

Inventors Network of the Capital Area

P.O. Box 18052
Baltimore, Maryland 21220

April 18, 2011

The Honorable John A. Boehner
Speaker
United States House of Representatives

Dear Mr. Speaker:

We are a local D.C. area group of small business and entrepreneur inventors. We are writing to you about **the patent reform bill, H.R. 1249**. We are deeply concerned that **its proposed “First to File” (FTF) provision has an overlooked but unusually dangerous defect that seriously threatens our national defense**. Although most of H.R. 1249 is almost incomprehensible except to the small inner circle of patent attorneys who drafted it, the national security defect is simple for anyone to understand, with a little background on cyberspace espionage.

Our principal competitor in technology is China. China is widely acknowledged to be the world leader in industrial espionage. China’s advanced cyber espionage capability has allowed it to break into the most secure U.S. military networks repeatedly. Far less secure is the Internet, which is effectively defenseless against the kind of sophisticated state-sponsored industrial espionage already underway on a massive scale. Even technology leader Google was successfully attacked by China with impunity. Moreover, non-state sponsored cyber criminals have already shifted their main focus to stealing and selling the intellectual property of global organizations.

This extreme vulnerability to cyberattack is unlikely to change anytime soon. The U.S. Department of Defense is heavily focused elsewhere, primarily on its own offensive cyber capabilities, based on the conventional assessment that effective network defense is technically impossible. The Defense Department has no authority over civilian networks anyway. No current private sector cybersecurity system is capable of providing an effective defense against the existing excessive cyberattack vulnerability. All of this is public knowledge.*

In this unfortunate real world situation today, the new “First to File” provision threatens all individual and corporate Research & Development in America, the backbone of our national defense and economic security.

Under the FTF provision of H.R. 1249, Chinese hackers who steal U.S. R&D secrets can easily become the very first to file U.S. patent applications covering those technology secrets and thereby own that new U.S. technology even in the U.S., instead of now just being able to copy it in China. China could own the new jobs worldwide in the entirely new industries that develop those stolen U.S. technologies. China could even legally exclude a U.S. company that actually invented a new breakthrough technology from developing or using or selling that U.S. company’s own invention in the U.S.

Defense technologies would be the prime target of this threat. The cyber espionage branch of the Chinese Army could break into Northrop Grumman (again), steal newly invented secret weapon designs, immediately file the very first U.S. patent applications, and then use U.S. patents to stop Northrop Grumman from ever using their own newly invented weapons anywhere, even in the U.S. **Under the FTF provision of H.R. 1249, the U.S. patent system would become the most effective weapon in the Chinese arsenal, effectively disarming America in legal preemptive strikes.**

Ironically, the Chinese Army would be enabled by FTF to function as a **giant super patent troll**, funded by the vast sovereign wealth of China, with far greater powers of U.S. economic destruction than any of the relatively tiny alleged patent trolls whose activity H.R. 1249 is designed to restrict.

The FTF of provision of H.R. 1249 thus creates an unimaginably huge new incentive for industrial espionage in the U.S. by China and non-state cybercriminals that directly threatens U.S. national defense and economic security in an entirely new and highly dangerous way. The probable damage is severe and far outweighs any possible legal benefits.

Rather than supposedly providing U.S. patent law with a long overdue update to deal with the brand new, utterly transformative Internet digital technology of the 21st Century, the FTF proposal is so old that it has been made obsolete by the Internet itself. The FTF provision was first proposed in the Johnson Commission report of the late 1960's, which predated all but the most primitive computer networks, and then was proposed again in the Mossbacher report of 1992, which predated the widespread use of the Internet and the World Wide Web.

In conclusion, the "First to File" provision of H.R. 1249 has classic unintended consequences of a scope that goes far beyond patent law and far outweigh any presumed improvements in that limited legal area. The U.S. is under no international obligation whatsoever to expedite this entirely voluntary major change in its national law. Therefore, a careful and unbiased evaluation of this serious and logically inevitable threat to U.S. national defense should be made by the responsible House Committees before any further action.

The only House action that is necessary now is to refer H.R. 1249 to at least the Armed Services Committee, the Homeland Security Committee, and the Permanent Select Intelligence Committee for appropriate evaluation of the dangerous threat to our national defense posed by the First to File provision. Much more than patent law is at stake. At the same time it should be evaluated by the Crime, Terrorism, and Homeland Security Subcommittee of the Judiciary Committee, as well as the House Foreign Affairs Subcommittee on Oversight and Investigations.

