Kernochan Center for Law, Media and the Arts Panel Transcript: Who's Left Holding the [Brand Name] Bag? Secondary Liability for Trademark Infringement on the Internet

Proposed Secondary Liability Regimes for Trademark Infringement Online: Commentary

JANE GINSBURG: This is our last panel, and the object is to bring a number of experts, including practitioners and academics, from the United States and from abroad, to react to the two proposals that we just heard. Each of the panelists will give initial comments, and then we are going to go around the table again so that our panelists can react to one another's comments. We will go in the following order:

First, Amy Cotton from the Patent and Trademark Office. She's our government representative. I'm not sure if you're speaking with your government hat or disclaiming—

AMY COTTON: Disclaiming.

JANE GINSBURG: Disclaiming—but she's still from the government.

Next, Bob Weigel, at the far end, who is with Gibson Dunn and represented Gucci in the *Gucci v. Frontline* case.[1] Bob will be speaking, I suspect, from the brand owner point of view.

BOB WEIGEL: That's a fair bet.

JANE GINSBURG: Next, Bruce Rich from Weil Gotshal, who happens to have been the successful counsel in the *eBay* case.[2] I think you'll be standing in for the service providers.

And then, crossing a couple of oceans—one ocean first: Miquel Peguera, from the Open University of Catalonia, who is a leading expert on the liability or non-liability of service providers. He has, among other things, published an important article in the *Columbia Journal of Law & the Arts*,[3] which will be publishing the proceedings of this symposium a couple of months hence.

And then, from across yet another ocean—Irene Calboli, who is currently visiting at the National University of Singapore and who will be talking about the effect of the free trade agreements and the potential trans-Pacific partnership on questions of secondary liability for service providers.

AMY COTTON: Thank you, Jane. I'm wearing my invisible government hat, so watch out.

1. Gucci Am., Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228 (S.D.N.Y. 2010).
2. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010).
3. Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481 (2009).

Graeme raised an interesting point about process. What's the process that we're using to get to the substantive rule? And I think that pretty much summarizes where I'm coming from—my paradigm when I'm looking at policy regulation. I proceed with lots of caution as to regulatory action. For instance, my default position on the Lanham Act is don't amend it. So when I hear calls for, "Oh, we need a statutory change! We need to implement a statute," I start twitching a little bit.

Certainly, in doing my due diligence to see if such a change would be useful, necessary and reasonable, I look at other models. The DMCA [Digital Millennium Copyright Act] is certainly the first thing that we're going to look at.[4] Talking to my copyright colleagues, and learning about some of the issues with the DMCA and safe harbors, gives me pause in terms of proceeding down that path. And then, of course, we butt right up against the SOPA [Stop Online Piracy Act]/PIPA [PROTECT IP Act] conflagration and concerns that the atmosphere is pretty toxic right now on Capitol Hill for anything that smacks of net censorship.[5] At this point, I look for other options for addressing these needs. For the past thirteen years, I have worked a lot on the ICANN [Internet Corporation for Assigned Names and Numbers] portfolio,[6] looking at that bottom-up, consensus-based market organization.

The U.S. government has put a lot of time and effort into trying to make sure that we have all of the players at the table and that all of the players are discussing, on equal footing, what the administration of the domain name system should look like. As you know, the domain name system is quite a choke point for regulating behavior in these various top-level domains. So, over thirteen years, I've looked at a couple of expansions of the domain name system. This most recent one, with 1943 applications for new top-level domains, is a bit overwhelming, but it presents an amazing opportunity for market innovation.[7] And I keep reminding the trademark owners who came screaming to the USPTO and the U.S. government, saying, "I'm going to have to police 1900 TLDs [top-level domains]! What are you doing? How can you agree to this?" I say, "Well, it was always contemplated that the domain name system was going to expand."

But look at it this way: with a lot of these new TLDs, there are opportunities for trusted spaces for retailers, for brand owners and for consumers. I think these dot brands, in particular, are a really interesting idea: that you've got places where, for example, Abbott Pharmaceuticals can market legitimate, true Abbott Pharmaceutical products to their whole distribution chain, and they control the heck out of it to make sure consumers get what they want. I think that's a really

4. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 and 28 U.S.C.).

5. Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011); PROTECT IP Act, S. 968, 112th Cong. (2011).

6. Internet Corporation for Assigned Names and Numbers. *See* INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS, http://www.icann.org (last visited Feb. 25, 2014).

7. *See* Karen E. Klein, *The Latest Domain-Name Gold Rush*, BUSINESSWEEK (June 4, 2012), http://www.businessweek.com/articles/2012-06-04/the-latest-domain-name-gold-rush.

interesting idea.

I know there are different ideas in the room about this, but some of the closed generics—dot book run by Google or Amazon, or dot generic term run by one particular company, are closed, so the company would control the terms of use and control who got in. I thought that was very interesting to watch—perhaps anticompetitive, but very interesting to watch—to see what they would do to make it valuable to the consumer. How are you going to pull people out of the unregulated Wild West of dot-com and into these trusted spaces, so that we can be sure as consumers that we are getting what we want, and so that the retailers can make sure that they are not being flooded by illegitimate products? It is very much an innovative idea that could happen, but it could also very well get tanked. The expansion of the domain name system could get overregulated.

We've been working for a long time to make sure that there was a balance, that intellectual property owners and the registrars and all these entities were talking to come to some sort of consensus about what was reasonable, what the market could bear, so that these TLDs would actually succeed.

