Testimony of James Pooley
"Safeguarding Trade Secrets in the United States"
U.S. House of Representatives Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet
April 17, 2018

Good morning Chairman Issa, Ranking Member Johnson, and Members of the Subcommittee. Thank you for inviting me to address you today. My name is James Pooley. I started my career as a lawyer in Silicon Valley in 1973, and over the years since I have handled hundreds of trade secret disputes, including trials, arbitrations and settlements, in state and federal courts throughout the country. My legal treatise "Trade Secrets" was published twenty years ago and has been updated semiannually since then. For many years I have taught trade secret law and litigation as an adjunct professor at the University of California, Berkeley and at Santa Clara University. My first business book about secrets was published in 1982 and my most recent one, *Secrets: Managing Information Assets in the Age of Cyberespionage*, was released in 2015. In December of that year I had the privilege of testifying to the Senate on the then-pending Defend Trade Secrets Act. I am currently Chair of the Sedona Conference Working Group 12 on Trade Secrets, and am Co-Chair of the Trade Secrets Task Force of the International Chamber of Commerce.

I am grateful for the Subcommittee's holding this hearing and for your continuing support for a robust system of laws protecting the investments of U.S. companies in their information assets. And I believe that term "information assets" best captures the significance of your work in this area. Over the past forty years we have witnessed the most profound change in the nature of business assets since the beginning of the Industrial Revolution. We have transformed an economy that depended primarily on tangible assets such as buildings, heavy machinery, railroads and metals, to an economy that depends primarily on data. Whether it falls into the rarified classification of artificial intelligence algorithms, whether it

defines a secret process for manufacturing a better product, or whether it provides better understanding of markets and customers, information provides the competitive edge for U.S. industry.

In effect, information is the new oil, and U.S. companies continue, as they have in the past, to set the world standard for production of this asset. We created the information economy, and because we have more of it, more high quality information than anyone else, our companies are often targets for theft or other acquisition by improper means.

Importantly, this new property that fuels our economy is mainly protected as trade secrets. In a recent survey by the National Science Foundation and the Census Bureau, companies classified as "R&D-intensive" – which collectively account for 75% of private R&D spending in the U.S. – were asked to rank the importance of various kinds of IP laws in protecting their competitive advantage. Trade secrets came out on top, rated at more than twice the level of patents.[1] This is particularly true for small businesses, which traditionally rely on simple secrecy much more than costly patents.

Trade secret theft hurts all kinds of companies, as well as our economy. When businesses lose secrets to a competitor, the competitor can go straight to manufacturing without the costs and risks of honest R&D, allowing it to undercut the original innovator, resulting in lost profits and jobs. And things can be much worse for a small business that relies on a single line of products. When it loses the technology that gives it a competitive edge, it may have to shut down.

To maintain legal protection, companies have to take reasonable steps to keep their information secret. When I first started working in this area, information security was fairly simple: all a company had to do was guard the photocopier

[1] *Business Use of Intellectual Property Protection Documented in NSF Survey*, NSF 12-307 (2012), available at http://www.nsf.gov/statistics/infbrief/nsf12307/.

and watch who went in and out the front door of the building. Since then, advances in electronics like flash drives and smartphones have made data theft almost infinitely easier and faster. The new environment enables not just external hacking of corporate networks, but also misappropriation by trusted insiders like employees, consultants and suppliers. This puts a premium on careful management of information assets, to reduce the risk of loss. But no management system is perfect, and so trade secret law exists to back up a company's protection systems and to provide judicial intervention when despite best efforts the integrity of its information assets is compromised or threatened.

Trade secrets are the oldest form of intellectual property. For centuries craft guilds protected their advantage by keeping certain techniques within a small group of trusted masters. In the U.S., trade secret law emerged in the nineteenth century to accommodate the shift from agrarian and cottage production to larger-scale industry, in which the secrets of production had to be shared with workers or business partners. Court decisions sought to enforce the confidence placed in those who were given access to valuable information about machines, recipes and processes. At the core of every case was a confidential relationship. Protecting this trust, the courts explained, was a simple matter of enforcing morality in the marketplace.

The common law origins of trade secrets – in contrast to the federal patent statute – meant that the majority of cases were heard in state court. Since most disputes were local, this did not present a problem through the first half of the twentieth century. But as the economy grew and companies increasingly operated across state lines and internationally, the state-based system became a difficult and inefficient place to resolve some important disputes. The widespread adoption since 1980 of the Uniform Trade Secrets Act didn't help much since, ironically, many states insisted on tweaking the standards to such an extent that we ultimately had less harmonization across the states than before the act was proposed. Adding to that variation was a patchwork quilt of local procedural rules

that made some trade secret enforcement efforts almost prohibitively expensive and unreliable.

