May 2025

National Security Implications of Foreign Third-Party Litigation Financing

PERSPECTIVE

American Security Project

National Security Strategy

In this Report

Third-party litigation financing (TPLF) allows outside investors to fund the attorneys' fees and expenses incurred in another party's lawsuit. While TPLF can broaden access to legal recourse, its unregulated and generally unreported status raises concerns that U.S. adversaries and competitors could be using this practice to steal or misappropriate intellectual property (IP), obtain confidential business or industry information, and harass U.S. businesses and even entire industries without oversight or accountability.

The potential for states like Russia and China to use TPLF as a conduit for economic espionage, especially in critical technology sectors such as AI, pharmaceuticals, and chip manufacturing, presents a potential threat to U.S. strategic interests. This is particularly true in the context of patent litigation, which accounted for 19% of all third-party litigation funding capital in 2023. Drawing on a review of the literature, legal databases, and interviews with industry stakeholders, the paper outlines how TPLF may be exploited to access sensitive intellectual property and recommends targeted policy responses to mitigate these risks.

IN BRIEF

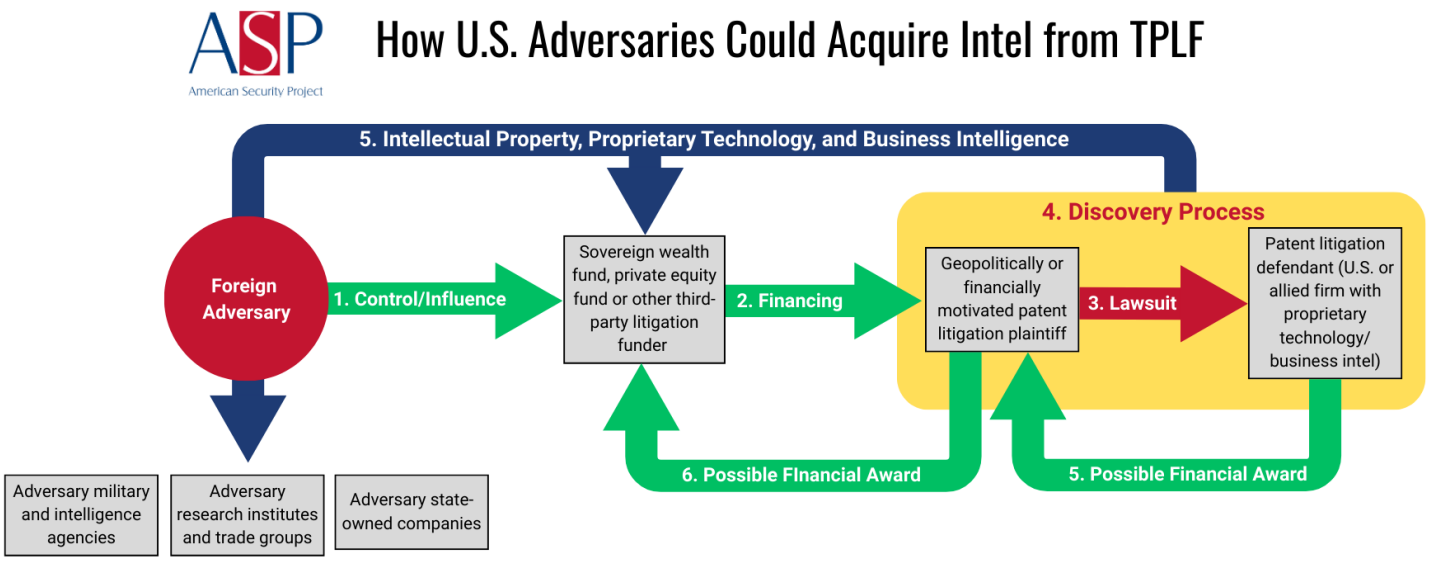
- The current lack of disclosure requirements for foreign TPLF presents a vulnerability that could be used to exploit the legal system for the purpose of committing economic or industrial espionage and subsequently threaten U.S. national security.
- Smaller companies are more sensitive to patent litigation costs and lawsuits and, with fewer specialized in-house litigation personnel, are susceptible to exposing confidential information through senior staff or leadership.
- Empirical data on whether TPLF is being used by foreign entities for nefarious purposes is lacking due to the confidential nature of the discovery process in U.S. federal courts. More research should be conducted to develop actionable measures to reduce exploitable vulnerabilities.
- The cost of litigation is significant, reducing the likelihood that a for-profit company will frivolously spend capital on lawsuits to simply harass without a high chance of return on investment.
- Instituting reasonable, targeted reforms will help preclude the risk of foreign TPLF exploiting the legal system to inflict harm on U.S. national security, while maintaining the legitimate need for recourse on patent infringement.

About the Author

Peter Charles Choharis is an ASP Adjunct Fellow and the founder of an international law firm in Washington, D.C. He has been a U.S. litigator for decades and published the first law review article on investing in litigation in the Yale Journal on Regulation. He has also published dozens of articles on U.S. foreign policy, national security, and international law, including in The New York Times, Wall Street Journal, Washington Post, Los Angeles Times, National Interest, and scholarly legal publications.

