Cybersecurity Implications of The America Invents Act

By Gary Lauder, Managing Director, Lauder Partners

Updated November 26, 2014

Summary:
This bill, which was signed into law on September 16, 2011, will create a new reward system for those who steal others' intellectual property by enabling such stolen IP to either: 1) be patented by the thief, or 2) prevent the actual inventor from receiving a patent. Historically the economic value of hacking has been quite limited, but this change threatens to create new incentives for this illegal activity — at a time when we should be trying inhibit hacking rather than rewarding it.

The Leahy-Smith America Invents Act, formerly known as the "Patent Reform Act of 2011," makes many changes to US patent law, but the one most relevant to cybersecurity is the change from First-to-Invent (FTI) to First-to-File (FTF) for applications filed on or after March 16, 2013 (18 months post-enactment). America was the last remaining country with a FTI system and also enjoys the most vibrant innovation ecosystem. Under FTI, if two people both file for the same invention at the Patent and Trademark Office (PTO), the party who can prove an earlier invention date is entitled to receive the patent. That process is called an "interference proceeding" and is rare (<100/year, <0.01% of patents filed) and expensive. Under FTF, invention date does not matter and the main thing that matters is the date of application filing. Under FTF, if an inventor alleges that someone else filed based on misappropriated IP, that party can initiate a "derivation proceeding," in which one must prove that the information was derived from the inventor. Since the inventor does not have the right to discovery, and, more importantly, since someone who knowingly applies for a patent based on stolen ideas knows they must cover their tracks, it is not likely that evidence can be found to prove derivation. Under the former FTI interference proceedings, each party only needed to provide their own evidence of invention timing. Derivation proceedings are expected to be at least as expensive as interference proceedings, but much less likely to succeed.

Our FTI system discouraged theft much more than FTF. As a result, in countries where FTF prevails, the standing advice that entrepreneurs receive is to apply for patents PRIOR to talking to investors (whose money might be needed to apply) and PRIOR to talking with customers (whose input might refine the invention or cause one to re-evaluate the wisdom of pursuing a patent at all).

If a competitor or customer wishes to prevent the original inventor from receiving a patent, but doesn't have the chutzpah to apply for the patent, it can be prevented by publicly writing about it in a way that the inventor can't prove derivation. Such publications prior to filing are deemed prior art and would preclude getting a patent. Again, there is no right of discovery to prove derivation.

The economic value of patents have recently reached new heights with the Nortel patent portfolio of 6,000 patents being sold for $4.5B or $750K/patent. Also reaching a crescendo is hacking. There is another new development in the hacking world, which may make this a perfect storm: the emergence of markets for stolen information.[1] Previously, most hackers hacked for mischief or actionable financial information (e.g. credit card and bank numbers), and mostly for their own account. Since non-financial information is much more prevalent on hackable computers and is less well-protected, the opportunity to cash in on this via anonymous markets represents a dangerous new development. With stolen IP suddenly being worth much more due to FTF, hacking could dramatically increase even further. It is worth noting that state-sponsored hacking is occurring by China, and that foreign patent applications to the USPTO now exceeds domestic.

The Obama Administration issued a favorable Statement of Administration Position despite not having even been aware of the cybersecurity implications. Nor has congress seriously considered this issue despite one public attempt to raise awareness about it.[2] I have spoken with many cybersecurity officials in the US government, and NONE have ever been aware of how the AIA/FTF might impact it, nor were any consulted on whether this would be good policy.

The national security implications of making this change to our patent laws should have been properly evaluated prior to passing or signing this legislation. The potential harm to start-ups and other small and early-stage companies was also not taken into account. As with any governmental mistake, it can be undone — but it will require leadership. The best time to have done this was prior to passage. The second best is now.

An additional moral of this story is that congress did not even *consider* these unintended consequences of the AIA since it is ill-equipped to comprehend such issues as complex as IP. As of 11/14, congress is getting ready to further damage our economy by passing "anti-troll" legislation despite troll lawsuits waning due to recent Supreme Court decisions.

Gary Lauder is a venture capitalist based in Silicon Valley and has been a venture capitalist since 1985. His advocacy on this issue is based on not wanting to see more self-inflicted wounds, such as Sarbanes-Oxley, hindering the innovation ecosystem that has already shrunk dramatically in the past decade. For more on this subject, see http://www.lauderpartners.com/PatentReform/ He can be reached at:

---

[1] "Cybercriminals target corporate data," 3/28/11, http://www.tgdaily.com/security-features/55037-cybercriminals-target-corporate-data

[2] Letter from the Inventors Network of the Capital Area to Speaker Boehner, http://www.dcinventors.org/wp-content/uploads/2011/07/incaletteronHR1249.pdf http://www.dcinventors.org/wp-content/uploads/2011/07/UPDATEtotheApril2011INCALetter.pdf

(650) 323-5700 or via Gary@LauderPartners.com…but does not have much time for this due to his day job.