So, I start from that space of avoiding overregulation in order to promote innovation. I'm certainly looking at the idea of the voluntary agreements. You heard about the EU MOU this morning.[8] We have about four or five voluntary agreements percolating in the United States. We are watching those very carefully to see who is coming to the table and what they are negotiating. We're not at the table; we're just watching what's going on at the table, because there is concern. We heard about anticompetitive concerns with regard to big platforms coming to the table and not the little guys.

But I think that the industry setting the standards for what is reasonable, what is sustainable and what is a good business model, is really important. And it will probably end up being a safe harbor in many respects as the case law in the United States evolves. So, those who are coming to the table are sort of setting what the standard of care should be, what the duty of care should be. I think it's a very interesting development to watch.

JANE GINSBURG: Thank you.

BOB WEIGEL: The way I come at this is that the whole reason for this conference is that the people who are actually doing the counterfeiting are crooks, not to put too fine a point on it. There are plenty of laws to prohibit them from doing what they're doing. The problem is that it is hard to get at them and to hold them accountable. And so, we're having an entire conference about how to hold someone else liable for what they're doing, which is intentional and wrong. And I think that's important to recognize, because in these instances, they have factories. They're churning out handbags or jewelry or sneakers or jeans every day. They pop off the line, and they have to sell them. So it is a constant game of cat and mouse as to what the brand owners can do. The brand owners are also trying to run

8. European Commission, *Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet* (May 4, 2011) [hereinafter Memorandum of Understanding], *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf.

a business at the same time that these folks, every day, are going home and saying, "How can I get around what the brand owners are doing?"

If you think about it, a company with the resources of Microsoft, and the talent, and the software and so forth—they shut down nineteen million Web sites in a year, and they didn't get them all. As Tom said, all they're trying to do is push these guys back to page ten or eleven or twelve on the Google search, so that you can't find them.

I do worry, if you try to impose liability on the ISPs—and with statutory damages, it could be a big number—how are you going to get an ISP to do better than Microsoft? Because there's always going to be somebody out there selling stuff. Clearly, if the ISP has notice and they keep doing it, they should be liable. But I do think there's some flexibility as to where the "should have known about it" lies, because I think that, as the technology keeps getting better and better, there may be ways for an ISP to determine, either electronically or at low cost, that a Web site is selling fake stuff. People are coming out with new techniques all the time to try to tell the electronic signature of a Web site—they've left some sort of fingerprint here, and we can scale that across the Web and find other places where they've left that signature. And that may become feasible over time.

But I'm also going to take a somewhat radical position and say that it doesn't matter. Because if you stop all the responsible ISPs, the folks who have assets, the folks who you could go against, from hosting these Web sites, then all you're going to end up doing is pushing the Web sites to ISPs in locations that are difficult to police and difficult to enforce. I've gotten injunctions against counterfeiters, and presented it to an ISP—in that case, it was China—and they basically told me to pound sand. There were other ways we were able to shut down the Web site, but there are alternatives for counterfeiters besides the traditional Web sites—besides GoDaddy and so forth. And it would be good to stop GoDaddy from allowing people to register fake domain names, but it's not going to solve the problem. It's just going to push the problem to a different place.

When you look at these Web sites that are selling fake products, it's fog—there's nothing that's true on that Web site. The pictures are not pictures of what you're going to get when you order it. The pictures are pictures of, probably, the legitimate goods. The addresses and the names of the people who registered, even if you get behind the privacy providers, are going to be fake, or it's going to be a name in some place where it's going to be hard to chase them.

The problem really is, to my mind, that the only things that are real are the email address that you buy the goods with and the way that they process the money that you send to them. And that, I think, is ultimately their weakness. We've been able to establish in certain instances that when somebody has an economic interest, when they're dealing with a Web site holder as a business proposition—for example, the bank that processes the credit cards—it is, in effect, in a credit relationship with that Web site. And because they are, in effect, lending money to that Web site every time that they process a sale and give them the money from the sale, they know what that business is. And those banks are legitimate, and those banks have assets, and if you can hold those banks accountable, then you can make

it that much more difficult, because somehow the goods have to come across the ocean and the money has to go the other way. And the only way you can really do that is sue the banking system.

BRUCE RICH: I've had the good fortune of thinking about these important and difficult issues in the crucible of what's become—little did we know at the time—a major bellwether of secondary liability. We represented eBay in the *Tiffany v. eBay* case.[9] And what I came away with from this experience is that the real world is dirty and messy, that this isn't a binary, clean situation, and that what appears to work best—and the question is, what are the mechanisms to make it work—is really a cooperative endeavor.

What you want in a workable trademark system is obviously ample and even robust protection for the rights of trademark owners, but also, in the setting of Internet commerce, to encourage innovation, to exalt this amazing new technology that benefits so many in so many ways, and also to encourage good faith enforcement activities and efforts by, among others, online intermediaries like eBay.

The experience we had, at least with eBay and its efforts, is—number one—that you need the cooperative effort for the system to work. You need the combination of continuing the primary policing role of the trademark owner, for all the reasons that are obvious. The trademark owner has the primary economic incentive and investment in its product and in the goodwill behind the trademarks. It has unique knowledge as to which of its goods are legitimate and which aren't. And the record in *eBay* was just filled with testimony from gemologists at Tiffany and quality assurance folks who said, "Oh my God! I've got to pull out my calipers and study this stuff in the lab." We all know that there's no way that eBay could look at a picture and figure out what's legitimate or not. That's just the reality. That's the dirty, real world reality that we face here: try as it might, eBay couldn't possibly replicate what the trademark owner can in terms of separating the wheat from the chaff, in terms of what's legitimate and what's counterfeit.