Introduction

Third-party litigation financing (TPLF)[1] allows outside investors to fund the attorneys' fees and expenses incurred in a lawsuit, instead of plaintiffs funding the litigation themselves or attorneys funding the lawsuit by means of a contingency fee arrangement.[2] Should the plaintiff prevail, the damages collected are used to repay a non-recourse loan plus an additional amount reflecting the risk and time value of money—whether calculated as interest, a multiplier of the loan amount, or a percentage of the recovery.[3]



TPLF agreements are typically confidential and not disclosed to the defendants, the court, juries, or the broader public, making these arrangements difficult to analyze.[4] In 2023, there were thirty-nine active third-party litigation funders who made 353 new investments with $15.2 billion in assets under management. Patent litigation was the most common type, with 19% of capital going to these cases. The average investment in a single lawsuit was $4.8 million.[5]

Some argue that the lack of transparency surrounding TPLF, coupled with the threats posed by Chinese economic espionage and Russian foreign interference, can pose national security concerns by enabling access to sensitive information[6] and by using litigation to harass U.S. companies,[7] especially startups and small to medium-sized enterprises (SMEs) in the critical technology sector.[8] In September 2023, Senators John Kennedy (R-LA) and Joe Manchin (D-WV) introduced legislation to address some of these concerns, by requiring disclosure of foreign funders of U.S. lawsuits and by making "unlawful" any agreement to pay proceeds from a civil action funded by "money that has been or will be directly or indirectly sourced" from "a foreign state or a sovereign wealth fund."[9] This bill was recently re-introduced in 2025 by Representative Ben Cline (R-VA).[10]

A primary concern is that outside funding of patent litigation enables companies owned or controlled by U.S. adversaries to gain access to valuable intellectual property (IP) that is sensitive to U.S. national security interests.[11] IP that might implicate U.S. national security would include a wide range of U.S. industries,[12] such as artificial intelligence (AI), supercomputing, pharmaceuticals, computer chip manufacturing, and aeronautics, among others. These national security risks are especially acute for manufacturing processes, which enable rivals to create the stolen product more quickly, cheaply, and accurately. And while national security interests appear to be the most heightened concern, U.S. economic security may also be at risk, given how crucial the IT sector is to American economic growth.

In short, the worry is that TPLF provides a legal mechanism for U.S. adversaries to conduct industrial espionage to the detriment of the United States and its security interests.

This paper explores how serious these threats might be to the United States. Our analysis draws on a review of the research literature, a review of some relevant databases,[13] and interviews[14] with market participants—including a prominent U.S. company that has been a frequent target of patent lawsuits funded by third parties and legal counsel for TPLF firms operating in the U.S. that specialize in IP litigation. Despite the limited scope of research and limited transparency in civil litigation proceedings, we make numerous recommendations in Section 5 to address the national and economic security concerns that may arise in some third-party litigation funded lawsuits. We also recommend a more comprehensive study to gather additional data and strengthen awareness of this issue.[15]

Potential Risks: Third-Party Financing of Patent Cases

Critics of third-party litigation funded patent cases tend to raise three national security concerns: (1) theft or misappropriation of IP; (2) theft of confidential business or industry information; and (3) harassment of U.S. businesses and even entire industries.[16] TPLF defenders argue that, to the extent that any of these problems exist, they are a function of U.S. civil litigation rules of evidence and procedure and that TPLF does not have a material impact on patent litigation.[17]

Under U.S. patent laws, a patent may be assigned or sold to another entity that had nothing to do with the development of that patent. There are several justifications for permitting someone to acquire a patent and then challenge another patent holder's patent rights, such as providing liquidity for a company that is not otherwise commercially exploiting a patent and preventing overly broad patent claims that would crowd out innovation. On the other hand, defendant companies have long chafed at the time and expense of defending against a person or company that acquires a rival patent and then brings a lawsuit to challenge a defendant company's patent, with such patent plaintiffs sometimes derogatorily referred to as "patent trolls."

But a relatively new development is for private equity funds to invest in firms that employ patent experts to identify third-party patents that may be violated by another patent holder.[18] Private equity and other investors invest in third-party litigation funders, sometimes more than one such funder. These third-party litigation funders then form a Limited Liability Company (LLC) to acquire the patent(s) from a company that is not commercially exploiting these patent rights. The money received from the LLC gives that company some liquidity for an unutilized asset—one or more of their former patents. The LLC—what the industry calls a "PAE" or Patent Assertion Entity—then files a lawsuit in a U.S. federal court, thereby becoming a plaintiff. This plaintiff LLC-PAE brings claims that some other company's patent infringes on the patent(s) that were acquired by the newly created plaintiff LLC-PAE. This plaintiff seeks damages against the competing patent holder, who is now a defendant in the lawsuit. Depending on the case, damage claims can be hundreds of millions of dollars or more.[19]

Once a patent case hits the discovery phase, the plaintiff's attorney can uncover details about the patented product or process in several ways. Written discovery can seek extensive information about the nature of the actual product and process that might not otherwise be available. The plaintiff LLC can also depose a defendant company's employees regarding the patent. Furthermore, both the TPLF-funded plaintiff and the defendant company whose patent is being

challenged can employ one or more expert witnesses to analyze technical information about the product or process that has been patented. The materials that such expert witnesses review, the information they may provide in a report, and the testimony they provide from being deposed can also yield an enormous amount of non-public information.

While courts typically adopt protective orders to limit the disclosure of confidential information during discovery, such orders cannot protect against mistakes, hacking, or a nefarious actor purposely transferring the information to a third party, including a U.S. competitor or adversary. As discussed below, in addition to violating a protective order, the intentional or knowing disclosure of confidential information about patented products and processes to a foreign entity could constitute economic espionage under the Economic Espionage Act, which carries hefty criminal penalties.

