Statement of Mike Sax

President
Sax Software
Eugene, Oregon

Board President
Association for Competitive Technology

Testimony before the Senate Committee on Finance, Subcommittee on International Trade, Customs, and Global Competitiveness

"International Trade in the Digital Economy"

November 18, 2010

Chairman Wyden, Ranking Member Crapo and distinguished Members of the Committee: My name is Mike Sax and I would like to thank you for holding this important hearing on international trade in the digital economy, and the role it plays in driving innovation, fostering economic growth and, most importantly, creating new jobs.

I am here today wearing two hats: In my "day job" I am an independent software developer who makes his living creating and selling software for multiple platforms. My livelihood depends on my ability to write compelling applications and reach customers in a purely digital marketplace. In addition to developing my own software, I also serve as the board president for the Association for Competitive Technology (ACT). ACT is an international advocacy and education organization for people who write software programs - referred to as application developers - and providers of information technology (IT) services. ACT represents over 3,000 small and mid-size IT firms throughout the world and advocates for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

Despite the down economy, entrepreneurs in the technology industry are still optimistic about the prospect of expanding into new markets and creating new jobs. Foreign markets, particularly high growth markets like China, India, and Brazil offer immense opportunities for technology companies. Today, foreign markets represent more than 50% of revenues for the technology industry and far more than that in growth opportunities. While the future looks bright for America's most innovative firms, some foreign laws are creating both intentional and unintentional barriers for our members.

In this discussion of innovation and exports, I think my personal story may be of some interest to Members of the Committee. I, like many entrepreneurs, was not born in the United States. In 1994, after feeling limited by the lethargic pace of innovation in the European Union and a difficult environment for innovators, I emigrated from Belgium to Eugene, Oregon, on an investor visa. I invested my personal savings into Oregon because I could see that the United States offered an environment where innovative entrepreneurs could thrive. The U.S. offered bright people willing to take risks, a strong intellectual property system that rewarded risk-takers, and a dynamic software market with low barriers to entry for start-ups.

My story is certainly not unique, but it has become a talking point for leaders in the EU who want to reclaim Europe's position as an innovation hub. During the recent European Commission Patent Conference, Minister of Economy and Reform Vincent Van Quickenborne gave a keynote speech on the importance of creating a unified European Patent. In that speech he discussed me specifically; presenting my story as an example of an innovative and successful entrepreneur who had to leave Europe to innovate. He went on to say that Europe needed to do a better job simplifying and strengthening its patent system so that people like me would stay, instead of heading off to Oregon!

Because of my history, I can easily identify the opportunities in export markets, but I am also more aware of the pitfalls found in actually getting paid for software or services sold abroad. Based on my own export experience and that of other ACT members, I believe three issues are key to expanding opportunity for digital exports:

1. Protection of IP rights, from curbing piracy to promoting patent harmonization;
2. Addressing the multiplicity of laws affecting privacy, data storage, and payment methods
3. Eliminating outright import barriers through standards mandates, domestic support programs, and difficult to manage joint venture requirements.

Protection of IP rights

Let me state clearly that IP is a driver of economic growth and development through innovation so ensuring strong IP laws and awareness is critical. Members of this Committee and the entire Senate have heard repeatedly about the loss of revenue related directly to piracy. The Business Software Alliance, which represents many large software companies, annually commissions a study that attempts to calculate the cost of software that is in use, but not paid for.

However, what those numbers fail to capture is the economic opportunities that are lost because rampant piracy discourages small firms from even entering the Chinese market. In general, entrepreneurs are an adventuresome group – willing to explore and make the most of opportunities in any market. No single country presents a bigger opportunity than China, and yet entrepreneurial software developers have, for the most part, decided

to spend their time elsewhere. They know that the opportunity in China may be great, but the obstacles to capitalizing on that opportunity have proved almost insurmountable.

It isn't simply a matter of software distributed in China and not paid for; instead, most small independent software vendors (ISV) don't even bother to try and enter the Chinese market.

