Testimony of David Hirschmann
President and CEO, Global Intellectual Property Center &
Senior Vice President, U.S. Chamber of Commerce
Before
The United States Sentencing Commission
March 13, 2013

I. Introduction

Good morning Commissioners, and thank you for the opportunity to speak with you on the important subject of deterrent penalties for trade secret theft. My name is David Hirschmann and I am the President and CEO of the Global Intellectual Property Center (GIPC) and a Senior Vice President of the U.S. Chamber of Commerce.

The Global Intellectual Property Center (GIPC) was established in 2007 as an affiliate of the U.S. Chamber of Commerce. Today, the GIPC is leading a worldwide effort to champion intellectual property rights as vital to creating jobs, saving lives, advancing global economic growth, and generating breakthrough solutions to global challenges.

The U.S. Chamber of Commerce is the world's largest business organization representing the interests of more than 3 million businesses of all sizes, sectors, and regions. Our members range from mom-and-pop shops and local chambers to leading industry associations and large corporations.

The GIPC and the Chamber advocate for the right rules to protect intellectual property (IP), the necessary resources for critical government agencies, and enforcement of the law against IP criminals.

On behalf of the broad business community, I am here this morning to urge you to adopt appropriate, deterrent penalties for trade secret theft, including minimum penalties that include some amount of imprisonment. These are necessary to deter crimes that threaten American businesses, competitiveness, and the jobs of American workers.

II. What are trade secrets?

Trade secrets are a form of IP. The "secret" may be almost anything from the formula for a popular soft drink, to a manufacturing technique, to a computer algorithm. But that doesn't begin to describe their significance to the companies that hold them. It has been estimated that of the S&P 500, 81% of their market value is derived from their intangible portfolios.[1]

Trade secrets are often the crown jewels of a company. Because that formula may make their drink uniquely appealing, that technique may lower their costs of production, or that algorithm may make their service superior, trade secrets are nothing short of a company's competitive advantage in the marketplace. And that is precisely why industry competitors and even foreign governments covet them.

III. Trade secrets are under attack

When Congress enacted the Economic Espionage Act of 1996, it was aware of the value and growing importance of IP, and trade secrets in particular. The Senate Judiciary Committee wrote at that time that:

> In a world where a nation's power is now determined as much by economic strength as by armed might, we cannot afford to neglect to protect our intellectual property. Today, a piece of information can be as valuable as a factory is to a business.[2]

The Committee also understood the fundamental formula and motive for trade secret theft:

---

[1] H. Rept. 112-610, July 19, 2012 at 4 *citing, Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, March 28, 2011 at 6, *available at*: http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf.

[2] S. Rept. 104-359, Aug. 27, 1996 at 6.

> This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft.[3]

While the availability of criminal penalties under the Economic Espionage Act of 1996 no doubt helped reduce trade secret theft from what it might have been over the past 17 years, it has not been enough. The theft of trade secrets has reached epidemic proportions. Measured by the number of civil cases in Federal courts, trade secret theft has grown exponentially over the past fifty years, and shows no sign of slowing down.[4]

Translating that increase into estimates of business losses is staggering: from hundreds of millions of dollars lost by individual companies, to $13 *billion* lost by a group of companies collectively over a six-month period, to *over $1 billion lost by a single company in a matter of only days*.[5] This is the scenario that makes executives wake up in the middle of the night in a cold sweat. Overall, it has been estimated that trade secret theft costs U.S. companies as much as $300 billion every year.[6]

You have already heard this morning directly from individual companies that have had the unfortunate experience of being victims of trade secret theft. Between those individual cases and the broad statistics I have just cited, there is a fundamental truth; trade secret theft is a threat across the entire business community.

This reality is understood not only throughout the business community, but in Congress and the Administration as well. The law that brings us here today, the Foreign and Economic Espionage Penalty Enhancement Act, enjoyed bipartisan support in Congress, was supported by the Administration, and was lauded by the Chamber (see Appendix). And, as you know, the Administration's Intellectual Property Enforcement Coordinator

---

3 *Id.*

4 Almeling *et* al, A *Statistical Analysis of Trade Secret Litigation in Federal Courts,* 45 Gonzaga L. Rev. 291, 301 (2010).

5 H. Rept. 112-610 at 4-5.

6 Almeling at 292, *citing* Office of the Nat'l Counterintelligence Executive, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2002 vii (2003), *available at* http://www.fas.org/irp/ops/ci/docs/2002.pdf.

recently released an enforcement strategy particularly directed to reducing the theft of trade secrets from American companies.[7]

IV. The nature of trade secret theft

The advent of digital technology and the interconnectedness of the Internet have been incredible boons to companies and consumers alike. They have brought us new services, innovation, and creativity and opened new markets. But criminals have also abused them to engage in theft on an unprecedented scale.

It has been said that there are two types of companies, "those that know they've been compromised, and those that don't yet know."[8] The entirety of the ongoing cyber-security discussion is broader than trade secret theft and beyond the scope of this proceeding. What we aim for today is a source of deterrence that can reduce the source of the problem.