China's J-35 (FC-31) fighter likely incorporates hacked U.S. F-35 designs stolen in 2009, illustrating the consequences of illicitly acquiring sensitive national security information. Image credit: China News Service via Wikimedia Commons CC Attribution 3.0 Unported

Disclosure of highly sensitive information about patented products and processes that have national security implications presents one set of concerns. In addition, confidential business information can be gleaned from certain kinds of discovery,[20] and some have expressed fears that TPLF may be used to harass established U.S. businesses as well as suppress startup innovation.[21]

Competing Views on Third-Party Patent Litigation Financing

Arguments for Third-Party Litigation Financing

Supporters of third-party litigation financing point out that abuses or national security threats posed by patent litigation could exist whether or not a plaintiff is funded by an investor. They posit that there is currently no publicly available evidence of a foreign adversary using TPLF to obtain sensitive IP through discovery; therefore, there is no clear national or economic security risk to the United States.[22]

Additionally, TPLF funders argue that their goal is to be profitable. Private firms have a duty to their investors to exercise sound business judgment and not engage in nefarious conduct on behalf of a foreign adversary.[23] Bringing patent litigation to obtain non-public IP or other confidential information or to use patent litigation to harass legitimate patent holders or suppress U.S. innovation would be counter to their goal of profit maximization.[24]

TPLF supporters interviewed for this report point out that the cost of patent litigation can be substantial—as much as $8-10 million, depending on the particular litigation and what fees and expenses are included. This means that the size of a patent litigation portfolio for even large TPLF firms is limited to about forty to fifty cases. Thus, individual TPLF firms have insufficient capital to bring non-meritorious lawsuits that have little chance of success. In other words, there is no financial incentive to use patent litigation for nefarious purposes in aid of America's foreign adversaries.[25] Finally, TPLF backers say that while patent litigation could, in theory, provide a mechanism to obtain improperly IP or other confidential information, there are several more effective and less expensive measures to obtain

that same information—including hacking, traditional industrial espionage, and other illicit means.[26] TPLF, they argue, does not change the equation regarding national security vulnerabilities that may result from patent litigation.

Arguments Against Third-Party Litigation Financing

Critics of third-party litigation financing argue that both TPLF financings and patent litigation are too opaque to ascertain the actual risks posed by both to U.S. national and economic security.[27] Identifying a case where a foreign funder obtained sensitive IP or business intelligence during discovery would be extremely difficult, because much of federal discovery is non-public and, in the patent context, almost always involves protective orders that require confidentiality. However, a lack of evidence regarding TPLF furthering national and economic security threats does not indicate that no threats exist, but rather, that it is too difficult to collect such information. Critics also say that whatever the current security threat, there is nothing to prevent foreign adversaries from employing TPLF methods for IP misappropriation, technology transfer, competitive advantage, or other strategic goals or illicit purposes instead of for profit.[28]

"...a lack of evidence regarding TPLF furthering national and economic security threats does not indicate that no threats exist, but rather, that it is too difficult to collect such information."

Critics further argue that TPLF methods provide foreign adversaries with anonymity and plausible deniability so that they may operate clandestinely and with less risk than traditional corporate espionage methods.[29] They also argue that protective orders are not always adequate to safeguard sensitive IP since accidental disclosures can occur. Policing purposeful disclosures in violation of a protective order can be challenging, as law firm files have been hacked and sanctions can fail to dissuade intentional abuse.[30] While these shortcomings might be endemic to patent and other kinds of U.S. civil litigation, by expanding the number of cases and providing a clandestine means, TPLF-funded patent litigation enhances the risk of highly sensitive information being released.

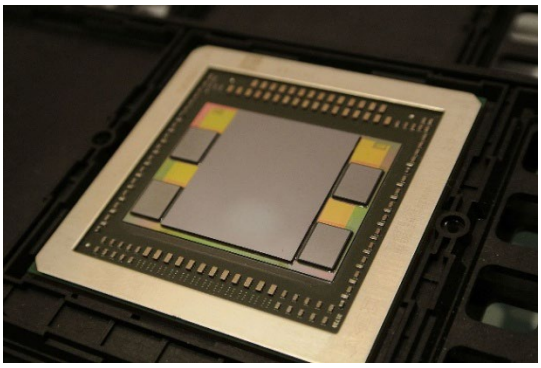
Findings and Observations

The extent of the threat to U.S. national security posed by TPLF of patent litigation is unclear and will remain so under current federal rules governing civil litigation. This is so for several reasons. The first is that the existence of TPLF in a case is typically not disclosed. In addition, disclosure of discovery results in U.S. civil litigation is usually limited, and patent litigation invariably involves protective orders. Neither plaintiffs nor defendants have an interest in public disclosure about their discovery requests or responses. While there are a few databases that identify patent litigation brought by LLC plaintiffs, they link to public filings only. The author of this report conducted several interviews with past and current TPLF counsel; a patent counsel experienced in TPLF litigation; in-house patent counsel and other senior company officials at a leading technology company; and a patent research firm to gain valuable insights and perspectives. This information was non-public. No interviewee agreed to share detailed information about discovery requests, responses, attempted illicit conduct, or other issues—even confidentially. As for the public record, the current system makes it very difficult to obtain even anecdotal or generalized information about TPLF, especially involving highly sensitive IP.[31]

Nonetheless, the research does support a number of observations and conclusions.

Risk of Exposing Strategic Information

The potential national and economic security threats posed by patent litigation should not be understood as binary nor conceived too narrowly. There are many dual-use technologies that have both civilian and military applications. The People's Republic of China (PRC) has for years exploited a range of methods in the West, including open source information, academic research, and espionage to obtain information that could bolster its military and strategic posture.[32]



The AI industry could be a prime target for extracting strategic information, like proprietary GPU schematics. Image Credit C. Spille/pcgameshardware.de Wikimedia Commons. CC by-SA 4.0.