But at the same time, it does behoove the intermediary to provide ready, accessible tools, a workable means to facilitate the notice-and-take-down system. In our record, we had something like a quarter of a million notices, and the record showed that in each and every case, without dispute from Tiffany, within twenty-four hours—and by trial, typically within four hours—eBay took this stuff down. Now does that mean other stuff slipped through? Absolutely yes. Is there a perfect system? Absolutely not.

But the second opening comment I want to make is that I do believe that the current legal regime and the current rule evolving out of *Inwood* is sufficiently flexible and adaptable over time to make it work.[10] I don't think it encourages

9. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010).

10. *See* Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 854 (1982) ("Even if a manufacturer does not directly control others in the chain of distribution, it can be held responsible for their infringing activities under certain circumstances. If a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorially responsible for

minimal enforcement. It certainly doesn't encourage lying back and doing nothing but the minimum in terms of waiting for that notice.

I think the combination of cases like *Fonovisa*,[11] and *1-800 Contacts* in the Tenth Circuit[12] and *Louis Vuitton v. Akanoc*[13] all indicate that where a court senses that the defendant was lying back, and had a reason to know, if not actual knowledge, of infringing activity, there are ample means within the knowledge branch and the reason-to-know branch. And in grafting the willful blindness doctrine, [there are ways] for courts to separate out truly good faith efforts, amplified by significant investments in the case of an entity like eBay, from somebody who is just trying to slide under the radar, or worse, really trying to shield and foment infringement. So while the system isn't perfect, it strikes me that it works well.

Last preliminary comment: I think we ought to give the law time to keep working through, to really keep developing those factual situations. If and when there's a time to look at a statutory remedy, personally I'd prefer to see it down the road a bit, after more applications of the knowledge take-down standard against the real world facts we confront.

MIQUEL PEGUERA: Thank you very much. I'll try to be brief. I think the word is "balance," as we heard this morning. I would like to discuss some elements that may be relevant for achieving that balance.

On the one hand, I think that the nature of the underlying infringement must be taken into account. The mere use of an identical or similar mark doesn't necessarily raise a red flag of infringement. And of course, the search for a better balance in secondary liability for trademark infringement should not be a means to expand trademark rights, giving trademark owners exclusive control of the trademarked words—for instance, trying to prevent legitimate commerce or legitimate uses of them.

On the other hand, I think the current common law standards in the U.S. should be clarified in order to achieve more legal certainty. Legal certainty must be a goal. However, we must also take into account that a high level of certainty may actually impair the balance sought. In fact, open rules, with some inevitable degree of uncertainty, are necessary if all interests at stake are to be taken into consideration, while by contrast, clear-cut rules tend to be one-sided, as is the case, for instance, with Section 230 of the Communications Decency Act.[14] It works very well, but at the expense of giving service providers absolute immunity and completely disregarding the interests of the aggrieved parties.

In order to achieve a better balance, should we place a special duty of care on Internet intermediaries? Some duty of care is already established under the current law, as intermediaries are at least expected to react to notices of specific

any harm done as a result of the deceit.").

11. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1995).
12. 1-800 Contacts, Inc. v. Lens.com, 722 F.3d 1229 (10th Cir. 2013).
13. Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 658 F.3d 936 (9th Cir. 2011).
14. 47 U.S.C. § 230 (2012).

infringements. This standard might evolve to require the adoption of some reasonable measures, but I don't think that the service providers should bear the duty of monitoring or actively seeking infringement. This is not the current law in trademark, or in copyright, and I don't think this should be radically changed. Thus, the burden of policing should remain mainly on rights holders—though, of course, voluntary agreements by platforms to take preventive measures are certainly desirable.

That said, I think that bad actors—meaning those who clearly and purposely induce infringement or are willfully blind to rampant infringement—should not escape liability. Of course, willful blindness under current law is somewhat ambiguous, particularly regarding the question of whether or not it must refer to specific instances of infringement. I think that to find liability, willful blindness must be clear enough, but not necessarily constricted to specific instances of infringement.

Regarding particular types of intermediaries, such as credit card processing services and other financial intermediaries, I share the concerns expressed by the Ninth Circuit in *Perfect 10 v. Visa*, on the perils of expanding secondary liability to include such companies.[15] However, in light of facts that clearly indicate bad faith, such as in the *Gucci* case, I think that liability could attach.[16] Regarding the level of control needed to find contributory liability, I think that the Ninth Circuit's standard in *Lockheed Martin* sets the threshold too high when it requires direct control and monitoring of the instrumentality used to infringe the mark.[17] This standard should be better defined, and it should be clarified whether it requires actual control or just the ability to control.

I would also like to say something about the European situation, which I don't find to be satisfactory either, but maybe that could be in the following round.

IRENE CALBOLI: In this first round, I will focus my comments on two primary points. First, I would like to briefly react to some of the remarks that have been made today by panelists and commentators. Second, I would like to briefly mention the issues and, primarily, the challenges that have to be considered when discussing the international harmonization of laws in this area. In the second round, I will focus specifically on some of the challenges that I have witnessed firsthand while researching in this area with respect to the current status of the law in South East Asian jurisdictions.