The joke amongst developers is that "you only sell one copy to all of China, so you better charge a lot for it." This feeling is held by the vast majority of the ISV community. Here are a few telling quotes from a website focused on selling software in China:

> *Getting Paid*
>
> *The first thing I need to say, right off the bat: Chinese users will not buy your software. Period.*
>
> *[It is] very hard for westerners who do not speak the language nor have contacts in China to provide such services, but there are opportunities to partner with local independent professionals or small businesses in your target industry.*
>
> *A word about consumer-oriented microISVs: I am extremely skeptical about independent microISV B2C [Business to Commercial] sales in China, because I honestly cannot imagine an individual paying for independent software.*

All of that from a website aimed at helping developers enter China. And if that's from the "pro" side of selling software in China, here's some experiential information from developers who have pursued software sales in China, discussing their experience via a developer-focused website:

Question: Does anyone have any further suggestions or insights about the best way to approach the Chinese market?

> *Yep. Don't. Gigantic international corporations have wasted billions of dollars trying, unsuccessfully, to turn a profit from China. It's a great big sink-hole.*
>
> *Craig Welch*

Chinese users do not pay for software (or music, or movies). You might be able to sell it if your product is SaaS,[Software as a Service] but it's a very hard sell. Chinese users might pay if you sell them a service (i. e.: installation, support, customization, etc...), but forget about selling just the software.

Felipe Albertao

The preferred method is not to pay. While China is a huge market it is also the bane of software developers who wish to make a living. Theft and piracy are rampant and essentially government sanctioned.

I'd stay away.

[Anonymous]

This pervasive (and largely accurate) view of China means that independent software developers aren't losing sales in China, they aren't even bothering to attempt selling to China.

And those who do brave the Asia market find that dealing with stolen license authorization codes may be more trouble than it's worth. Ambrosia Software, an upstate New York software developer with 12 employees, has been running in-house case studies on the rate at which stolen license codes are used to request software updates from their servers. Back in 2001, they found that an astronomical 50% of unique requests for updates were coming from stolen codes. In 2010, they have lowered that rate through a mixture of product and support changes, but still have to dedicate a full time developer to managing license issues–this is a person who would otherwise be making new products and helping to grow the company. Recently Ambrosia began selling some software in Asia, including retail boxed software in Japan. Here's what they found:

…we made a change to our licensing system to allow for the sale of software in retail boxes in Japan. These codes are easier to steal, since they need to remain active while the software sits waiting to be sold at retail… attempts to use codes[tailored for the boxed software market in Asia] have made up a whopping 75% of the total retail registrations logged by our system in the past 2 months.

This shortfall of our retail venture likely limits the volume of business we can do in this space.

The tale told here is clear–piracy is not just stolen sales, it stifles sales before they are made.

Fortunately, China isn't all grim tales of failure, there are a few bright spots. Mobile applications sold though stores like iTunes, Microsoft's App Marketplace and others give developers some hope for the future. But overall, small independent software developers currently see more barrier than opportunity.

If certainty about piracy stops developers from entering into China, uncertainty about patents creates roadblocks for developers expanding into markets that otherwise have a solid IP track record. For example, the complexities of the European patent system in particular pose real challenges for innovative American companies and even European ones.

The European Patent Office provides a uniform patent application process for up to 40 European countries, but it does not provide uniform laws for patentability and enforcement. Therefore, the majority of a company's work in obtaining and defending a patent must be done on the national level, not the European level. This requires every patent to be officially translated into each European language. The result is that obtaining and protecting a patent in Europe is at least 10 times more expensive than a United States patent (according to a 2002 GAO study)[1].

To make matters worse, the complexity and expense of the international patent system can leave American inventions completely unprotected abroad. One of ACT's member companies, DigitalNow, had a similar problem. DigitalNow developed a new type of high-end film scanner for businesses to convert physical photographs into digital images. DigitalNow's scanner technology was protected by patents in the U.S. and EU, covering elements of the hardware and software, but DigitalNow's patent protection did not extend to all nations within the EU.