Sincerely,
The Below Signed Members of the
Inventor Network of the Capitol Area

Natalie Young

Paul Weir

Chris Carlin

E.P. Williams

Ernest M Danderfor

Donald R. Wulfinghoff

Glen Kotapish

Maurice Daniel

Vargashak Vartanian

Michael Medhin

Richard Hansen

A. Crystal Williams

Leslie Wilson

George R Miller

Frampton Ellis

*** See the Following Related Background Extracts and Links to Full Articles**

Related Background Extracts and Links to Full Articles:

Patently Absurd or: How to Go From the World's Best Patent System to Worse-Than-Most in a Single Step

by Gary Lauder, HUFFINGTON POST, March 7, 2011

...Under FTF, if someone else finds out about your invention, and if they **apply first, they can win**. Overturning that requires proving that they derived their idea from yours. This would be almost impossible to prove since there is inadequate right to discovery. What's most scary to me is that **this creates strong financial incentives for usurping patents rights by hacking and industrial espionage, which is increasingly state-sponsored (think China)**.

http://www.huffingtonpost.com/gary-lauder/patently-absurd-or-how-to_b_832703.html

Innovation, Espionage, and Chinese Technology Policy

Statement of Adam Segal, Council of Foreign Relations, April 15, 2011
Before the **House Foreign Affairs Subcommittee on Oversight & Investigations**

...In the September 2010 issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn III argued that **though the “threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyber threat that the United States will face over the long term.”**

There is, however, an emerging debate whether the traditional methods of cybersecurity—public-private partnerships and information sharing—are adequate to the threat. **Given the attacks on Google and other technology companies, there is a real question whether the private sector can defend itself against state-backed attacks. At the very least, private companies must get used to the idea that any information that is digitalized cannot be made completely secure.**

...The United States should continue to try and shape the debate within China, **but the most important actions will be improving the defense of its computer networks and intellectual property.**

<http://www.cfr.org/china/innovation-espionage-chinese-technology-policy/p24686>

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation

Prepared for The US-China Economic and Security Review Commission, 10/22/09

...Chinese espionage in the United States ... now comprises the single greatest threat to U.S. technology, according to US counterintelligence officials....

http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

U.S. Firms, China Are Locked in Major War Over Technology

THE WALL STREET JOURNAL, February 2, 2011

A titanic battle is under way between U.S. business and China, a battle reflected in President Barack Obama's State of the Union address last week and destined to dominate relations between the two countries for years.

At issue: Innovation.

...To hear U.S. business executives describe it, **Beijing's mammoth new industrial policy is like the Borg in "Star Trek" —an enormous organic machine assimilating everything in its path, in this case the inventions of other nations.** Notably, China's road map, which is enshrined in the "National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)," talks in those terms. China will build its dominance by "enhancing original innovation through co-innovation and re-innovation based on the assimilation of imported technologies."

"**It's a huge, long-term strategic issue,**" says a top executive at a U.S. technology firm operating in China. "**It isn't just the crisis of the day for U.S. business. It's *the* crisis.**"

<http://online.wsj.com/article/SB10001424052748703439504576116152871912040.html>

China's Drive for 'Indigenous Innovation'

U.S. Chamber of Commerce Website

...[China's Medium and Long-Term Technology Development Plan 2006-2020] explicitly states that a key tool for China to create its own intellectual property and proprietary product lines will be through tweaking foreign technology. Indeed, **the [Plan] defines indigenous innovation as "enhancing original innovation through co-innovation and re-innovation based on the assimilation of imported technologies."** It also warns against blindly importing foreign technology without plans to transform it into Chinese technology. The report states: "One should be clearly aware that the importation of technologies

without emphasizing the assimilation, absorption and re-innovation is bound to weaken the nation's indigenous research and development capacity." As a result, **the plan is considered by many international technology companies to be a blueprint for technology theft on a scale the world has never seen before.**

<http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>

Cybercriminals Target Corporate Data

TG DAILY, March 28, 2011

Cybercriminals have shifted their focus from stealing personal information to targeting the corporate intellectual capital of prominent global organizations. According to McAfee CTO Simon Hunt, online criminals understand there is "greater value" in selling a corporations' proprietary information and trade secrets." **Sophisticated attacks such as Operation Aurora, and even unsophisticated attacks like Night Dragon, have infiltrated some of the largest, and seemingly most protected corporations in the world. [Clearly], criminals are targeting corporate intellectual capital and they are often succeeding."**

<http://www.tgdaily.com/security-features/55037-cybercriminals-target-corporate-data>

Google, China and the Shores of Tripoli

THE WALL STREET JOURNAL, January 24, 2010

Needed: a plan to sweep cyber pirates from the digital sea lanes.

