16, 2025, which requires government vendors and cloud providers to apply specific cybersecurity safeguards, while launching a new AI cyber defense pilot program.

- **Federal and state AI legislation.** On April 29, 2025, federal lawmakers took a significant step in federal AI legislation by passing S. 146, the TAKE

IT DOWN Act, which would criminalize publication of non-consensual explicit images and videos, including AI-generated content and would require websites to remove such content within 48 hours of a request to do so. The legislation now awaits Trump's signature. The myriad of pending federal bills continues, seeking to cover a range of areas including: H.R. 238 - Healthy Technology Act of 2025 (which would amend the Food, Drug and Cosmetic Act to permit certain AI and machine learning technologies to prescribe drugs); H.R. 6943 - No AI FRAUD Act (which would clarify property rights in a person's likeness and voice and related terms and damages); H.R. 7123- QUIET Act and H.R. 7116 - Do Not Disturb Act (analogous bills, requiring disclosures with respect to robocalls using AI). It is still unclear where the Trump administration stands on each of these bills.

Most US AI legislation continues to progress at the state level and generally, enacted AI laws focus on AI in elections, employment, unfair discrimination, deepfakes and consumer-facing communications. California has also passed laws focused on, for example, content sharing platforms and AI developers. State AI legislation introduced during Trump's first 100 days includes hundreds of bills across several areas, including: consumer protection from algorithmic discrimination (for example, Illinois S. 2203); use of AI or automated decision-making tools (for example, Georgia's SB 164); labelling or reporting of AI use in services (for example, New York's S.B. 934/A.B. 3411); requirements for chatbot providers to inform users who interact with AI (for example, Massachusetts' SD 2223); and energy demands in AI development (for example, California's AB 222). A notable pending AI bill is the HB 1709 - Texas AI Governance Act, introduced at the end of 2024, which models itself on EU legislation and is more comprehensive than any other US AI state law.

- **AI litigation.** While a detailed analysis of litigation is beyond the scope of this briefing, it is worth highlighting that there are many ongoing litigation developments focusing on generative AI. These pertain to trademarks; computer code, images, artwork, written works and music copyrights; trade secrets; patents; privacy; right to publicity; and antitrust. Defendants include smaller players as well as giants such as Microsoft, NVIDIA, and OpenAI. The progress of these cases and their outcomes will shape the future of AI regulation.

For a sample overview of some key considerations, see our prior briefing.

- **Data centers.** By issuing executive orders to cut regulatory barriers, Trump fostered a favorable climate for AI research and investment, expediting the permitting process and paving the way for a rapid expansion of data centers. This drive for AI development is set to bring substantial upgrades to data center infrastructure, enabling facilities to meet the growing computational demands of AI applications such as enhanced learning and data processing.

  However, Trump's trade policies, particularly tariffs on high-value electronics from China, could undermine efforts to boost the AI market. These tariffs risk increasing data center construction costs and, consequently, the cost of AI processing. Additionally, they may affect the cost and availability of crucial components needed for AI systems.

Balancing innovation with trade challenges will be key to sustaining the momentum in AI advancement.

The American Midwest is emerging as a significant hub for data center development, generally driven by factors such as cooler temperatures, proximity to water sources, and available land. President Trump, OpenAI CEO Sam Altman, SoftBank CEO Masayoshi Son and Oracle founder Larry Ellison have announced Stargate, a four-year, US$500 billion project to build data centers and other AI infrastructure in the United States. Stargate will play a key role in shaping America's AI future. The first phase of the Stargate initiative is underway in Texas, leveraging the state's infrastructure and favorable business environment.

For more information about data center developments, see our prior briefing.

Fostering Growth of Digital Assets

Following issuance of the Executive Order Strengthening American Leadership in Digital Financial Technology there are unprecedented changes in crypto policy , including the dismantling of the SEC's crypto enforcement program through the dismissal of cases against industry-leading exchanges, intermediaries, and digital asset issuers, the fostering of an environment of collaboration between industry participants and regulators through roundtables, advisory committees, transparency, and key regulatory actions (highlighted below), as well as growing momentum on Capitol Hill for stablecoin and digital asset market structure legislation in 2025.

For example, the SEC – previously a crypto industry antagonist – launched a Task Force undertaking a comprehensive review of digital assets regulation and the use of blockchain technology in the securities markets. In addition, various SEC divisions have provided useful guidance to the public on Meme Coins, crypto mining, covered stablecoins and digital asset securities offerings and registration. These policy statements follow on from the SEC's withdrawal of Staff Accounting Bulletin No 122, which had effectively prohibited financial institutions from providing crypto custody and related services. The Commodity Futures Trading Commission (CFTC) has also instituted policy and regulatory changes that should further drive growth and innovation in the digital asset markets.