Furthermore, IP is not the only strategic information that could be compromised through TPLF patent litigation. The dangers of exposing patented technology regarding a weapons system, foreign surveillance, or data encryption techniques would clearly implicate U.S. national security, but so too would disclosing commercial information about the firms and sectors developing and deploying such technologies. For example, having non-public insights into the kinds of AI research being conducted in the U.S., the capital expenditures by large firms in the AI sector, R&D budgets, commercial opportunities, startup funding, AI infrastructure development, and similar subjects would be quite helpful to U.S. adversaries.

This is especially so because the governments of two of America's foreign adversaries—the People's Republic of China and the Russian Federation—have extensive influence and, on some matters, actual control over their commercial industries. In the PRC, the government acting through the Chinese Communist Party has adopted both *de jure* influence[33] over virtually all high-tech companies and *de facto* control over their governance.[34] This extends to a vast array of sectors, including the internet generally, social media, and AI. The People's Liberation Army has partnered with or directed a host of Chinese firms to weaponize IT technologies,[35] so the possibility of the PRC employing government-controlled commercial entities to exploit TPLF is not far-fetched.

In the last few years, both the PRC and Russian oligarchs have used TPLF to fund civil proceedings in the U.S. and elsewhere. The two examples below illustrate that well-funded organizations in both the PRC and Russia are aware of and have already used TPLF in the U.S. to further their aims. They also raise the possibility that Russia or the PRC might use TPLF to pursue more nefarious objectives.

Case #1: Litigation Financing as a Potential Means of Evading Sanctions

A1, a Russian firm, funded lawsuits in London and New York both before and after three of its oligarch founders were sanctioned in the U.K. and U.S. following Russia's invasion of Ukraine.[36] A1 reportedly spent approximately $20 million in bankruptcy cases in both New York and London "on behalf of a Russian [regulatory] agency seeking to recover assets" from two Russians "accused of embezzling more than $2 billion from a Moscow bank."[37] A1 continued its funding even after three of its founders and a company associated with it were sanctioned. But prior to the Russian invasion and subsequent sanctions, A1 had "consistently won approval in New York state and federal courts to liquidate" the accused embezzler's assets.[38] The A1 saga has raised concerns that TPLF can enable sanctions evasion and money laundering. It also demonstrated that Russian firms could engage in U.S. litigation to pursue interests that may not be purely commercial.

Case #2: Litigation Financing as a Potential Tactic to Probe Patent Information

Purplevine IP, a PRC company, reportedly underwrote the cost of a number of lawsuits brought by a tech company, Staton Techiya, whose majority owner is a Florida private equity fund, against Samsung.[39] Although it appears that the lawsuits concerned sound technology for earbuds, tablets, and other devices and did not involve IP implicating national or economic security,[40] it is possible that the Purplevine financing was in part an effort to probe how much information can be derived about a patent through litigation.

Impacts on Small and Medium-Sized Enterprises

Unlike large defendant companies in patent litigation, such as Samsung in *Staton Techiya v. Samsung,* funded by Purplevine, it is much more challenging for startups and small and medium-sized companies who are sued in patent litigation to preserve confidentiality. Not only are smaller companies very sensitive to patent litigation costs, but such litigation could also scare away investment funding.[41] Furthermore, large companies with extensive patent portfolios have separate, dedicated persons in their general counsel office to respond to discovery, thereby compartmentalizing who responds to discovery and how discovery requests are managed.[42] By contrast, small companies and startups do not have the personnel or financial resources to sequester information in the same way. Instead, they must expose senior company officials to depositions, which can lead to the disclosure of a broader range of confidential information.

In theory, protective orders can limit disclosure to the plaintiff's firm and experts who are conducting discovery, and all confidential information is supposed to be returned or destroyed at the end of litigation. But there are unethical lawyers and experts, especially when confidential information could be worth vast sums of money or used to further the national security interests of a foreign adversary with whom the lawyers or experts may sympathize. It is even conceivable that a foreign attorney with relevant IP expertise will join the U.S. plaintiff's lawyers and function as a conduit for the defendant's trade secrets. Finally, accidental disclosure can happen, albeit rarely.[43]

The Potential of TPLF to Promote Economic Espionage

The Economic Espionage Act ("EEA"), 18 U.S.C. § 1831, provides criminal penalties for anyone who knowingly steals, copies, or misappropriates a trade secret for the benefit of a foreign government; a foreign firm or company that is "substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;" or a foreign agent. Depending on the facts, the EEA could apply to the intentional disclosure of patented products and processes produced during discovery to a foreign government, agent, or organization. With criminal penalties of "$5,000,000 or imprison[ment of] not more than 15 years, or both" for individuals and "$10,000,000 or 3 times the value of the stolen trade secret" for an organization,[44] the EEA can be a strong deterrent.

That said, industrial espionage by countries such as China remains a substantial problem,[45] so the EEA clearly has not stopped foreign adversaries from seeking information that implicates U.S. national and economic security. Furthermore, even if sensitive information obtained through discovery and then misappropriated to a foreign competitor does not violate the EEA because it did not benefit a foreign government or instrumentality, disclosing that confidential information to a foreign commercial competitor may still pose a risk to U.S. national or economic security.