It was to address this problem that the Congress enacted, virtually unanimously, the Defend Trade Secrets Act of 2016. It came into force on May 11 of that year, and I am pleased to report to you that it has been a great success. As Mr. Ameling [has described] [will describe] in his testimony, cases asserting the DTSA's original jurisdiction continue to be filed at a brisk pace. In my capacity as a litigator using the statute, and in many conversations with other lawyers and with judges handling these cases, it has become clear that this new statute is working as it was intended by Congress.

As you may recall, one of the issues of contention at the time the DTSA was under consideration was a fear that by creating an independent basis for federal jurisdiction, a new species of "troll" would emerge to use the law as leverage to exact tribute from unsuspecting companies and individuals. Back then I published an article arguing that this fear was ungrounded, because the very nature of trade secret misappropriation – which unlike patent infringement requires that the parties be in a confidential relationship or that one have stolen from the other – meant that there could not be any such "surprise attacks" in trade secret litigation as often occur in patent litigation.[2] I am pleased to report that our experience in the last two years confirms that "trade secret trolls" are indeed a mythical creature.

Another concern raised during the pendency of the DTSA was that its provisions allowing ex parte seizures would be widely and irresponsibly used, causing damage especially to small companies. Again, the actual experience shows that

[2] James Pooley, *The Myth of the Trade Secret Troll-Why the Defend Trade Secrets Act Improves the Protection of Commercial Information*, 23 George Mason LR 1045 (Summer 2016). Another important distinction with patent law that makes it impossible to "troll" for trade secret cases is that there is no strict liability, and independent development is always a complete defense.

this anxiety has not materialized, and only a small handful of seizures have been ordered. Whether that is due to the very stiff requirements established by the DTSA to justify the seizure process, or whether it is due to the natural preference of parties and courts to use the more straightforward path of Rule 65 injunctions, we can rest assured that this issue, which captured most of the attention in advance of passage, has faded out as a critical matter of concern.

Indeed, I am pleased to report that the attention of the bar and the academy has turned to finding consensus about best practices for the management of trade secret assets by companies and of trade secret cases by courts. This is the central mission of our new Sedona Conference Working Group 12 on Trade Secrets, which has assembled a large, diverse and well-respected group of lawyers, industry representatives, professors and judges.[3] Over the next two years we hope to craft and publish guidelines that will help federal and state judges do a better job of handling trade secret cases and companies do a better job at managing their information assets. This massive and very important project was catalyzed, and largely enabled, as a result of your work in supporting the Defend Trade Secrets Act.

One of the virtues of getting an improved legal environment for the protection of trade secrets is that it is easier to identify weak spots in the system. One of those relates to the operation of 28 U.S.C. §1782, which allows foreign litigants

[3] The Sedona Conference is a nonprofit research and educational institute focused on the advanced study of law and public policy. See https://thesedonaconference.org/wgs. Specifically, the mission of Working Group 12 is "to develop consensus and non-partisan principles for best practices in managing trade secret litigation and well-vetted recommendations for consideration in protecting trade secrets, recognizing that every organization, both large and small, has and uses trade secrets; that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade; and that trade secret disputes are litigated in both state and federal courts.

(or entities “interested in” a foreign proceeding) to petition U.S. courts for access to testimony and other evidence for use in foreign proceedings. This statute has been in effect for many years, but since it was interpreted very broadly by the U.S. Supreme Court in 2004 in Intel v. AMD, it has come to be used much more frequently, exposing potentially sensitive data from U.S. companies at the request of foreign entities who themselves do not face reciprocal discovery. In effect, it is a one-way street for the acquisition and export of U.S. information.

What does this have to do with trade secrets? Our own courts are very experienced in measures to restrict access and prevent misuse or publication of discovery material. However, when dealing with Section 1782 the ultimate recipient of the information is a foreign court, where trade secret protections can vary from relatively weak, to dangerous, to virtually nonexistent. This is true notwithstanding that the TRIPS Agreement sets basic standards for trade secret protection throughout the industrialized world, because actual enforcement of those rights depends on local procedures. The result is that the trade secret enforcement frameworks of most countries in the world are substantially weaker than in the U.S. Therefore, when the confidential information of a U.S. business is ordered produced in response to a Section 1782 petition, there are no reliable safeguards in place to ensure that the receiving court will provide adequate protection to maintain secrecy.

We should all be deeply worried that under Section 1782 as it now stands information belonging to U.S. companies can be sent to a foreign tribunal without any protections imposed by our courts. We should insist that U.S. courts, in granting these petitions, impose reasonable protections against misuse or disclosure before the information leaves our country. In my view, such a modest requirement would provide substantially enhanced protection for the trade secrets of U.S. businesses who are now inappropriately exposed to the loss of their property by complying with orders made pursuant to this statute.

I very much appreciate the opportunity to appear before you today, and I welcome any questions.