US banking regulators have also shown a new openness to crypto assets and blockchain. Both the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) have issued interpretive letters rescinding prior letters that foreclosed meaningful participation by banks and other regulated financial institutions in the digital asset sector. The Federal Reserve announced the withdrawal of a series of highly restrictive prior guidance letters for banks related to their crypto-asset and stablecoin activities, and the DOJ released a memo for department employees, titled "Ending Regulation by Prosecution," outlining refocused digital asset enforcement priorities that will likely narrow crypto prosecution by focusing on cases involving fraud.Action to date has not been limited to the regulatory agency sphere. There are currently two draft bills working their way through Congress with bi-partisan support that provide a framework for the regulation of stablecoins – STABLE Act and GENIUS Act. In addition, work continues on the development of broad legislation addressing digital act market structure and regulation.

In parallel, however, certain states have begun to bring investigations and announced their intention to "fill [the] enforcement vacuum left by federal regulators who are abandoning these cases under Trump administration." For example, Oregon's Attorney General recently filed a lawsuit against a leading exchange and participant in the crypto markets.

Competition Law Enforcement in the Tech Sector

The DOJ and the FTC have continued to pursue the antitrust enforcement actions that were ongoing at the time of the presidential transition, with little change in course from the previous administration. In April 2025, hearings began in two cases that were initially filed toward the end of the first Trump administration:

- the FTC's case against Meta, in which the FTC alleges that the company has monopolized personal social networking services and seeks a breakup of the company; and
- the DOJ's remedy hearing against Google related to Google Search, in which the DOJ is seeking divestiture of Google's Chrome browser and other remedies following a judicial decision in 2024 finding that Google had monopolized online search markets.

The rulings in these cases will significantly impact the tech sector.

The current leadership at both the DOJ and the FTC have indicated that they will continue to follow the 2023 Merger Guidelines, which were circulated jointly by the agencies under prior leadership, to maintain stability in merger guidance across administrations.

The agencies continue to indicate that they will prioritize enforcement in the tech sector and in digital markets, with one key area of focus being the use of algorithmic technologies by competitors to coordinate pricing. A new area of concern under the Trump administration is the potential for digital platform operators to deny or limit users' access to their platforms, through censorship or other means, in particular, as a response to those users' speech or affiliations.

In the Context of World Events

Regulatory developments described in this briefing inevitably exist in the context of larger world events, which are complex, fast-moving and interwoven. For example, contemporaneously with Trump's inauguration, Chinese AI startup DeepSeek released its AU models, V3 (AI chat) and R1 (reasoning models) and quickly dominated world news and the stock market. Its models were seen to perform on par with OpenAI's and Google’s top models but at a fraction of the cost, challenging the narrative that innovation is extremely expensive. Marc Andreessen, from VC firm Andreessen Horowitz, posted on X: "DeepSeek R1 is one of the most amazing and impressive breakthroughs I’ve ever seen – and as open source, a profound gift to the world.” A series of tests and debates ensued and a recent Congressional report highlights that DeepSeek "represents a profound threat to our nation's security."

In a continued clash over digital regulation between the United States and the EU, the US government's Mission to the EU has reportedly reached out to the European Commission to request that the EU pause the implementation of its landmark Artificial Intelligence Act (AI Act) and to push back against the draft

AI code of practice for providers of advanced AI models being developed under the AI Act. This follows other heated exchanges and developments on EU tech regulation. Even before the Trump administration issued its recent tariff packages, it argued that fines under major EU tech legislation – such as the Digital Markets Act (DMA) and the Digital Services Act – equated to tariffs or taxes imposed on US businesses. Foreign regulations governing digital services were one of the hot points called out in Trump's memorandum of February 21, 2025 Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties.

These comments from the United States did not prevent recent fines against US Big Tech, triggering further criticism and claims of extortion from the US administration -- on April 23, 2025, the European Commission announced the first-ever fines for breach of the DMA: EUR 500 million against Apple and EUR 200 million against Meta, respectively, following a process that lasted over a year.