[1] http://www.gao.gov/new.items/d03910.pdf

While at a major trade show, DigitalNow's owner, Gary Mueller, found a much larger competitor highlighting the virtues of new technology they had recently incorporated into their scanners–new technology that was identical to Gary's. Worse still, they were telling potential customers that the technology was the same as could be found on Gary's scanners, but backed by their much bigger brand. Gary's patent lawyers told him that while this company was clearly violating his patent, they were not selling to the U.S., and therefore it would be nearly impossible to pursue them for damages.

Additionally, many American companies begin the process of applying for patents abroad without a full understanding of the immense ongoing costs. When they run out of resources to finish the patent process or defend their patents in court, those companies may never be able to protect those inventions again.

Stories like Gary's have driven developers who create digital goods to question their ability to protect themselves from the sale of their product by legitimate competitors. Despite the doom and gloom, there are some positive actions being undertaken. The United States Patent and Trademark Office (USPTO) has been working with the IP 5, a group of patent offices made up of the USPTO, EPO, JPO, KIPO and SIPO[2]. Together, the IP 5 are working to create new efficiencies in the global patent system by "leveraging the search and examination work products of other IP Offices and providing the global patent community greater flexibility as to when patent applications may be examined and accelerated."[3] And more work can be done to help harmonization. The U.S. Congress should move forward to bring the United States into the modern age and support a "first inventor to file" change to our patent system.

Domestically, developers who look to the patent system to provide a way to secure their invention and to share their methodology have been hampered by the insane 40-month pendency that drags out the uncertainty for a small software firm, trying to find out if their "niche" is really a niche at all. We applaud much of what USPTO Director Kappos

---

[2] United States Patent and Trademark Office, European Patent Office, Japan Patent Office, Korean Intellectual Property Office and State Intellectual Property Office of the P.R.C.

[3] http://www.uspto.gov/blog/director/entry/reducing_pendency_through_worksharing_and

has been doing to reduce pendency, and call on Congress to continue to make sure the USPTO has the funds to make lowering pendency a reality.

Cloud Computing and the multiplicity of laws affecting privacy, document storage, and payment methods

Next, I'd like to discuss a growing way for software developers to offer their products to users throughout the world—through cloud computing.

Cloud computing refers to applications and services accessed remotely over the Internet. Anyone who has been using Web-based e-mail has been using cloud computing in some form. But advancements in broadband speeds and computing devices provide powerful new ways to connect with customers.

Instead of running software that resides on a single device, my customers can run applications and access data stored remotely using their laptop, smartphone, or other mobile device.

The potential benefits of cloud computing are enormous. But as is frequently the case, the legal system has not kept up with technological advancements. And with cloud computing, we're not just talking about one country's laws, but any country where data flows and resides—which, over the Internet, could be almost anywhere.

Application developers are worried about multiple and conflicting laws for privacy, data storage, and payment methods. These three areas are of primary importance for those who want to leverage the Internet to export their software or services to consumers in other countries.

Privacy

Divergent privacy-related laws in the European Union, Asia, and here in the U.S. that specify how data can be collected, used, and shared create difficult compliance barriers. To illustrate:

- EU data protection law requires multiple intercompany contracts, which are disproportionately expensive and challenging for small businesses.

- U.S. companies often launch new services in an unfinished "beta" format, but the EU doesn't favor this approach and wants privacy locked-down before a service is launched.
- Inconsistent privacy regulations result in opportunity costs, because new products are not launched, or are not exported to other countries.

Even when using model clauses for privacy approved by the European Union, it can be legally complex to transfer data from the EU member states to other parts of the world (outside the handful of jurisdictions deemed to provide "adequate protection" or to the U.S. under the U.S.-EU Safe Harbor Agreement). Many EU jurisdictions require prior approval of the clauses and some take as long as four months to finish their reviews.

Compounding things further, there is no one-stop-shop filing option for these agreements. Filing and translation requirements vary widely among EU member state jurisdictions. This adds significant cost and delay to cloud computing, global IT help desk support, and a wide range of other services that require trans-border data transfers.