If I can gather a general theme from today's many excellent contributions, it is that various parties across a large spectrum of constituencies—academics, legal practitioners and likely even the government—seem to generally agree that it is really the trademark owners who ultimately should carry the weight of policing the use of their marks in contexts of secondary liability. In other words, trademark owners are those "left holding the bag." This is not necessarily an unhappy ending for trademark owners, however. Instead, I would argue that this is an opportunity

15. Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788 (9th Cir. 2007).
16. Gucci Am., Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228 (S.D.N.Y. 2010).
17. Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980 (9th Cir. 1999).

for trademark owners, so that they can directly decide how to implement the monitoring protocols that they believe are best for their respective and varying business models. In other words, by setting ad hoc programs based upon their individual business needs, trademark owners can identify the types of infringement that they really care about. Not all infringements and infringers are equal, as we know; some are worse than others and nobody else can identify the "red alert" infringements better than trademark owners. To date, judicial decisions, in the United States in particular and perhaps also in Europe, seem to have fully embraced this approach, which I believe remains the best approach.[18] At one point, certain trademark owners were more interested in pushing for more liability for Internet service providers (ISPs), but did not succeed in their plea, as added liability for ISPs remains a very controversial issue. Of course, the heated debates in this area hide, at least in part, one of the main, yet not explicitly discussed, points of contention: namely the costs of "holding the bag." For trademark owners, intermediaries and the courts, costs (the cost of policing in particular) are not a negligent aspect of this debate. Still, at least in the United States, it seems that the courts have created a fairly balanced system, in which "bad guys" are usually stopped while legitimate business can continue in the marketplace. Moreover, today we have learned that the activity of policing can be outsourced to specialized entities, and that the costs of policing the Web are not as prohibitive as we may have thought. Accordingly, in spite of trademark owners' concerns, trademark owners can provide for those extra costs of monitoring, and in turn be able to have better and targeted information about the type and the extent of infringement that they want to stop. In light of these observations, not increasing the duty of care would thus be the best model for the future.

Still, from what Stacey Dogan again reminded us this morning, the debate about secondary liability remains in many ways a debate that reflects an underlying struggle between concepts such as morality and fairness in competition, but also about the efficiency of the overall market (and judicial) system. In other words, as the courts seem to indicate, it is a debate about stopping the "bad guys" but allowing (substantially) legitimate fair users and intermediaries to continue to do business, because they are useful for consumers, businesses and innovation.[19] Imagine a world without eBay, Google and Amazon, for example. I would not like to live in that world myself. Here is where I think that the American, and in general the common law, model has been able to find ways to strike a balance. This is a positive even if the balance relies on a very wide spectrum of standards to find secondary trademark infringement, spanning all the way from specific and actual knowledge to general and constructive knowledge, and even willful blindness to almost a negligence standard. Still, the real standard in most of these cases, at least in my opinion, remains a "we see the bad guys, and we know when we see it" standard.[20] The judiciary seems to carefully look at this standard first,

18. *See, e.g.*, Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 106 (2d Cir. 2010).
19. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).
20. *See, e.g.*, *id.*

and later elaborates on the type of knowledge and control that is required in the case at issue for a finding of secondary trademark liability. Stacey Dogan has argued this point in the past, and I defer to her work for a detailed explanation.[21] Ultimately, she argued, and I agree, that we are seeing a *Sony*-type of approach followed by the courts in many of these cases in the United States, and this is a positive development.

In light of these considerations, besides cultural differences, language barriers and so forth, I think that one of the main problems in creating a system of international harmonization in this area is one that is often at the center of many comparative law debates—the fact that we are dealing with two different types of legal systems: common law and civil law. We all know that the common law system heavily relies on judicial precedents, and that these precedents are authoritative. The civil law system considers judicial precedent, but does not rely on it in the same way. This difference is particularly relevant in this area, as most of the developments in secondary trademark liability standards have been happening as the result of judicial decisions rather than because of the implementation of new laws. This is an area in which the flexibility of the common law has permitted the courts to navigate difficult cases and ultimately adapt the law based on the facts of the specific circumstances at issue. Accordingly, even if it is true that the common law relies more heavily on statutory law than before, it remains a reality that, in most jurisdictions, statutory law does not yet include ad hoc provisions for secondary trademark infringement. In an area like the European Union, in which we have an integration of common law and civil law countries, this difference is something that we need to consider carefully while deciding how to create standards, particularly via legislative instruments. On the one hand, these instruments need to include guiding criteria for the civil law courts that cannot rely directly on the principle of *stare decisis*. On the other, these criteria need to be flexible enough to permit the courts to continue ferretting out the bad guys while allowing basically legitimate businesses to continue to serve consumers, as common law courts have been able to do so far.

JANE GINSBURG: Thank you very much. Before we go into our second round of reactions, I wanted to point out something that both Bob and Miquel talked about, because it might have been *sub rosa* in the morning but it deserves heightened attention now. In the morning, we mostly talked about the auction platforms and the service providers placing ads—those were our principal paradigms. Bob reminds us that there is another very important service provider, and that's the payment provider. With respect to trademark infringement, perhaps unlike copyright infringement, it really comes down to money. There are a lot of people out there liberating the content of motion pictures and popular music with non-monetary motives. But there's not a lot of file sharing of sneakers going on out there. So it does come down, to a large extent, to money, and perhaps we should focus a little more in this round of comments on how the standards for

21. *See generally* Stacey L. Dogan, *Is Napster a VCR? The Implications of* Sony *for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939 (2001).

secondary liability can reach the payment providers. Miquel evoked the two leading (and in some tension) decisions in the United States, *Visa International* and *Gucci*. You can take different lessons from those two cases. I think we'll stay in the order that we started, but I might ask that in addition to whatever comments you were going to make, please address the payment provider issue.

