SSRC

RE: 2011 Special 301 Review
Docket Number USTR-2010-0037

February 15th, 2011

Stanford McCoy
Assistant U. S. Trade Representative for
Intellectual Property and Innovation

Office of the United States Trade Representative
600 17th Street NW
Washington, DC 20508
Filed electronically via Regulations.gov

Dear Mr. McCoy,

The Social Science Research Council is concluding a 3-year study of software, film, and music piracy in developing countries, with forthcoming reports on Russia, India, Brazil, Mexico, Bolivia and South Africa. Last year, we submitted a comment that addressed the procedural and evidentiary requirements that inform the Special 301 process—subjects that the report explores at length. We made two general points:

(1) The steps taken in reforming the comment process (since 2008) and in allowing for public testimony (since 2010) are welcome and go some way toward bringing the Special 301 process into closer alignment with the generally recognized requirements of an "informal adjudication": namely, that "a minimum procedure must include at least some form of notice and an opportunity to be heard at a meaningful time and in a meaningful manner."[1] However, this should be only the beginning of a process of opening the Special 301 process up to the wider range of stakeholders and level of scrutiny that IP and trade policy increasingly require.

(2) The USTR has paid inadequate attention to the evidentiary requirements of the Special 301 process and, more generally, to OMB requirements for research relied upon by government agencies. Special 301's evidentiary requirements for submitted comments are modest but relatively clear: submissions should (1) "provide all necessary information for assessing the

[1] 32 Fed. Prac. & Proc. Judicial Review § 8201 (1st ed.) (stating "[s]everal courts have said that a minimum procedure must include at least some form of notice and an opportunity to be heard at a meaningful time and in a meaningful manner."

> effect of the acts, policies, and practices"; and that (2) "any comments that include quantitative loss claims should be accompanied by the methodology used in calculating such estimated losses."[2] Over the past two decades, the research submitted by the major industry organizations in the copyright area has not met a reasonable interpretation of these standards. Nor does it meet the newer, stricter OMB standards of "transparency" and "reproducibility" required for research used in policymaking processes. Because the Special 301 report relies heavily on this research, generally paraphrasing from the reports themselves, the USTR has been out of compliance with these requirements. Because the USTR the primary audience for this research, it could insist on more credible and transparent research practices. It has not done so.

For 2011, we note that although the prior procedural reforms are welcome, there remains a strong participatory deficit in the Special 301 process that undermines its legitimacy and value to US taxpayers. This is not a matter of "fairness" toward countries on the receiving end of USTR warnings. It is a matter of recognizing the strong stake of other US sectors in the formulation of trade and IP policy, on issues ranging from health, to innovation, to education, to culture. We would draw particular attention, in this context, to the involvement of US state health officials in the 2010 hearing, who expressed concern that USTR negotiations would constrain the ability of US states to implement effective health care reform. The shift of copyright enforcement from targeting commercial infringement to consumer infringement is another area of clear expansion of the purview of trade negotiations, and one that brings USTR actions into tension with a wide range of other stakeholders and regulatory roles. The industry-centered participatory process that informs Special 301 is, in this context, obsolete and in need of change. Reforms to the comment process, report drafting, and advisory committee structure to address these issues are clearly within the existing authority of the USTR.

With regard to evidentiary standards, we note again that the Special 301 report has avoided the quantitative loss estimates produced by industry for the past several years—perhaps reflecting the recent critical coverage of those methods by OECD, GAO, and other groups. But the underlying assumptions of the industry studies still clearly inform both the spirit and letter of the Special 301 reports. Piracy is assumed to generate massive losses to US business, and to require a wide range of legal reforms and new public investment in enforcement. Our work, over four years and across six countries, suggests that neither the losses nor the efficacy of enforcement should be taken for granted. Rather, these should demonstrated and

[2] 19 USC 2242(b)(2)(B)

subject to open review and debate. Our report goes into considerable detail about these methodological issues. Because of the frequent references to software losses in the 2010 Special 301 report, we will offer some limited remarks on software piracy and the organization of the software market.