In contrast, some significant policymakers have been unexpectedly quiet about upcoming measures. On April 28, 2025, the new German government approved its policy plans for the next four years. Despite having been negotiated in the middle of the current trade climate, the coalition agreement between German Conservative and Social Democratic Parties does not reference the current environment and what strategy the new German government may wish to apply, beyond a very general intention to avoid a trade conflict and reduce tariffs.

More generally, jurisdictions outside of the United States are also taking measures to enhance their competitiveness, digital sovereignty and strategic autonomy. This is the case for example in the EU, which is launching multiple strategies and initiatives in critical tech areas, such as AI, key tech infrastructure and assets including computing infrastructure and cloud and data centre capacity, cyber protection, strategic components like chips, data and quantum technologies, amongst others. In parallel, we are also seeing a move in the EU to simplify the existing tech rulebook and reduce the administrative and regulatory burden for businesses. Several initiatives have been launched, others are expected looking ahead. To what extent this can help alleviate some of the existing tensions remains to be seen. Irrespective, this is something businesses will want to track going forward.

For an overview of the AI Continent Action Plan, see our prior briefing.

Conclusion

The Trump administration's first 100 days have been extraordinary in many respects and its tech-related actions have reverberated both domestically and around the world. We expect the level of activity to continue across the areas highlighted in this briefing, as well as others, and we will continue to keep our clients informed on key insights and themes.

For an overview of Trump Administration's first seven days in office, see our prior briefing.

C L I F F O R D
C H A N C E

CONTACTS

AI

Devika Kornbacher
Partner,
Houston

T +171 3821 2818
E devika.kornbacher
@cliffordchance.com

Inna Jackson
Tech Knowledge & Innovation Attorney – Americas, New York

T +1 212 878 3292
E inna.jackson
@cliffordchance.com

Competition

Peter Mucchetti
Partner,
Washington, DC

T +1 202 912 5053
E peter.mucchetti
@cliffordchance.com

Timothy Lyons
Associate,
Washington DC

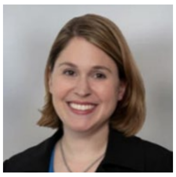
T +1 202 912 5910
E timothy.lyons
@cliffordchance.com

Data centers

Adriana Vélez-León
Associate,
Washington, DC

T +1 202 912 5173
E adriana.velez-leon
@cliffordchance.com

Data governance



Megan Gordon
Partner,
Washington, DC

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Brian Yin
Associate,
Washington, DC

T +1 202 912 5902
E brian.yin
@cliffordchance.com

Fintech

Steven Gatti
Partner,
Washington, DC

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Jesse Overall
Counsel,
New York

T +1 212 878 8289
E jesse.overall
@cliffordchance.com

CONTACTS CONTINUED

Policy

Phillip Souta
Global Director of Tech Policy, London

T +44 20 7006 1097
E phillip.souta@cliffordchance.com

Seika Osafune
Trainee Solicitor, London

T +44 20 7006 2775
E seika.osafune@cliffordchance.com

Tariffs

Janet Whittaker
Senior Counsel, Washington, DC

T +1 202 912 5444
E janet.whittaker@cliffordchance.com

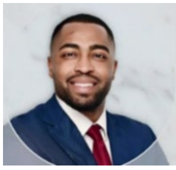
Mary Elizabeth Bultemeier
Associate, Washington, DC

T +1 202 912 5041
E maryelizabeth.bultemeier@cliffordchance.com

Trade and export controls

Renee Latour
Partner, Washington, DC

T +1 202 912 5509
E renee.latour@cliffordchance.com



Curtis Sails III
Associate, Washington, DC

T +1 202 912 5193
E curtis.sailsiii@cliffordchance.com

Nicolas Friedlich
Associate, Washington, DC

T +1 202 912 5197
E nicolas.friedlich@cliffordchance.com

Martina Kneifel
Associate, New York

T +1 212 880 5692
E martina.kneifel@cliffordchance.com

Global Perspectives

Alex Kennedy
Knowledge Director – CE Tech Group, Paris

T +33 1 4405 5184
E alexander.kennedy@cliffordchance.com

Torsten Syrbe
Partner, Düsseldorf

T +49 211 4355 5120
E torsten.syrbe@cliffordchance.com

Michel Petite
Of Counsel, Paris

T +33 1 4405 5244
E michel.petite@cliffordchance.com

Lei Shi
Managing Partner, Mainland China

T +86 21 2320 7377
E lei.shi@cliffordchance.com

Kimi Liu
International Partner (Shanghai He Ping Law Firm)

T +86 10 6535 2263
E kimi.liu@cliffordchancehp.com