When national and economic security is at stake, it is reasonable to ask whether existing litigation protections are sufficient to protect against a determined effort by a foreign adversary to acquire patent-protected information. This question is not theoretical, given the participation of foreign sovereign wealth fund investors in third-party litigation funding.[46] A recent example would be Abu Dhabi's sovereign wealth fund investment arm, Mubadala Investment Co., which acquired Fortress Investment Group last year.[47] Fortress financed[48] a U.S. patent holder's infringement case against Samsung last December.[49]

Risks of Litigation Harassment

Finally, the claim that litigation "portfolio funding encourages funding [of] low-merit or even frivolous claims as part of the speculative market that TPLF is creating inside the litigation system" is belied by industry data.[50] Professor Donald J. Kochan does not provide a source in support of his argument, and the data shows the opposite.[51]

The size of their portfolios suggests that TPLF funders must employ heightened due diligence to bring cases that they believe are the most meritorious and lucrative. Based on the 2023 data cited above, each of the 39 active third-party litigation funders had an average of roughly $390 million in assets under management to deploy. This amount is not inconsiderable, but it is quite small by private equity standards. More importantly, the data shows that these 39 funders together made 353 new investments in 2023, which means that, on average, each third-party litigation funder invested $4.3 million in each of the 9 cases that they filed in 2023. That is too small of a portfolio and too small of a financial cushion to be reckless. Put simply, an average of 9 new cases annually is too small of a portfolio to alter third-party litigation funders' risk calculus and fund what were formerly "too-risky-to-fund" cases.[52] And while averages may not provide a complete picture since some of the larger TPLF firms have access to more capital and can bring more cases,[53] the number of cases and investment capital is still so limited that it is far more rational to invest in a small number of potentially high-value cases (calculated by multiplying potential damage awards by the chance of success) than to invest limited resources in lots of high-risk cases in hopes of getting lucky.

Reporting on the TPLF industry seems to support the above analysis.[54] Where portfolio risk diversity does take place is not at the third-party litigation funder level, but rather at the level of the investors in third-party litigation funds. Such investors often invest in several funds and consider such investments as uncorrelated to financial markets (*i.e.*, as having a low or zero "beta" in finance terms).[55]

Furthermore, 284,220 civil cases were filed in the United States in 2023,[56] which means that 0.124% of the civil cases filed in the U.S. in 2023 received third-party litigation funding. Only 19% of these were patent cases, meaning that the 67 patent cases that received TPLF funding in 2023 constituted 0.0236% of the total civil cases filed that year. This is not to say that abuses do not occur, and prevailing defendant companies must still pay litigation fees and expenses. But it does undermine the idea that there is a threat to our justice system that needs a systemic remedy. As the above data shows, the limited number of funders, cases, and capital, in turn, limits the size of litigation portfolios of the third-party litigation funders. As a result, the human and financial capital are insufficient to bring large numbers of weak or meritless claims in hopes of getting lucky. That does not mean that such awards do not take place, but in the patent context, the U.S. Court of Appeals for the Federal Circuit which hears patent appeals is well-positioned to reverse meritless jury awards.

Recommendations

From a public policy perspective, an unclear evidentiary record about the extent of national security threats posed by TPLF patent litigation does not preclude good faith reforms—especially when U.S. national and economic security may be at risk. Given the extensive record of industrial espionage by some of our foreign adversaries, it would be folly to wait until vulnerabilities in our civil litigation system are exploited before acting. But we also do not want to restrict patent litigation based on speculation or just because some cases may be third-party funded or involve sensitive IP. The question is: What targeted measures will address potential national and economic security threats posed by TPLF patent litigation while still allowing a robust legal system to vindicate patent rights? It is also true that U.S. national and economic security will be promoted by allowing legitimate patent holders to challenge patent infringements. For smaller companies, obtaining third-party funding may be the only practical means for them to protect their patent rights. And even larger companies must retain the ability to bring good faith patent claims against their competitors, including companies owned by foreigners.

It is with these goals in mind that we offer four potential reforms for further inquiry and debate.

1. Require disclosure of third-party financed litigation.

Chief Judge Connolly of the U.S.D.C. of Delaware has a standing order that requires a party receiving litigation funding to file a statement setting forth identifying information about the funder; whether the funder's approval is required for litigation or settlement decisions and the terms of such approval; and a "description of the nature of the financial interest" of the funder.[57] The order also permits discovery regarding the funding terms under some circumstances. This order is not restricted to patent litigation but instead applies to all cases before Chief Judge Connolly. The U.S. District Court for the District of New Jersey[58] and the U.S. District Court for the Northern District of California[59] require similar disclosure of outside financial interests.

Chief Judge Colm F. Connolly

On October 10, 2024, the U.S. Judicial Conference's Advisory Committee on Civil Rules agreed to create a subcommittee to examine TPLF,[60] but that process will likely take several years. To reach an informed understanding of how TPLF functions and what problems, if any, exist, the subcommittee will need empirical data, not simply a forum for various stakeholders to argue their respective cases. To generate data quickly, the Judicial Conference should encourage more District Courts to adopt the kind of disclosure required by the New Jersey U.S. District Court. Another way of generating data would be for half of the judges of a District Court to adopt Local Rules like those of Judge Connolly and the other half not to require such disclosure. The U.S. District Court for the Eastern District of Texas, which has become a common forum for patent cases, would be a good place to generate such comparative data.

Indeed, required TPLF disclosure to a court may not be very controversial (although disclosure to a jury could raise some problems). TPLF can indicate that the plaintiff is serious, has the resources to fight, and therefore may foster faster and fairer settlement, particularly against a larger defendant.[61] Conversely, learning more about a plaintiff's resources, decision-making, and other information would be helpful to a patent defendant.[62]

2. Require disclosure of information relevant to U.S. national and economic security and adopt specialized discovery procedures.

Another type of disclosure would permit either plaintiffs or defendants to disclose to the court that the patent litigation implicates national or economic security, along with an explanation and supporting evidence. The opposing party can either concur, object, or seek to modify the statement with its own evidence and the court could hold an evidentiary hearing if necessary. Once the court finds that the patent or related information may implicate U.S. national or economic security, it could then designate the information as "U.S. security sensitive."[63]

Courts can then adopt special discovery rules designed to protect such sensitive information, while still preserving the right of litigants to obtain information and the court's ability to ensure the "just, speedy, and inexpensive determination of every action and proceeding."[64] Rather than have individual District Courts or even judges issue their own rules, the Judicial Conference may be the appropriate body to amend the Federal Rules of Civil Procedure (FRCP) to tailor discovery of such sensitive information.