...The Chinese government's fingerprints are all over the cyber attacks against dozens of Silicon Valley companies, plus the hacking of the personal Gmail accounts of individuals in the U.S. and elsewhere. Although Beijing apparently aimed at accessing information from human-rights advocates, the violation of personal email privacy potentially can affect anyone, anywhere. This comes after **many incidents of hacked computers at the Pentagon, congressional offices and other government agencies.**

<http://online.wsj.com/article/SB10001424052748703439504576116152871912040.html>

Hackers Stole Data on Pentagon's Newest Fighter Jet

CNN.com, April 21, 2009

Thousands of confidential files on the U.S. military's most technologically advanced fighter aircraft have been compromised by unknown computer hackers over the past two years, according to senior defense officials. ...the attacks appeared to originate in China....

<http://www.cnn.com/2009/US/04/21/pentagon.hacked/index.html>

How to Fight and Win the Cyberwar

THE WALL STREET JOURNAL, December 6, 2010

...Mr. [Richard] Clarke argues in his book [**Cyberwar**] that China is one of the key players in developing a cyberwar capability. The Chinese use private hackers to engage in widespread penetration of U.S. and European networks, successfully copying and exporting huge volumes of data. That's on top of their capacity to attack and degrade our computer systems and shut down our critical networks. He believes that the **secrets behind everything from pharmaceutical formulas, bioengineering designs, and nanotechnologies to weapons systems and everyday industrial products have been stolen by the Chinese army or private hackers who in turn give them to China.**

<http://online.wsj.com/article/SB10001424052748703989004575652671177708124.html>

Operation Aurora

Wikipedia, 6 April 2011

Operation Aurora is a [cyber attack](#) which began in mid-2009 and continued through December 2009.^[1] The attack was first publicly disclosed by [Google](#) on January 12, 2010, in a [blog](#) post.^[2] In the blog post, Google said the attack originated in [China](#).

The attack has been aimed at dozens of other organizations, of which [Adobe Systems](#),^[3] [Juniper Networks](#)^[4] and [Rackspace](#)^[5] have publicly confirmed that they were targeted. According to media reports, [Yahoo](#), [Symantec](#), [Northrop Grumman](#), [Morgan Stanley](#)^[6] and [Dow Chemical](#)^[7] were also among the targets.

As a result of the attack, Google stated in its blog that it plans to operate a completely [uncensored](#) version of its search engine in China "within the law, if at all", and acknowledged that if this is not possible it may leave China and close its Chinese offices.^[2] Official Chinese media responded stating that the incident is part of a U.S. government conspiracy.^[8]

...According to McAfee, **the primary goal of the attack was to gain access to and potentially modify source code repositories at these high tech, security and defense contractor companies. “[The SCMs] were wide open,” says Alperovitch. “No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways — much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting.”**^[10]

http://en.wikipedia.org/wiki/Operation_Aurora

Tinker, Tailor, Soldier, Hacker

THE WALL STREET JOURNAL, April 21, 2010

The Internet was designed for easy communication. Security? Not so much.

... Nor are electric-generating facilities, already the target of thousands of known hack attacks, the only vulnerability. Military secrets and valuable intellectual property are also at risk, Messrs. Clarke and Knake note. **Yet efforts to protect against hacker-attacks have lagged behind increasingly sophisticated threats as the Pentagon concentrates on offensive, not defensive, cyberwar techniques.**

<http://online.wsj.com/article/SB10001424052748704671904575193942114368842.html>

The Greatest Changes of the U.S. Patent System in the Last 50 Years

China Intellectual Property News, 2007

...the [similar previous patent] bill ... is friendlier to the infringers than to the patentee in general as it will make the patent less reliable, easier to be challenged and cheaper to be infringed. It is not bad news for developing countries which have fewer patents. Many of the Chinese companies are not patent owners in the U.S. market and their products are often excluded from the market because of patent infringement accusations. **This bill will give the companies from developing countries more freedom and flexibility to challenge the relative U.S. patent for doing business in US and make it less costly to infringe.**

Hacker Raids Sony Videogame Network

THE WALL STREET JOURNAL, April 27, 2011

A hacker stole the names, birth dates and possibly credit-card numbers for 77 million people who play online videogames through [Sony](#) Corp.'s PlayStation console, in what could rank among the biggest data breaches in history.

...The attack on Sony is the latest in a string of high-profile breaches recently. Email marketing firm Epsilon Data Management LLC, a division of Alliance Data Systems Corp., said this month it had detected an intrusion into its systems and that hackers may have stolen some of the names and email addresses it manages for clients that include J.P. Morgan Chase & Co. and Best Buy Co.

<http://online.wsj.com/article/SB10001424052748703778104576287362503776534.html?KEYWORDS=Sony+Playstation+3>