STINSON

News & Insights

Trump's First 100 Days: Intellectual Property, Artificial Intelligence and Cybersecurity

Analysis of New Administration
12.09.2024

During his first term, Trump appointed a U.S. Patent and Trademark Office (USPTO) director who instituted a number of reforms widely regarded as pro-patent, and the general consensus is that the incoming administration will be more pro-patent than the outgoing one. The more significant shift in IP&T policy will come from rapid advancements in artificial intelligence, as Trump has indicated he will rescind Biden's executive order on AI to drive innovation, particularly as it relates to national security.

AT A GLANCE

- Patent stakeholders will be watching to see if Trump restores standard essential patent (SEP) policy that favors an owner's right to enforce their SEP against implementers.
- Trump is expected to pivot from the Biden administration's focus on ethical AI governance toward a more hands-off approach aimed at advancing technological supremacy over China.
- Regardless of what actions the incoming administration and Congress take, state laws and real world threats will encourage organizations to continue to invest in data privacy and cybersecurity.

PATENT RIGHTS

The general consensus is that the second Trump administration will be more pro-patent than the outgoing Biden administration. During his first term, Trump appointed Andrei Iancu to be the next Under Secretary of Commerce for Intellectual Property and Director of the USPTO. Iancu instituted a number of reforms widely regarded as pro-patent, enhancing Patent Trial and Appeal Board regulations and reducing the number of patent applications and appeals awaiting settlement.

Although Trump is yet to tap anyone to lead USPTO, stakeholders in the patent system will be watching to see if his administration will:

- Restore standard essential patent (SEP) policy that favors an owner's right to enforce their SEP against implementers.
- Reverse the Biden administration's "march-in rights" guidance that established a process for taking back patents for certain drugs developed with government funding.
- Appoint another USPTO director who, like Iancu, will institute additional pro-patent reforms.

Finally, there are a number of patent bills pending in Congress to reform the laws around subject matter eligibility, the Patent Trial and Appeal Board and the right of a patent owner to obtain an injunction against infringement. The Trump administration has not yet taken a position on these bills, all of which have the potential to shift the playing field in favor of the patent owner.

ARTIFICIAL INTELLIGENCE

Under Trump, AI policy is poised for a dramatic shift with significant implications for business strategy, regulatory landscapes, and international trade. President Trump is expected to pivot from the Biden administration's focus on ethical AI governance toward a more hands-off approach aimed at advancing technological supremacy with a focus on national security.

Driving Innovation Through Deregulation

This shift may begin with the reversal of Biden's executive order on AI, signaling a reduced emphasis on such considerations as privacy, transparency and bias in favor of accelerating AI innovation. The overarching goal will likely be to solidify U.S. dominance in the global AI race and compete with China.

For businesses, this shift could lead to faster development and deployment of AI technologies by easing compliance burdens, especially in consumer-facing sectors like healthcare, education and finance. However, companies in national security-sensitive industries, such as defense contractors, may face increased scrutiny when it comes to technology transfers and foreign partnerships. This dual approach highlights the administration's broader strategy to drive economic growth through innovation while safeguarding critical technologies from adversarial access.

Elevating National Security Priorities

Biden's executive order touched on national security and competition with nations like China, but Trump has made these a central part of his political platform, promising to counter China's access to U.S. technological advancements. His administration is expected to impose tighter export controls on critical

AI technologies and implement stricter limits on foreign investments in U.S. technology companies. Tariffs and other trade measures may further restrict Chinese entities from leveraging U.S. innovations, signaling an aggressive effort to safeguard critical technologies.

For businesses, this policy shift could result in heightened scrutiny and compliance requirements, particularly in industries like semiconductors, advanced computing and defense. Export controls and trade barriers may disrupt supply chains, elevate operational costs and complicate international trade. Companies with global operations or customers in China should prepare to navigate an increasingly complex landscape, proactively manage risks and adapt strategies to ensure compliance with evolving regulations.

Boosting Investment in Tech Infrastructure

To counter China's growing AI capabilities, Trump's administration is expected to prioritize domestic investment in AI innovation. Federal funding will likely focus on infrastructure—data centers, energy systems and semiconductor production—alongside AI technologies with military and national security applications. Investments in emerging fields like quantum computing may accelerate, given the potential to revolutionize AI and cybersecurity. Businesses in defense, technology and advanced computing could see increased opportunities through government contracts in areas that could counteract cyberattacks or enhance border security and immigration enforcement such as predictive analytics, facial recognition and surveillance systems.