AMY COTTON: One of the reasons that I am reticent to engage in the statutory notice and takedown paradigm at this point is because it could very well be overtaken by events with the development of technology. I'm trying to understand the cloud—I don't know if you all are as well, but I'm having trouble with that. There are a couple of issues coming out. What's the obligation of a cloud service provider with regard to secondary liability? That remains to be seen. This new idea of content curation: are rights holders going to be able to identify the physical location of offending content that is retrieved by the curator? This relates to mobile applications. If you have a mobile app that tells you what gas stations are close by, there is no central takedown point. How is notice and takedown going to help you if everything is floating in the cloud, and these new mobile apps are pulling down from the cloud, with no central takedown point to get at it anyway? It seems to me that it's going to end some reliance on [notice and takedown procedures].

I think another point to think about—which in light of the domain name expansion process seems a little scary—is are we moving away from URLs? Are we moving away from search? Is scanning technology going to eliminate the need for browsers and search engines, when you can just scan in the code that takes you directly where you want to go? The idea of this new collective intelligence is can rights holders retain control over the public image of their brand when the online community increasingly wants to provide feedback about the brand? The brand is going to pop up all over the place, and how are brand owners going to be able to control that? With that on the horizon, and potentially the immediate horizon, it seems a bit backwards-looking to legislate a notice and takedown statutory regime. But certainly, I think that seems to be pretty well embedded in the system. Certainly it could be regularized. The notices could be better regularized, and I think the voluntary agreements in Europe are certainly informing that process in the United States.

Since we are talking about payment processors, there is a voluntary agreement with payment processors. They're all trying to make it so that the terms of use for that particular payment processor include a provision that says, "If you violate our policies, we will terminate your account." So, with that in mind, it seems that the trick is putting a lot of attention on these terms of use and enforcing them. What I like about the payment processor voluntary agreement is that the International AntiCounterfeiting Coalition stepped in to make it easier for both sides to implement it. They aggregate complaints for a particular payment processor or particular URL, and deliver those to the payment processors in a standardized form, which sort of greases the skids for the whole process. This is another way that the industry is stepping in to promote communication between the two sides, so that it can be a more efficient process.

ROBERT WEIGEL: You mentioned the *Perfect 10* case. I think it was probably my first day in law school, back in 1978, when somebody said: "Bad facts make bad law." If you just hear the facts of the case—one pornographer sued Visa because another pornographer had taken his pornography and was selling it on the Internet and accepting Visa cards—you just know how that case is going to come out.[22] It came out the way it did in part because it really was not a trademark case; it was a copyright case, and people could download it easily. The court held that you didn't need to take money to infringe on this person's pornography.[23] Judge Kozinski dissented;[24] I don't know what that means. But the *Frontline* case that we argued was a hard goods case. It was pocketbooks.[25] As Jane said, nobody is giving away pocketbooks. You need to get paid before the goods get shipped over the ocean. Somehow, money needs to go back to where the goods are made. Basically, a merchant contracts with a bank to process its credit card transactions, and the merchant will then, at the end of the day, present its transactions to the bank, and the bank will give the merchant ninety-five, ninety-six cents on the dollar. The bank will then process it through Visa, and it will eventually end up on your credit card statement. At the end of the day, the bank is actually lending money to the merchant when it gives the merchant the money, the ninety-five cents on the dollar, because if the transaction doesn't go through for whatever reason, or gets reversed, or somebody complains that they got a fake instead of a real thing, or it broke apart, the bank is on the hook to Visa to refund that money. And then the bank has to go look for the merchant. We were able to use that process to say that the bank is performing credit analysis on its merchants before it agrees to accept them. By having that interaction, the bank knew what they it doing, and that's how we convinced the court not to dismiss the case and to hold that the bank was liable.

In another case, one of the parties was an agent of the bank whose job was to go out and sell credit card processing services to various merchants.[26] It's a big industry that probably not many of us know too much about, but people do go out and say that they can get you credit card processing services. These folks were advertising that they could do things that nobody else could do, or that they would take on products that nobody else would take on. They would take on pornography, they would take on herbal supplements, they would take on gambling and they would take on replica Web sites. The judge found that we had stated a claim, on the grounds that they were inducing people to commit trademark violations.

At the end of the day, if you're shipping goods, the money has to go back, and that really is the only thing that's real on any of these Web sites. The money has to get to the person who makes the stuff, somehow. If you can get in the middle of that—if you can hold the people liable who are actually interacting with the

22. *Perfect 10*, 494 F.3d at 793.
23. *Id.* at 796–97.
24. *Id.* at 810 (Kozinski, J., dissenting).
25. *See* Gucci Am., Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228, 238 (S.D.N.Y. 2010).
26. *Id.*

merchant in some way and having a business relationship—you're not talking about scanning Web sites, but instead targeting somebody who actually reaches out and has some economic interest in knowing what this person does. If you can hold them liable and disrupt the payments, I think you can actually make some progress here.