3. Impose strict penalties for intentional disclosure of information relevant to U.S. national and economic security.

Judges are traditionally reticent to sanction litigants and their counsel. But the duty to prevent the judicial system from being a means for foreign adversaries to breach U.S. national and economic security must become an intrinsic component of the judicial process. The vast majority of courts fully understand their duty and do their best to meet it. To assist them, the Judicial Conference should consider amending the FRCP to include strict, mandatory sanctions for intentionally violating protective orders or otherwise intentionally disclosing information that has been designated national security sensitive. Of course, for a knowing or intentional disclosure of a trade secret in violation of the EEA, a criminal referral would be warranted. The owner of the trade secret could also bring a civil claim for damages and injunctive relief for an EEA violation.[65]

4. Investigate foreign proceedings for similar vulnerabilities.

Both the PRC and Europe (especially Germany) are prominent *fora* for bringing patent claims. Patent litigation in those courts may also pose national security threats, especially when TPLF funders will sometimes bring the same or similar patent claims in different *fora*.[66] A comparative study of what takes place in these courts would be quite helpful for the U.S. to secure IP from misappropriation by U.S. adversaries bringing claims in foreign *fora*.

Conclusion

In light of extensive industrial espionage by foreign adversaries, the possible threat to U.S. national and economic security posed by TPLF patent litigation must be taken seriously. This is not the only way that foreign adversaries may exploit the U.S. judicial system to appropriate American IP, lawfully or unlawfully. However, it is a lesser-studied practice and one that may be occurring out of sight of U.S. regulators and the judicial system. Further research would yield important answers about the extent of the threat and appropriate, tailored responses that preserve the full due process rights of litigants in patent litigation. As an initial, relatively uncontroversial step to facilitate such research, U.S. District Court judges or the Judicial Conference should consider adopting disclosure rules for TPLF parties (at least in patent litigation) and making those disclosures public (at least at the conclusion of the litigation and exhaustion

of all appeals). Appellate courts or the Judicial Conference should consider adopting similar rules for third-party funding of appeals. This data can help Congress and the Judicial Conference assess how extensively foreign adversaries utilize TPLF patent litigation and the nature and extent of the threat to national and economic security. The Judicial Conference should then consider adopting specialized discovery rules to protect designated national security information, including rules to enforce those protections. Depending on the results of the study, Congress should consider barring foreign TPLF when IP that involves substantial national or economic security is at stake.

Endnotes

[1] This report addresses commercial litigation claims between commercial entities. TPLF is also available for consumer claims brought by one or more persons against a company or wealthy person(s). Third-party litigation funded class actions are arguably a third category or a hybrid, because the plaintiff class consists of a large number of individuals, the litigation funders are the large commercial lenders, and the aggregate damage claims are quite large. *See, e.g.*, U.S. Government Accountability Office, GAO-23-105210, "Third-Party Litigation Financing: Market Characteristics, Data, and Trends," (Dec. 2022) ("GAO Report"), *available at*: https://www.gao.gov/assets/gao-23-105210.pdf.

[2] *See generally* Prof. Victoria Sahani Written Testimony, Hearing on "The U.S. Intellectual Property System and the Impact of Litigation Financed by Third-Party Investors and Foreign Entities," House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet, United States House of Representatives (June 12, 2024), *available at* https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/Sahani%20Testimony.pdf.

[3] *See, e.g.*, GAO Report, *supra* n. 1, at pp. 8-10.

[4] *See id.*, p. 15.

[5] The Westfleet Insider, "2023 Litigation Finance Market Report," *available at* https://www.westfleetadvisors.com/publications/2023-litigation-finance-market-report/.

[6] *See* Thibault Denamiel, Matthew Schleich, and William Alan Reinsch, "Is Third-Party Litigation Financing a National Security Problem?" CSIS (Feb. 23, 2024).

[7] *See* Prof. Donald J. Kochan Written Testimony, Hearing on "The U.S. Intellectual Property System and the Impact of Litigation Financed by Third-Party Investors and Foreign Entities," House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet, United States House of Representatives, at p. 6 (June 12, 2024). Available at https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/Kochan%20Testimony.pdf.

[8] An academic study of Chinese patent litigation's impact on "micro and small-sized enterprises (MSEs)" found that "[w]hether winning or losing, defendant MSEs participating in litigation significantly inhibit their innovation performance at different levels." Yuting Den, Yong Qi & Qing Guo, "The Impact of Patent Infringement Litigation Decisions on Firms' Innovation Performance in China," Nature Portfolio, Scientific Reports (2024).

[9] S.2805 "Protecting Our Courts from Foreign Manipulation Act of 2023" U.S. Senate, Introduced September 14, 2023, *available at* https://www.congress.gov/bill/118th-congress/senate-bill/2805/text.

[10] H.R. 2675 "Protecting Our Courts from Foreign Manipulation Act of 2025," U.S. House of Representatives, Introduced April 7, 2025, *available at* https://www.congress.gov/bill/119th-congress/house-bill/2675/text#:~:text=Introduced%20in%20House%20(04%2F07%2F2025)&text=To%20amend%20chapter%20111%20of,funds%2C%20and%20for%20other%20purposes.

[11] *See generally* Michael E. Leiter, John H. Beisner, Jordan M. Schwartz, James E. Perry; Skadden, Arps, State, Meagher & Flom LLP; ILR Briefly, "A New Threat: The National Security Risk of Third Party Litigation Funding," U.S. Chamber of Commerce, Institute for Legal Reform (Nov. 2022), *available at*: https://instituteforlegalreform.com/wp-content/uploads/2022/11/TPLF-Briefly-Oct-2022-RBG-FINAL-1.pdf.