However, companies may also face challenges from rising production costs tied to domestic manufacturing incentives and trade policies. Also, tighter export controls could complicate operations for businesses with global supply chains or customer bases, requiring careful adaptation to align with evolving compliance demands.

Additionally, the U.S. Copyright Office (USCO) is set to release key reports on Copyright and AI in 2025. These will address issues such as the copyrightability of AI-generated materials and the implications of training AI on copyrighted works. Businesses leveraging AI should closely monitor these developments, as they could influence strategies for protecting intellectual property and navigating compliance risks.

In the first 100 days and beyond, companies must remain agile and informed of key developments relating to AI policy. Proactively engaging with policymakers, adapting strategies to align with regulatory developments and carefully assessing operational risks and opportunities will be critical. By staying ahead of these changes, businesses can both safeguard their competitive position and capitalize on the global opportunities AI has created.

Trump's First 100 Days: Intellectual Property, Artificial Intelligence and Cybersecurity

DATA PRIVACY & CYBERSECURITY

Congressional Action on Data Privacy

A number of bills have been proposed in both the House and Senate over the past several years; however, there has been little to no movement since California lawmakers passed the first-of-its-kind California Consumer Privacy Act in 2018. Today, 19 states have their own privacy laws. Despite one-party control of Congress, data privacy experts doubt a comprehensive federal privacy bill is a priority for the incoming administration.

It's more likely Republicans will halt consumer protection initiatives related to data privacy. Two days after the election, Sen. Ted Cruz, R-Texas, sent FTC Chair Lina Khan instructions to "immediately stop all work on outstanding rules, regulations and guidance" and "focus only on matters at that are uncontroversial and would be approved unanimously by all members," warning that any FTC action taken now will receive "particular scrutiny."

However, a roll back of the FTC's data privacy or data security oversight in the U.S. is unlikely to affect the continually building wave of class-action lawsuits for data breach and data privacy violations that companies will continue to grapple with in the coming years.

Spotlight on Cybersecurity

Cybersecurity should remain a top issue for organizations during the Trump presidency, if only for self-preservation. Companies must build and maintain resiliency against outside threat actors and the increasing risk of class action litigation. In his first term, Trump favored a strong defense, establishing the Cybersecurity and Infrastructure Security Agency (CISA). However, despite CISA's explicit mandate to protect the functioning of US critical infrastructure, Trump officials have noted their disdain for the agency, with Trump famously firing its director in a tweet. It is unclear whether the incoming administration will take a strong stance on cybersecurity, though costs and risks continue to mount for businesses and citizens alike.

The Trump administration may roll back certain federal rules requiring organizations to protect against and report cybersecurity incidents, in particular the Securities and Exchange Commission's new rules for reporting "material cybersecurity incidents." However, well-established rules like the Health Insurance Portability and Accountability Act (HIPAA) are expected to remain, as well as state laws requiring the disclosure of data breaches to those affected and to state attorneys general. In addition, most contracts today between organizations include notice requirements around systems failures and cybersecurity incidents. Such notices allow an entity providing data and systems access to a third party to hold that third party accountable in the event of a breach. Without such language, an organization is left holding the bag

for a breach it was not responsible for.

Cybersecurity experts are concerned these measures to roll back security requirements will encourage lax cyber resilience and encourage ransomware and other cyberattacks, particularly from state-sponsored threat actors from Russia, China and Iran. Even with less federal regulatory oversight to require such protective measures, forgoing adequate cybersecurity has become practically untenable for most organizations who cannot risk losing personnel data, customer lists, proprietary knowledge and intellectual property in increasingly sophisticated cyberattacks.

This article is part of a broader analysis examining the anticipated challenges and opportunities created by an administration change. Attorneys from several different practice areas contributed to this series of article across multiple legal areas.

RELATED CAPABILITIES

Artificial Intelligence

Cybersecurity & Data Privacy

Intellectual Property & Technology

Patent Litigation

Patent Preparation & Prosecution

Post-Grant Proceedings