Compliance with international data privacy law is hard enough, but American companies must also abide by multiple state laws. In recent years, state legislatures have enacted more than 100 privacy and data security related laws. These include security breach laws, data security laws for the protection of personal information, data disposal, RFID privacy laws, spyware laws, spam laws, and online privacy laws. Some of these laws are similar, many are different—but in every case we must follow applicable state rules in addition to U.S. federal law and the laws of other nations.

Data Storage

Data storage raises new questions for national sovereignty. Whose law applies to data in the cloud? While answering this might be an interesting exercise for a legal team, the uncertainty confounds small software developers and ultimately harms innovation.

Here's one example: If I have a customer in China whose data is stored in a data center in Australia, but I'm an American company and the data flows from Australia to China through other countries, whose law applies? Is it the Chinese law, because that's where

my customer lives? Is it Australian law, because that's where the server is located? Is it U.S. law, because it's an American company that's providing the service? And what happens when those national laws conflict?

Even legal experts will say that there is no clear answer. If every country's rules must be followed, how can we expect entrepreneurs to compete against larger companies that have a team of lawyers?

There is also the issue of obtaining access to data stored in "the cloud" by law enforcement. Multiple jurisdictions may seek access to a user's information. But there's not one agreed-upon set of rules governing the standards law enforcement must follow to obtain such access. I fear that should I hold data from users worldwide, I will face divergent and conflicting demands from law enforcement over user content and data. And I will have to weigh each law enforcement request with varying laws on privacy rights and data retention.

This global thicket of competing and conflicting laws makes it difficult for application developers to use the Internet to create an international customer base. But there is also some concern among foreign governments and data protection authorities about allowing their data to be stored in the U.S. because of concerns that the U.S. government will secretly obtain access to that information. In order to deal with this, and other issues surrounding cloud computing, I recommend four areas where the U.S. government can undertake to strengthen cloud computing globally:

- Improve privacy protection and data access rules to ensure users' privacy, starting with reforming and strengthening the Electronic Communications Privacy Act to more clearly define and strengthen protections for consumers and businesses;
- Modernize the Computer Fraud and Abuse Act so law enforcement has the tools it needs to go after malicious hackers and deter instances of online-based crimes;
- Improve transparency so that consumers and businesses will know by whom and how their information will be accessed and used by cloud service providers;
- Support the creation of a new multilateral framework to address data access issues globally.

Payment methods

As my applications move to the cloud, so do the payments I receive from my customers. But accepting payments from customers in other countries involves more than the conversion of foreign currency into dollars.

Payment information involves personally identifiable information, so privacy and security breach laws apply. There are also a number of domestic financial regulations that apply to foreign payments, including those that pertain to money laundering.

With regard to cloud computing and online commerce, now is a critical time for international policymakers to reassess their approach to privacy, data storage, and financial regulation. In formulating and amending policies in these areas, it is absolutely essential that consultations include entrepreneurs and small company innovators. Cloud computing will only reach its full potential if providers can establish datacenters and offer services in multiple jurisdictions, without fear that each step will invite competing claims of jurisdiction and government access to data. The rules must balance the legitimate needs of law enforcement, industry, and users, and it is vital that all stakeholders are represented in any deliberations.

Standards mandates, domestic support programs, and difficult-to-manage joint venture requirements.

While tariffs and direct subsidies are an obvious problem, IT companies also face global trade barriers due to disparate forms of intellectual property laws and enforcement, competition regulations, government preferences, and standards setting and procurement policies. These barriers are a new form of protectionism—"Protectionism 2.0"—that uniquely harm innovative American IT companies.

Within the realm of tariffs, the 1996 Information Technology Agreement (ITA) has provided a solid framework for understanding and eliminating tariffs on digital goods (but notably not digital services). Unfortunately, this successful tariff agreement has been under assault. Recently the EU attempted to impose tariffs on items that were excluded previously, but had since been improved through the addition of features. Since

the digital age is all about the constant addition of new features and repurposing of old ones, the EU's position could have been fatal to the ITA agreement. Fortunately, the U.S. Trade Representative (USTR) was able to push back and keep "improved'" products on the list. However this experience does point to the need for the government to revisit the ITA in light of the enormous changes that the industry has undergone since the 1996 agreement. Consider that in 1996, the World Wide Web was barely three years old, Google was two years from incorporation, and Facebook's founder Mark Zuckerberg was only 12 years old. Given all of the new products available, it is clear we need to expand the list of digital goods included in the ITA.