[12] *See* Camille A. Stewart, "Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings," 10 J. NAT'L SECURITY L. & POL. 277 n. 3 (2019).

[13] *See* Case List, Unified Patents, *available at*: https://portal.unifiedpatents.com/litigation/caselist.

[14] As a condition of speaking candidly and fully and to protect their respective employers, the interview subjects requested that their identities and employer information not be disclosed.

[15] *See* GAO Report, *supra* n. 1, pp. 15-18.

[16] *See* House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, "Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party" (Dec. 2023); John H. Beisner, Jordan M. Schwartz, Alexander J. Kaspari (Skadden, Arps, Slate, Meager, & Flom LLP), "Grim Realities, Debunking Myths in Third-Party Litigation Funding," U.S. Chamber of Commerce Institute for Legal Reform at pp. 12-19 (Aug. 2024).
[17] *See generally* Written Testimony Sahani, *supra* n. 2 at pp. 16-19 (describing TPLF in patent litigation).
[18] *See generally* U.S. Government Accountability Office, GAO-25-107214, "INTELLECTUAL PROPERTY Information on Third Party Funding of Patent Litigation," (Dec. 2024), available at https://www.gao.gov/assets/gao-25-107214.pdf.
[19] *See* Interview, Head of IP Policy, Fortune 100 technology company. Feb. 20, 2025 ("Head of IP Policy Interview").
[20] *See id.*
[21] *See id.*
[22] *See* Interview, Patent Attorney, private law firm partner, former TPLF in-house counsel. Mar. 6, 2025 ("Patent Atty. Interview").
[23] *See* Interview, TPLF in-house counsel, former private law firm managing partner. Jan. 16, 2025 ("TPLF In-house Counsel Interview").
[24] *See* Patent Atty. Interview, *supra* n. 22.
[25] *See* TPLF In-house Counsel Interview, *supra* n. 23.
[26] *See* Patent Atty. Interview, *supra* n. 22.
[27] *See* Interview, Chief of IP Litigation, Fortune 100 technology company. Mar. 6, 2025 ("Chief of IP Litigation Interview").
[28] *See generally* Kochan *supra* n. 7.
[29] *See* Hon. Bob Goodlatte Written Testimony, Hearing on "The U.S. Intellectual Property System and the Impact of Litigation Financed by Third-Party Investors and Foreign Entities," House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet, United States House of Representatives at p. 5 (June 12, 2024) (describing "Chinese firm, PurpleVine IP," as "bankrolling four patent infringement lawsuits in U.S. courts" and the TPLF litigation brought by VLSI Technology against Intel).
[30] *See* Chief of IP Litigation Interview, *supra* n. 27.
[31] *See generally* GAO Report, *supra* n. 1 at pp. 15-18.
[32] *See generally* Courtney Manning, "Code War" American Security Project (October 17, 2023), *available at* https://www.americansecurityproject.org/perspective-code-war-how-chinas-ai-ambitions-threaten-u-s-national-security/.
[33] *See, e.g.,* China's National Intelligence Law of 2017 obligates all Chinese organizations and citizens to collaborate with state intelligence operations. China Law Translate, "PRC National Intelligence Law (as amended in 2018)" (June 27, 2017), *available at* https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/. Also, in 2017, the PRC passed the National Cybersecurity Law, which "compels companies and individuals to make networks, data, and communications available to the police and security services." Law Info China, "Cybersecurity Law of the People's Republic of China" (Nov. 7, 2016), *available at* https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3. The Data Security Law of 2021 gives the PRC authority "to access and control private data, including China's 'national' data processed overseas." China Law Translate, "Data Security Law of the PRC" (June 10, 2021), *available at* https://www.chinalawtranslate.com/en/datasecuritylaw. China's recently revised Counter-Espionage Law of 2023 bolsters the state's authority, making clear that all technological developments, whether designed for civilian or military use, must be available to state security and intelligence services. China Law Translate, "People's Republic of China Counter-Espionage Law (2023 Edition)" (Apr. 26, 2023), *available at* https://www.chinalawtranslate.com/counter-espionage-law-2023.
[34] See Ryan McMorrow, Qianer Liu, and Cheng Leng, "China Moves to Take 'Golden Shares' in Alibaba and Tencent Units," FINANCIAL TIMES (Jan. 12, 2023), *available at* https:// archive.md/PmxYE; Foundation for Defense of Democracies, "5 Things to know about Bytedance, TikTok's Parent Company" (Mar. 12, 2024), *available at* https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company; Rachel Lee, Prudence Luttrell, Matthew Johnson, and John Garnaut, "TikTok, ByteDance, and Their Ties to the Chinese Communist Party, Submission [No. 34] to the [Australian] Senate Select Committee on Foreign Interference through Social Media" (Mar. 14, 2023) (the "Australian Report"), *available at* https://www.scribd.com/document/633015202/TikTok-ByteDance-And-Their-Tis-to-the-Chinese-Communist-Party.
[35] See Australian Report, supra n. 34; Nita Farahany, "TikTok is Part of China's Cognitive Warfare Campaign," Opinion, GUARDIAN (Mar. 25, 2023), *available at*: https://www.theguardian.com/commentisfree/2023/mar/25/tiktok-china-cognitive-warfare-us-ban; *see also* Bill Gerts, "Chinese 'Brain Control' Warfare Work Revealed," WASH. TIMES (Dec. 29, 2021) (reporting "three reports by the People's Liberation Army [that] shed light on the depths of China's brain warfare research and [that] show that it has been underway for several years." One PLA report said that the "focus is to attack the enemy's will to resist, not physical destruction,"), *available at* https://www.washingtontimes.com/news/2021/dec/29/pla-brain-control-warfare-work-revealed/.