To summarize:

- Unlike recorded media business models such as the CD and DVD businesses, piracy is not primarily a drain on the software business, but rather a critical part of the business model that allows the building market share in low-income countries and the effective locking out of open source alternatives. These network effects are enormously valuable to quasi-monopoly providers like Microsoft, but also smaller vendors seeking to establish a foothold in foreign markets.

- Unlike recorded media business models, the software industry has strong forms of technical protection at its disposal that go mostly unexercised because for fear of inconveniencing paying customers.

- Unlike recorded media business models, the software industry has an entirely viable business model in developing countries, based on institutional licenses to large businesses and the public sector. The consumer/retail sector is effectively ignored through western-level pricing. This model has allowed Microsoft, for example, to report 100% growth in sales in China in 2010, despite what the 2010 Special 301 report characterizes as a near total lack of enforcement.

- Enforcement plays a role in this strategy in the form of pressure on institutions to legalize. But the key market factor is the threat of the adoption of open source alternatives, which creates competitive pricing pressure and leads to lower-prices on licenses.

- The USTR plays an appropriate role in this context by encouraging countries to legalize software in the public sector and to enforce against commercial pirate vendors under the TRIPS agreement. But in our view, given the complex relationship between legal, unlicensed, and open source adoption, that is as far as the evidence of harms goes. The assumption that there are massive overall losses to US software industries from piracy or significant benefits to stronger criminal provisions for end-user infringement should be heavily discounted. The problem of business sector piracy is best left to the technical protection measures of the vendors and the civil courts. The question of software choice, often involving open source adoption as a strategy for combating piracy, should be left to governments.

Our report will be available by the end of February at http://piracy.ssrc.org . We look forward to an opportunity to share it and testify at the March hearing.

Thank you for your consideration on this matter.

Sincerely,

Joe

Joe Karaganis

Program Director
Social Science Research Council

Findings on Software Piracy

The 2010 Special 301 report refers repeatedly to software industry losses suffered in Watchlist and Priority Watchlist countries, echoing longstanding Business Software Alliance claims. Throughout the past decade, BSA loss claims have dwarfed those of other industries by an order of magnitude or more. In 2009, the BSA estimate of losses reached $53 billion.

In 2010, however, the BSA abandoned the concept of losses in its (IDC-conducted) reports, in favor of a more carefully hedged notion of 'the commercial value of unlicensed software.' While apparently trivial, the change ended the BSA methodology's much criticized assumption of a 1-1 ratio between pirated software and lost sales, and therefore makes the BSA work much more credible. But it also means that the BSA no longer makes any quantitative claims about industry losses.

In our view, the business software market is unique to an extent that warrants a very different understanding of piracy, losses, and business models. Consistently, we find the enforcement discussion around software to be divorced from many of the critical factors shaping software markets—especially the network effects generated by piracy in emerging software markets.

In software markets, network effects refer to contexts in which the value of software rises with the size of the installed base. The more widely used a piece of software or software service, the more it becomes a de facto standard that shapes user decisions about adoption and investment. Platform technologies such as operating systems exhibit strong network effects because a popular platform will foster a rich secondary market in applications and services, which in turn increases the platform's value. "Lock-in" occurs when the costs of leaving a particular software environment are high—whether because switching would require significant repurchasing of software, or because the use of less common standards is disadvantageous, or simply due to costs of retraining. For near-monopolies such as Microsoft in the operating systems and office software markets, network effects reinforce market power and increase the value of their products. Lock-in effects, in turn, ensure that customers are less likely to switch to competitors.[3]

[3] There is an extensive and—for the most part—highly speculative business literature on network effects that has attempted to model the decision points that shape policies of tolerance and enforcement toward software piracy (for an overview, see Katz [2005]). The actual estimation is highly complex, and we are unaware of any compelling estimates across different software lines or in developing countries.

As BSA piracy figures indicate, these dynamics in emerging economies are primarily (and sometimes overwhelmingly) a function of pirated-software adoption, not legal adoption.[4] Piracy, in effect, has allowed the major vendors to dominate low- and middle-income markets (or, as they develop, market segments within them) that they have little financial incentive to serve. Perhaps most important for market-dominating firms, piracy acts as a barrier to entry for competition, especially "free" open-source alternatives that have no upfront licensing costs. When these emerging markets begin to grow, as most did in the last decade, piracy ensures they do so along paths shaped by the powerful network and lock-in effects associated with the market leaders.