Beyond specific trade agreements, small developers have also been affected by a different part of the "protectionism 2.0" thicket—countries that have different rules for marketing software based exclusively on its country of origin. One of the most obvious examples is China's different rules for computer games. Today, a Chinese company that develops a video game can directly market and sell their product within China, without extensive government review or involvement. However, game developers from the U.S. must have their product reviewed by two separate agencies with two separate review processes before it can be marketed legally in China. Obviously, this puts a huge strain on the game developer, as well as any local partners he may have. Worse still, if the game proves popular in the U.S., pirated copies will be widely available for sale months before the dual review process is finished.

Another delaying or forestalling tactic is the use of standards to exclude or limit foreign competition. In the EU, we have seen governments mandate specific standards for government procurement that are chosen not because they are technologically superior, but rather because they tilt the playing field in favor of a domestic company. China has taken standards preferences a step further, and has moved to create, and mandate, their own standards in the commercial context. Two of the most famous cases deal not with software standards, but standards for mobile platforms: China's own version of the 3G wireless standard, called TD-SCDMA, and a domestic version of WiFi, called WAPI.

With TD-SCDMA and WAPI, China provided support for local broadband technologies in a way that would allow domestic companies to avoid paying royalties to U.S.-based

Qualcomm and other tech manufacturers, even after the Chinese government had agreed not to favor its own standards as part of its World Trade Organization (WTO) commitments. While these fights were primarily between big players in the handset market, it proved to be a setback for U.S- based small software developers who were looking to piggyback on the efforts of the bigger phone manufacturers. In some cases China has moved to be more amenable to working with international standards in recent years, but the initial push for a domestic standard harmed small businesses that lacked the deep pockets to deal with the artificial multi-standard environment China had created.

On the positive side of the ledger, we see Europe moving to reconsider their Standardization Strategy to allow for standards from consortia and non-traditional standards bodies like the World Wide Web Consortium (W3C). The United States should support this effort so long as it continues to stress that the best technical standard be available to consumers, regardless of the country of origin.

Finally, many nations use onerous joint venture requirements to make it more difficult to sell products in-country. Some require companies to have a local partner who owns 51%, others allow for 100% foreign ownership, but make it difficult to sell products locally, or require significant sums of money to be "banked" before agreeing to allow the sale of software or services. We hope that USTR and others will continue to urge our trade partners to do away with these kinds of barriers.

Though much of my testimony has focused on the problems small software developers face, it's important to note that we still need fair and open international trade.

Increased access to global markets is vital for American entrepreneurs and small IT companies. Ninety-seven percent of all exporting companies are small- and medium-sized enterprises, accounting for 29% of U.S. exports by value. So that small businesses can produce locally and distribute globally, the U.S government must work to ensure that trade is both fair and open.

Fair trade ensures that other nations have the laws and infrastructure to enforce the patents, copyrights, and trademarks of U.S. companies. Open trade ensures that countries

open their markets to American products, and that their laws and procurement policies do not disadvantage U.S. businesses.

Fair and open trade is an essential part of bilateral trade agreements. Opening access to export markets creates incentives for innovation and technological progress and increases sales opportunities for American IT companies.

The Department of Commerce, the International Trade Administration, and the USTR must work to ensure that entrepreneurs and small IT companies have fair and open access to global markets.

Chairman Wyden, Ranking Member Crapo, and distinguished members of the Subcommittee, the future of the digital marketplace looks bright for small business, so long as the marketplace remains dynamic and competitive. I hope that the subcommittee will continue to focus the spotlight on the contribution small business makes to the future of the digital economy and the way government can do a better job to open export markets. Thank you for your time and consideration on this important topic.