[36] *See* Emily R. Siegel and John Holland, "Putin's Billionaires Dodge Sanctions by Financing Lawsuits (1)," Bloomberg (Mar. 28, 2004), *available at*: https://news.bloomberglaw.com/litigation-finance/putins-billionaires-sidestep-sanctions-by-financing-lawsuits.
[37] *Id.*
[38] *Id.*
[39] *See* Emily R. Siegle, *China Firm Funds US Suits Amid Push to Disclose Foreign Ties (2)*, BLOOMBERG NEWS, *available at*: https://news.bloomberglaw.com/business-and-practice/china-firm-funds-us-lawsuits-amid-push-to-disclose-foreign-ties.
[40] *See Staton Techiya, LLC v. Samsung Electronics, Co., Ltd.*, 23 CV 00319 (E.D. Tex. 2023), Dkt No. 1, Complaint for Patent Infringement; Siegle, *China Firm supra* n. 39; Unified Patent database listing cases, *available at*: https://portal.unifiedpatents.com/litigation/caselist?flag=DC&flag=SC&flag=CAFC&flag=CFC&plaintiff=Staton+Techiya+LLC&sort=-filed_date.
[41] *See* Head of IP Policy Interview, *supra* n. 19.
[42] *See* Chief of IP Litigation Interview, *supra* n. 27.
[43] *See, e.g., Apple, Inc. v. Samsung Electronics Co., LTD.*, Case No. 5:11-cv-01846-LHK (PSG) (N.D. Cal. Jan. 29, 2014) (ordering $2 million sanction against defendant and defendant's law firm after law firm associate's inadvertent failure to redact information sent to client Samsung hundreds of times); *see* Stan Gibson, "Apple v. Samsung Sanction Decision: the Bark Is Worse Than the Bite as Apple and Nokia Overreach in Their Request for Sanctions," Patent Lawyer Blog (Feb. 3, 2014), *available at*: https://patentlaw.jmbm.com/2014/02/apple-v-samsung-sanction-decis.html.
[44] 18 U.S. Code § 1831.
[45] *See* Center for Strategic & International Studies, "Survey of Chinese Espionage in the United States Since 2000" (last visited April 6, 2025) *available at*: https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000/.
[46] *See* GAO Report, *supra* n. 1 at p. 10 & n. 25.
[47] *See* Lydia Tomkiw and Erin Arvedlund, "Fortress, Mubadala complete acquisition of Fortress Investment Group," Pensions & Investments (May 15, 2024), *available at*: https://www.pionline.com/alternatives/fortress-mubadala-complete-acquisition-fortress-investment-group.
[48] *See* Purported "Industry Cast-out" Sues Samsung, RPX Empower (Dec. 30, 2024), *available at*: https://insight.rpxcorp.com/news/details?searchq=ents%3A%281784545%29&sort_list%5B%5D=publication_date-DESC.
[49] *See Radian Memory Systems LLC v. Samsung Electronics Co., LTD*, 24 CV 01073 (E.D. Tex Dec. 24, 2024) Complaint for Patent Infringement, Dkt No. 1, *available at*: https://insight.rpxcorp.com/litigation_documents/15962896.
[50] *See* Kochan, *supra* n. 7 at p. 6.
[51] The analysis presented in the main text is based on data reported in *The Westfleet Insider*, *supra* n. 5, which is the most prominent publication covering the TPLF industry.
[52] Kochan, *supra* n. 7 at p. 7.
[53] *See* Patent Atty. Interview, supra n. 22.
[54] *See* GAO Report, *supra* n. 1 at pp. 12, 22; TPLF In-house Counsel Interview, *supra* n. 23.
[55] *See* GAO Report, *supra* n. 1 at p. 22.
[56] *See* Judicial Caseload Indicators - Federal Judicial Caseload Statistics 2023, *available at*: https://www.uscourts.gov/data-news/reports/statistical-reports/federal-judicial-caseload-statistics/judicial-caseload-indicators-federal-judicial-caseload-statistics-2023.
[57] Standing Order Regarding Third-Party Litigation Funding Arrangements, Ch. J. Connolly (Apr. 18, 2022) *available at https://www.ded.uscourts.gov/sites/ded/files/Standing%20Order%20Regarding%20Third-Party%20Litigation%20Funding.pdf.*
[58] U.S. District Court for the District of New Jersey, Local Civ. Rule 7.1.1, Disclosure of Third-Party Litigation Funding (revised as of January 22, 2025), *available at*: https://www.njd.uscourts.gov/sites/njd/files/CompleteLocalRules.pdf.
[59] *See* Standing Order for All Judges of the Northern District of California, Contents of Joint Case Management Statement, Par. 17 (updated Nov. 2023), *available at*: https://www.cand.uscourts.gov/wp-content/uploads/2023/03/Standing_Order_All_Judges-11-30-2023.pdf.
[60] *See* Nate Raymond, "US judicial panel to examine litigation finance disclosure," Reuters (Oct. 10, 2024), *available at*: https://www.reuters.com/legal/government/us-judicial-panel-examine-litigation-finance-disclosure-2024-10-10/.
[61] *See* Patent Atty. Interview, *supra* n. 22.
[62] *See* Chief of IP Litigation Interview, *supra* n. 27.
[63] The EEA procedure for a court order to preserve confidentiality could serve as a rough model. *See* 18 U.S. Code § 1835.
[64] Federal Rules of Civil Procedure 1.
[65] *See* 18 U.S. Code § 1836.
[66] *See* Chief of IP Litigation Interview, *supra* n. 27.