In our view, these factors should figure in any full accounting of the costs and benefits of software piracy. Top-tier vendors have established and maintained their dominant positions in emerging markets through piracy, often prior to or in the absence of significant local investment. Any losses they incur at the margins of the consumer and business markets in those countries should be weighed against the value of maintaining their dominant positions. For near-monopolies, we would argue that this value is very high. For vendors working in highly competitive markets or selling products that do not function as standards or platforms, that value is clearly lower. We have seen no work that empirically measures or distinguishes these effects and so can only speculate here as to their relative worth.

Enforcement representatives interviewed for this project generally disagreed with this view of how software markets work and held to the notion that piracy is first and foremost a loss of revenue and a disincentive for investment—both foreign and local. We view this as a form of elective blindness to how software markets work. The relationship between piracy and network effects appears to be well understood elsewhere in these firms—including among such industry leaders as Bill Gates, who has referred repeatedly to the importance of piracy in securing market share and undercutting Linux adoption in China.[5] As Microsoft executive Jeff Raikes observed:

[4] BSA-derived rates of software piracy in Russia hovered around 90% through the early 2000s. China was at 90% as recently as 2008. India has spent most of the past decade around 70%; Brazil, 60%–70%.

[5] Microsoft Chairman Bill Gates to students at the University of Washington, in 1998: "And as long as they're going to steal it, we want them to steal ours. They'll get sort of addicted, and then we'll somehow figure out how to collect sometime in the next decade" (Grice and Junnarkar 1998). Or more recently: "It's easier for our software to compete with Linux when there's piracy than when there's not. . . . You can get the real thing, and you get the same price" (Kirkpatrick 2007). The same logic also holds for smaller companies seeking to establish a presence in developing markets, such as LogMeIn, a $320 million vendor of remote access software. As CEO Michael Simon observed, echoing Gates, "If people are going to steal something, we sure as hell want them to steal our stuff" (Vance 2010).

“In the long run the fundamental asset is the installed base of people who are using our products. What you hope to do over time is convert them to licensing the software” (Mondok 2007).

The major vendors have done just that in the past decade in the institutional sectors of emerging markets, through a combination of price discrimination and enforcement. This strategy has focused on computer manufacturers and vendors, large businesses, school systems, and other public-sector institutions because they combine two things the software companies like—relatively high ability to pay and vulnerability to enforcement—with two things that they don’t like but must confront: sufficient market and/or political power to extract pricing concessions and sufficient technological capacity to make credible threats of open-source adoption. In 2007, the Russian government played this game with a consortium of commercial vendors to obtain a 95% discount on Windows and a bundle of productivity applications for Russian schools. Chinese municipalities did so in 2008, following a Chinese edict requiring legal software in government use. The Indian state of Karnakata did so in 2009 for its government agencies, and so on. In both the Russia and China cases, the BSA cited the licensing of public institutions as a major factor in reported drops in the local rates of piracy (BSA/IDC 2009). When these licenses come up for renewal (in the Russian case, at the end of 2010), network effects and lock-in costs will factor on the side of commercial vendors in any renegotiation.

In the retail channel, in contrast, prices remain very high relative to local incomes—usually matching and sometimes exceeding US or European levels. One might reasonably ask why. It is no secret, including among vendors, that very few Indian or Brazilian customers will pay $300 for Windows or $1,000 or more for Adobe’s Creative Suite. There is no significant market at that price level. In practice, however, vendor strategies don’t require one. The retail channel plays a very small part in the marketing strategies of the major vendors even in developed countries and far less in developing ones where price/income ratios are several multiples higher.[6] The institutional channel is the revenue generator.

Retail prices, in these contexts, can remain high because the retail market is not needed to build market share. Piracy does that. High retail prices are, nonetheless, valuable for two reasons: they prevent arbitraging of low-priced goods across borders,[7] and they set expectations about how much software should cost—and

[6] According to quarterly earnings reports, Microsoft’s consumer market—here including retail purchases and (often discounted) sales through manufacturers—represents around 20% of total business software revenue.