I would just like to disagree a little bit with this concept that it is so hard to tell whether a site is selling fake stuff. If you look at a Web site, and they're selling fifteen different Tiffany jewelry products, and they're shipping it from China—and they'll say, "We're shipping it via EMS," the Chinese postal service—that's a fake Web site. I know that. I may not be able to go into court and say that just yet, but I know it. Why can't we have a system that imposes some requirement on somebody to shut that down until somebody comes and says, "Oh, by the way, my grandmother gave me a really big pile of Tiffany's stuff and I'm trying to sell it"? That will never happen. It's really a matter of who pays for the cost of looking at these Web sites and shutting them down. In reality, everybody knows. There'll be some exceptions around the edges, but certainly, I think there should be some sort of reasonableness standard imposed on the people who interact with these Web sites to say, "Come on, look at it, you know it's fake."

BRUCE RICH: The *Tiffany* case was brought—if anybody wants to dig back to the annals of the complaint and the earliest filings—on the premise that sales of lots offering five or more items of Tiffany jewelry were "invariably" counterfeit.[27] I remember standing up before Judge Buckwald, who was our judge originally, at our first conference just to chat about the case. She immediately pushed back on my able adversary by saying, "Wait a minute. I'm a Tiffany shopper. Are you telling me that if I decide someday, as I get my affairs in order, that I want to clean out some of my Tiffany goods and put them online, that I'm going to be in that category of counterfeiter if it is a lot of five?" The problem is, and the record of course demonstrated, that you could walk into the 57th Street Flagship Tiffany as part of a bridal shower and say, "I want to buy five gifts for my bridesmaids here," and they will gladly sell it to you. The problem is that the assumptions of "almost invariably" are wrong, and therefore finding that rule of reasonableness—let alone across, in the case of an eBay, potentially millions of new listings per day—is really an impossibility. And that is, again, dirtying our hands with the real-world facts.

I want to add just a couple words on why I think the accretive approach to development of the law makes sense here. We counsel a wide range of folks on both sides of the equation, but also a lot of social media platforms, intermediaries and content hosts. And I would say that, certainly dealing with the level of sophistication we typically deal with (and I know that issue came up earlier, and it's a challenging one), there is almost a uniform view that more is better, that not cutting the close line is the right way to go. Nobody really wants to test the implications of the back end of the *Tiffany Inc. v. eBay Inc.* ruling: had eBay not

27. Complaint at 11, Tiffany (NJ) Inc. v. eBay Inc., 576 F. Supp. 2d 463 (S.D.N.Y. 2008) (No. 04 Civ. 4607).

done all of these proactive things,[28] nobody quite knows what the inference from that is or should be. But I think no responsible person in this day and age wants to test it. I think the general view is there is a harmony of interest: safe trading sites and places where consumers are going to feel that they can trust the experience are a good thing, but the more people can do proactively—as a business matter that is also consonant with good legal practice—the better. And I think all of that, again, is going to continue to shake out over time.

Finally, on Jane's question: I am colored by an experience of about four years representing Bertelsmann in one of the post-Napster environment cases.[29] In that case, Bertelsmann, on the theory that no good deed goes unpunished, lent $85 million to the old Napster to assist it in converting to a fully compliant subscription service.[30] It was met by a class action lawsuit, on behalf of all music publishers in the United States, and each of the major record labels—then more than we have today—also sued.[31] Conservatively, the estimated damages were about $17 billion, on the premise that the money, which it was alleged was used to propagate Napster for eight months longer than it otherwise would have survived, at the rate of 10,000 estimated infringements per second—think about that—gave rise to this punishing liability.[32] So we gave a lot of thought to the issue of how far down the chain of investors—liability concept, in that case, under copyright law—makes sense. And I think, no differently than what we are debating and discussing today, there are deep and important policy considerations about how far down the line you reach, at least to good faith investors. And I think at least some of that resonated with me when I read *Perfect 10, Inc. v. Visa*.[33] I think it is just a really difficult area. It is somewhat facile, it seems to me, to say, "Well, they are the deep pockets. They can shut it off. Let them do it." I think we have to think beyond the immediate to the longer-term consequences for what fuels the economy.

MIQUEL PEGUERA: Yes, I agree with what Bruce was saying. We have to think about the consequences, and there are clearly dangers in expanding liability to these types of intermediaries. The mere fact that the payment processor is able to stop the transaction or make it more difficult for those transactions to take place is not enough to find liability.

On the other hand—I was reserving this final comment for the European situation—as you know, in Europe, we have this horizontal safe harbor scheme, but there are problems as well. Not only because of the different traditions in every national law, but also because of the interpretation of the safe harbors by the European Court of Justice. For instance, to benefit from the hosting safe harbor of the E-Commerce Directive,[34] the European Court of Justice has established a

28. *See* Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 98−100 (2d Cir. 2010).

29. UMG Recordings, Inc. v. Bertelsmann AG, 222 F.R.D. 408 (N.D. Cal. 2004).

30. In re Napster, Inc. Copyright Litig., 377 F. Supp. 2d 796, 799 (N.D. Cal. 2005).

31. *Id.*

32. A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 902 (N.D. Cal. 2000), *aff'd in part, rev'd in part sub nom*. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

33. *See* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 796 (9th Cir. 2007).