Our member companies describe to us essentially three sources of trade secret theft. In no particular order, one category is malicious acts and theft by individuals or small groups of independent actors such as hackers, thieves, and/or disgruntled employees. They may hack or exceed permitted access into corporate networks on the rationalized basis of opposition to company practices, perceived vengeance, or pure greed. While they may lack the resources of institutional-based thieves, this category of actors may have specialized knowledge that facilitates their efforts and can lead to tremendous economic damage. Further, these independent actors may become tools and agents of the institutional actors mentioned below.

---

7 *Available at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

8 Alperovitch, *Revealed: Operation Shady RAT*, McAfee White Paper (2011) at 1, *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

A second category is theft by competitors. This paradigmatic framework is straightforward; one company seeks to neutralize the competitive advantage of another. The company engaged in this type of espionage may be a foreign or domestic competitor of the holder of the trade secret.

A third category is acts by foreign governments to obtain the trade secrets of U.S. companies. In the most brazen cases, it involves state-sponsored espionage. As you are no doubt aware, this has gotten particular attention in the mainstream media in recent days and weeks.[9] Foreign government efforts in this area can also be more direct, such as mandating the disclosure of trade secrets as a condition for access to that country's domestic marketplace.

To a substantial degree, these are issues that need to be addressed on an ongoing basis by the U.S. Government in dialogue with foreign governments. And the Chamber has advocated strongly for such action in the trade context. We recognize that a foreign government hacker who works from his home country is beyond the reach of U.S. law enforcement and unlikely to be deterred by penalties under our law. However, there can also be a domestic U.S. element as well.

Just as in the days of the Cold War, foreign espionage against the United States is sometimes aided by people in the U.S., either agents of a foreign government or the types of individuals described in the first category above. In such cases, U.S. authorities clearly do have the authority to arrest and prosecute the offenders.

V. Why greater penalties are needed

Deterrence is the goal; we seek to reduce the amount of trade secret theft by intimidating potential thieves away from that course of action. Once the theft has occurred and the crown jewels are out the door, seeing the thief prosecuted is surely justice, but that is scant consolation to the people laid off because the company lost its competitive advantage.

[9] *See* http://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html.

To be sure, high-profile prosecutions with impressive sentences can add to the deterrence value of the law. And that is a good and useful thing for the companies that have not yet been victims of catastrophic trade secret theft. But for the company that was the victim, it is too late. So, the goal is to deter as early as possible, with penalties that promise incarceration in a Federal prison and leave a potential thief with as little doubt as possible that getting caught means not only the loss of their ill-gotten gains, but a loss of freedom for a duration that will give them pause.

We recognize that deterrence is a formula also involving the risk of detection and the risk of conviction. Both of those factors weigh in favor of strong penalties.

As has been the case in other contexts, those engaged in theft utilizing the latest technology are difficult to track down and thus have a degree of confidence that their crimes will not be detected. Indeed, this situation is directly analogous to one the Congress and this Commission undertook in another IP context sixteen years ago. In adopting the No Electronic Theft Act and instructing this Commission to review the appropriate penalty levels for criminal copyright infringement,[10] the House Judiciary Committee wrote:

> Many computer users…simply believe that they will not be caught or prosecuted for their conduct….In light of this disturbing trend, it is manifest that Congress must respond appropriately with additional penalties to dissuade such conduct.[11]

In addition to the low risk of being detected and caught, thieves may indulge their hopes because of the low risk of prosecution and the high standard of evidence sufficient to reach the level of proof needed in criminal prosecutions.

The final variable in the deterrence equation is the potential profitability of the crime. As is discussed above, the value of trade secrets is tremendous. That, of course, translates into high profit potential for the thief.

10 Pub. L. 105-147 (1997).
11 H. Rept. 105-339, October 23, 1997 at 4.

This almost perfect storm of high potential profits and low chances of detection and successful prosecution means that to achieve deterrence, severe penalties must be available and applied. The Chamber supported the initial draft of the Foreign and Economic Espionage Penalty Enhancement Act, which would have statutorily raised the maximum imprisonment from 15 to 20 years. While we also supported the final version of that bill that lacked that provision, we continue to believe it is critically important. The Chamber also supports a minimum sentence that guarantees imprisonment as a key element of deterrence. And we note with appreciation the Administration's support for increased penalties in this area as well.

VI. Conclusion

Intellectual property, trademarks, patents, copyrights, and trade secrets, are the foundation of a tremendous part of the American economy. Collectively, IP-intensive industries provide over 55 million American jobs, over $5 trillion in output, and 74% of American exports. It is no wonder that these industries and their valuable IP are the envy of the world and a target for thieves. Companies spend untold millions fighting to protect their innovation, creativity, and good name, but they cannot do it alone. Law enforcement is a partner and has a critical role. We urge you to provide the right rules for criminal trade secret theft to protect American companies, competitiveness, and our economic wellbeing.

Thank you.