[7] Even of local-language software, which generally sells at no more than a slight discount.

accordingly set a baseline for licensing deals. Some vendors have made efforts to “complete” these underserved markets through price discrimination in the retail sector, but without notable success. Efforts to sell stripped-down versions of Windows—the various “Starter” packages announced over the past decade—are perhaps the best-known example, widely distributed but doomed in markets where full versions are available at little or no cost. As an Indian respondent observed: free software in India means Microsoft Windows.

The BSA’s valuation (until 2010) of every pirated copy as a lost sale is worth returning to in this context because we can now see that it answers the wrong question. In a market dominated by volume-licensing deals, the question is not “how many legitimate copies does piracy displace,” regardless of whether the answer is 90% or 10%, as IDC representatives have suggested, but rather: “given the high market share already achieved by vendors in high-piracy markets, for which segments of the market are price discrimination and enforcement profitable strategies?” Here, vendors face the downside of economies of scale: the smaller the customers, the higher the costs of engaging them in contracts or threatening them with enforcement. Completing a market, in this context, is an expensive proposition with diminishing returns. In our view, the BSA piracy rates are descriptions of this decision point.

Small business is the main enforcement frontier, actively contested by the BSA and local affiliates, the major vendors, and police. Small and medium-sized businesses face sharp dilemmas insofar as they are vulnerable to enforcement, lacking in leverage with software vendors, and often unable to afford operating fully within the licit economy. A software-compliance audit or raid can be a business-threatening experience in such circumstances, as we document in our Russia study. The BSA, for its part, is regularly criticized for its small-business enforcement tactics, which include unrealistic proof of licensing requirements and a practice of basing settlements on the unbundled, highest-possible-retail-price of infringing software rather than the actual purchase cost (Associated Press 2007). Such practices are in notable contrast to the accommodations and discounts made for large institutional infringers and are part of a dynamic in which enforcement does not so much dissuade piracy as enable price discrimination—down or, occasionally, up in the form of settlements—based on the power relations between the two parties.

The acceptability and even optimality of this approach can be weighed against the various alternatives available to business software vendors. All the major companies could adopt stronger online authentication measures, making it more difficult to use and maintain pirated software. All of them could create obstacles to the over-installation of licensed copies within businesses, which is routinely cited as the most prevalent form of infringement. But strong versions of these options go unexercised for a variety of reasons, including fear of alienating paying customers, fragmenting the installed-code base (which could increase security risks for licensed users), and diminishing the other positive network effects of widespread use.[8] The anti-piracy strategies of PC-game publishers in the past few years offer an informative contrast. Because games rarely function as platform technologies or standards, publishers have less to gain from the network effects associated with piracy and have moved much more quickly toward strong forms of online authentication. Despite a number of controversial missteps and botched launches (for example, *Spore* in 2008 and most of the Ubisoft lineup in 2010 when its authentication servers crashed), the lock down of the PC-gaming environment is well underway.

Credible threats of open-source software adoption in Brazil, Russia, India, South Africa, and many other countries also place a sharp upper bound on business software enforcement strategies. Once again, the logic is simple but rarely acknowledged: the most likely consequence of the widespread enforcement of licenses in Russia or China would be the widespread adoption of open-source alternatives—and very possibly a spur to development of alternatives where no open-source equivalents yet exist, as in the case of Autodesk's specialized AutoCAD tools. As we detail in our Russia and India chapters, these risks are not hypothetical: Microsoft and other vendors go to great lengths to underbid open-source providers in institutional contexts to ensure that open-source adoption does not reach the point where it generates comparable network effects.[9] Where the institutional or symbolic stakes are unusually high, this competitive dynamic can push licensing fees to zero.

Given the rules of this game, open-source adoption policies have become targets of IIPA criticism, despite the irrelevance of this issue to IP protection. The government of Indonesia, for example, characterized its recently announced open-source procurement policy, plausibly, as a measure to combat the use of infringing

[8] As Bradford Smith, deputy general counsel for Microsoft, characterized it in 2001: "By the late 1980s every single company abandoned that approach [copy protection] for the simple reason that legitimate customers did not like it. They found that there were times when they needed to make additional copies: they sold the computer and bought a new one and wanted to move their software, or their hard disks crashed and they needed to reinstall it. And even though at the time worldwide piracy rates for software were in excess of 80% the need to take care of the legitimate 20% of the market place took precedence over trying to deal with the rest. And that same bias very much exists today, I see it all the time when these issues are debated inside Microsoft" (Katz 2005). In late 2010, Microsoft abandoned its Windows Genuine Advantage program, which tied Windows and Office updates to regular authentication on Microsoft servers.