34. Council Directive 2000/31, art. 14, 2000 O.J. (L 178) 1, 13 (EC).

prerequisite that the service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored.[35]

I think this prerequisite is too stringent and does not comport with the actual language of the Directive. Actually, it was taken from a recital that does not actually deal with the hosting safe harbor, but with mere conduit and caching.[36] In any event, I believe intermediaries should be given more freedom to take voluntary preventive measures without the fear of falling outside of the safe harbors for not being neutral enough. That threshold should be lowered to avoid this situation. On the other hand, as we have seen this morning, when a defendant does not qualify for the E-Commerce Directive safe harbors, there is no harmonized regime for its potential secondary liability, as it depends on the national law of the member states with very different material regimes. In addition, injunctive relief is crucial, and nonetheless the E-Commerce Directive leaves it completely to national law, with the only limit that the relief granted does not amount to a general, rather than specific, monitoring obligation—a distinction that the Directive establishes in its recital 47.[37] And the meaning of that is not that clear. Some national courts have established an obligation to keep infringing content from reappearing in the future, though this may entail a sort of general monitoring obligation. I think that the limitations on injunctive relief should be clarified, particularly the relationship between Article 11 of the Enforcement Directive and Article 15 of the E-Commerce Directive.[38]

Finally, as a general remark, I would say that communication and cooperation between Internet platforms and rights holders is of the utmost importance, and some type of notice and take action procedure should be put in place. The Memorandum of Understanding on the sale of counterfeit goods via the Internet was a step in the right direction.[39]

IRENE CALBOLI: Following up on the remarks of the other panelists, I will first add a short comment on the issue of financial intermediaries, and from there I'm going to tie in the conversation about South East Asia. I agree that for financial intermediaries like Visa, Mastercard and PayPal, the same standard for secondary liability should apply that applies to other intermediaries. I think the courts in the United States have applied these standards quite efficiently so far, and

35. *See, e.g.*, Joined Cases C-236/08 − C-238/08, Google France SARL v. Louis Vuitton Malletier SA, 2010 E.C.R. I-2417, I-2514 ("Article 14 of Directive 2000/31 must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored.").

36. See *id.* at I-2512 to 13 (pointing to recital 42 in the preamble to Directive 2000/31).

37. Council Directive 2000/31, 2000 O.J. (L 178) 1, 6 (EC) ("Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.").

38. *See* Council Directive 2004/48, art. 11, 2000 O.J. (L 195) 16, 23 (EC); Council Directive 2000/31, art. 15, 2000 O.J. (L 178) 1, 13 (EC).

39. Memorandum of Understanding, *supra* note 8.

found financial intermediaries liable in several circumstances.[40] I also think that the possibility of finding financial intermediaries liable becomes even more crucial when it is linked to the previous discussion of harmonization of treatment of secondary liability across different jurisdictions. Sometimes, a Web site might be created in South East Asia, for example, and might sell products that are either explicitly counterfeit or that are made to look like genuine products. The Web site's IP address and corresponding ISP may be located in a jurisdiction in which the system of notice and take down does not work as well as it works in the United States and Europe. Thus, in the short term, the possibility of sanctioning payment service providers for this Web site in the United States may be the only means for trademark owners to stop the infringing activity.

I speak from firsthand experience. I wanted to purchase a DVD that was not available on Amazon, and I found it at the Web site www.pandadvd.com. The DVD was available for $16.99 USD. Because I did not know the Web site, I purchased the DVD via Paypal. Three weeks later, I received a "gift package" from Thailand, which contained a DVD that was obviously a counterfeit product. I had no idea that this DVD was counterfeit when I ordered it, but PayPal got its cut. A few weeks later, the Web site was gone. Obviously, this type of infringing activity is very difficult to stop just by "going after" the service provider or even the importers of the counterfeit products—as we know, only a small percentage of the contents of the shipments going through United States ports is actually inspected. This is why the ability to "go after" the financial intermediaries could be very effective to detect and stop, through findings of secondary liability, counterfeit activity that comes from foreign countries and that can be very, very difficult to detect.

And that brings me now to briefly address the situation in South East Asia. In particular, I was asked to address the current situation in the member countries of the Association of South East Asian Nations (ASEAN), which is set to formally launch the ASEAN Economic Community (modeled on the European Economic Community) in 2015 but which so far remains primarily a free trade area.[41] Just to better frame the discussion, ASEAN includes ten countries: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam. Three are common law countries—Malaysia, Myanmar and Singapore—while the others are civil law countries or mixed jurisdictions. What I found very interesting, while preparing my remarks, is that it does not seem that any of these countries has (at least explicitly and to date) developed a concept of secondary trademark liability as we have developed in the United States, in Europe and in other countries. Instead, in the various ASEAN countries, national trademark laws directly address only primary liability. Interestingly, in Singapore—the jurisdiction

40. *See, e.g.*, Gucci Am., Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228, 248 (S.D.N.Y. 2010).

41. *ASEAN Economic Community*, ASS'N SOUTHEAST ASIAN NATIONS, http://www.asean.org/communities/asean-economic-community (last visited June 1, 2014).

that I address specifically in the article that is published in this Symposium[42]—the Singapore Trademark Act provides that using a sign "to any material used or intended to be used for labelling or packaging goods" or "on any document described in subsection (4)(d) or in advertising" is not considered "use [of] the sign if, at the time of such application or use, [the defendant] does not know nor has reason to believe that the proprietor or a licensee of the registered trade mark did not consent to such application or use of the sign."[43] In other words, under Singapore trademark law, we have a de facto secondary infringement rule that is built within the provision on "acts amounting to the infringement of a registered trademark," which I elaborate upon in my article.