[9] For a textbook example, see Volker Grassmuck's study of Linux adoption in Munich in Karaganis and Latham (2005).

software. Rather than applaud the measure, the IIPA's 2010 report criticized Indonesia for establishing a trade barrier that "does not give due consideration to the value of intellectual creations" and, as such, "fails to build respect for intellectual property rights" (IIPA 2010).[10] Whether such procurement policies represent a trade barrier—unjustifiable or not—is a worthwhile question that has been debated within the open-source community (O'Reilly 2002). But the implication that open source undermines IP rights is tendentious. Quite the contrary, open-source licensing derives from and depends on strong copyright.

The BSA continues to push the enforcement envelope by calling for stronger penalties and audit powers, including the criminalization of "organizational end-user piracy" to increase pressure on businesses. End-user criminal provisions have been implemented in a handful of countries, mostly through US-driven bilateral agreements (for example, in Australia and Singapore), but they go significantly beyond international IP obligations under TRIPS and remain controversial. This is true in the United States as well, where end-user criminal liability is implied in the sweeping No Electronic Theft Act (1997) but has never been targeted. Given the viability of the institutional-legalization strategy and the balancing act between enforcement and open-source adoption, we see little incentive for the major commercial vendors to upset the status quo.

In the end, with growth rates around 30% and high-value network effects structuring key software markets, *we see no strong evidence that there are* any *real losses to market leaders from business software piracy*. But the enforcement effort does play an important role in defining the boundaries of vendor institutional-licensing strategies. With the massive subsidization of local IT infrastructures through pirated software and—to date—very inconsistent adoption strategies for open-source alternatives, it appears that most governments are also willing to play this slow game of legalization with vendors, with cooperation on enforcement and open-source adoption as the carrot and stick.

[10] Similar complaints appear in the 2010 IIPA reports on India, Brazil, Thailand, Vietnam, and the Philippines.

References

Associated Press. 2007. "Software 'Police' Accused of Targeting Small Businesses."

BSA/IDC. 2009. *Sixth Annual BSA-IDC Global Software Piracy Study*. Washington, DC: BSA. http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.

GAO (US Government Accountability Office). 2010. *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*. GAO-10-423. Washington, DC: GAO. http://www.gao.gov/new.items/d10423.pdf.

Grice, Corey and Sandeep Junnarkar. 1998. "Gates, Buffett a Bit Bearish." *CNET News*, July 2. http://news.cnet.com/2100-1023-212942.html.

IIPA. *Indonesia: 2010 Special 301 Report on Copyright Protection and Enforcement.* Washington, DC: IIPA. http://www.iipa.com/rbc/2010/2010SPEC301INDONESIA.pdf.

Katz, Ariel. 2005. "A Network Effects Perspective on Software Piracy." *University of Toronto Law Journal 55.*

Kirkpatrick, David. 2007. "How Microsoft Conquered China." *Fortune*, July 17. http://money.cnn.com/magazines/fortune/fortune_archive/2007/07/23/100134488/.

Karaganis, Joe, and Robert Latham. 2005. *The Politics of Open Source Adoption.* Wiki, Social Science Research Council, New York. http://wikis.ssrc.org/posa/index.php/Main_Page.

Mondok, Matt. 2007. "Microsoft Executive: Pirating Software? Choose Microsoft!" *Ars Technica*, March 12. http://arstechnica.com/microsoft/news/2007/03/microsoft-executivepirating-software-choose-microsoft.ars.

OECD (Organisation for Economic Co-operation and Development). 2007. *The Economic Impact of Counterfeiting and Piracy.* Paris: OECD. http://www.oecd.org/document/4/0,3343,en_2649_33703_40876868_1_1_1_1,00.html.

Vance, Ashlee. 2010. "Chasing Pirates: Inside Microsoft's War Room." *New York Times*, November 11. http://www.nytimes.com/2010/11/07/technology/07piracy.html.