Yet, apart from this provision in Singapore, it does not seem that other ASEAN countries have any provision on the potential liability of intermediaries with respect to trademark infringement. Most jurisdictions seem to find guidance in this respect from the general principles of torts or other civil liability, depending on whether a legal system is based on common law or civil law.[44] We should also not forget that the majority of ASEAN countries remain less developed than many Western countries or Singapore. Accordingly, it is important to note that e-commerce is not as developed in these countries as it may be in the United States or in Europe. In this respect, the priorities in enforcement may be different in ASEAN jurisdictions than in the United States and Europe, and we still do not see the same attention to secondary trademark liability that we see in the United States or in Europe. In most of these countries, the focus remains on the production and exportation of counterfeit products in the brick-and-mortar markets—and unfortunately, we are truly talking about very significant amounts of counterfeit products manufactured in these countries.

That said, what I found very interesting while preparing my remarks is the ongoing attempt to export the American models in the provision of the Trans-Pacific Partnership Agreement (TPP), of which Brunei, Malaysia, Vietnam and Singapore are negotiating parties. As a matter of clarification, when I refer to the "ongoing attempt," I necessarily have to rely—like all TPP commentators—on the drafts of the TPP that have been "leaked" to the public; the TPP negotiations have been conducted "secretly," or at least without sharing the proposed texts of the agreements with academics, consumer associations and so forth. Based on the

42. Irene Calboli, *Reading the Tea Leaves in Singapore: Who Will Be Left Holding the Bag for Secondary Trademark Infringement on the Internet?*, 37 COLUM. J.L. & ARTS 593 (2014).

43. Singapore Trade Marks Act, 1998, § 27(4). *See also* Angela Leong & Candice Kwok, *Singapore*, *in* WORLD TRADEMARK REPORT 301, 308 (2005) ("Merely placing a trademark on a website which may be accessed by Singapore citizens is unlikely to constitute use of a mark in the course of trade in Singapore. However, if there are advertisements encouraging people in Singapore to access the website and/or to purchase certain goods or services, this may well constitute use amounting to an infringement, or use sufficient to defend a registration from revocation for non-use.").

44. *See, e.g.*, Zhize Xia, *Intellectual Property—China: Effect of the Tort Liability on IP Protection*, INT'L L. OFFICE (Mar. 15, 2010), http://www.internationallawoffice.com/newsletters/detail.aspx?G=928a447d-5ca0-4836-8e1c-8bd8a13d0c71 ("[W]here laws such as the Copyright Law, Patent Law and Trademark Law contain specific provisions on IP infringement, such provisions prevail. However, if there are no applicable provisions, the Tort Liability Law becomes operational.").

provisions of the leaked 2011 drafts of the TPP, it seems that Article 16, which discusses the special measures that countries would need to adopt with respect to enforcement in the digital environment (still primarily focusing on copyright protection), requires that all TPP negotiating countries—including four ASEAN countries—ensure that enforcement procedures "are available under [their] law so as to permit effective action against an act of trademark, copyright or related rights infringement which takes place in the digital environment."[45] This includes "expeditious remedies to prevent infringement and remedies which constitute a deterrent to further infringement."[46] Even though the provision doesn't indicate specifically how to meet these objectives, the fact that the provision explicitly requires this type of enforcement is an important change for those countries that, to date, do not provide ad hoc secondary liability for trademark infringement in the online environment.

I conclude by noting that in the area of secondary copyright infringement, we still do not have many cases on point from ASEAN jurisdictions. For example, as I elaborate in my article, Singapore's courts have developed standards similar to United States contributory infringement standards in copyright decisions. They have addressed the concept of "authorizing" infringement under the Singapore Copyright Act, which (like other Commonwealth countries) still considers "authorizing" infringement to be primary infringement.[47] The principles elaborated on by the courts in those cases could be usefully imported into future trademark cases related to secondary liability. Still, we currently do not have specific provisions establishing secondary trademark liability in national laws of ASEAN countries, and we have limited or nonexistent national judicial decisions on point. Then, in some ASEAN countries, we have the possibility that following the adoption of the TPP (should the ongoing negotiations lead to a final agreement), American- or Western-model provisions on secondary liability may be implemented in the national laws of these countries. Ultimately, the current TPP draft provisions do not indicate what the standards to find secondary trademark liability should be.[48] Based on these observations, the next decade will certainly be an interesting time for the development of national laws on secondary trademark liability in ASEAN countries, and we may see interesting judicial developments as well.

45. *See* Draft Trans-Pacific Partnership Agreement, art. 16.1, Feb. 2011, *available at* http://keionline.org/sites/default/files/tpp-10feb2011-us-text-ipr-chapter.pdf. The same provision has been retained in a later draft, dated August 30, 2013 and leaked on November 13, 2013. Vietnam is opposing this provision, while Singapore supports it, and Brunei and Malaysia are still considering the language. *See* Trans-Pacific Partnership Intellectual Property Group Draft Treaty, art. QQ.H.10, Aug. 30, 2013, *available at* https://wikileaks.org/tpp/static/pdf/Wikileaks-secret-TPP-treaty-IP-chapter.pdf.

46. Draft Trans-Pacific Partnership Agreement, art. 16.1, Feb. 2011, *available at* http://keionline.org/sites/default/files/tpp-10feb2011-us-text-ipr-chapter.pdf.

47. Singapore Copyright Act, 1987, §§ 31(1), 103(1).

48. *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, STATEMENT OF THE MINISTERS AND HEADS OF DELEGATION FOR THE TRANS-PACIFIC PARTNERSHIP COUNTRIES (Dec. 10, 2013), *available at* http://www.ustr.gov/tpp.