SESSION 7: ENFORCEMENT AND MULTILATERAL LAW
7A. Copyright and Trademark Enforcement

**Moderator:**
Ann Bartow
*University of New Hampshire, School of Law, Concord*

**Speakers:**
Paul Maier
*European Union Intellectual Property Office, Alicante*

Transatlantic Cooperation Between Enforcement Authorities and Joint Actions Fighting Counterfeiting and Piracy

Raymond J. Dowd
*Dunnington, Bartholow & Miller LLP, New York*

New Help for Copyright Lawyers? How the Federal Communications Act Should Transform Television Antipiracy Strategies in the IPTV (Internet Protocol Television) and OTT (Over-The-Top) Era

Susan Scafidi
*Fordham University School of Law, New York*

Oxymoronic Infringement: Do “Legal Fakes” Exist?

Gareth Dickson
*Taylor Vinters, Cambridge*

The GDPR: Boon or Bust for IP Infringers?

Richard Pfohl
*Music Canada, Toronto*

Online Copyright Enforcement Developments

**Panelists:**
Fiona Phillips
PROF. BARTOW: In the interest of time, I am going to go ahead and introduce the speakers and panelists.

I will start with me. My name is Ann Bartow. I am on the faculty of the New Hampshire School of Law, formerly known as the Franklin Pierce Law Center — and yes, you can ask me why we dropped the Franklin Pierce. Didn’t we know anything about trademark law there? Yes, we do. Nevertheless, the University of New Hampshire is our name going forward.

Our speakers are: Paul Maier from the European Union IP Office; Raymond Dowd of Dunnington, Bartholow & Miller; Susan Scafid i from Fordham Law School; Gareth Dickson from Taylor Vinters in Cambridge; finally, Richard Pfohl from Music Canada in Toronto. Our two panelists who will be aiding with the discussion are Fiona Phillips and Mary Wong.

Take it away, Paul.

MR. MAIER: Good morning, ladies and gentlemen. It’s a pleasure to be here in this enforcement panel.

I want to talk about the transatlantic cooperation between enforcement authorities and joint actions fighting counterfeiting and piracy. I will not talk about case law at all; I will not mention laws as such; I will just make a pragmatic presentation on how transatlantic cooperation works — hopefully it works, but you will be the judge of that — and how we make it function in the best possible way.

The first thing is, just to set the scene, to give you an idea, these are some comparative figures between the United States and the European Union, about the importance of IP-intensive industries in our economies.

The importance of IP-intensive industries is considerable, as you can see.

- 28 percent of the employment in the European Union is generated by IP-intensive industries; 18 percent in the United States, much less.
- 42 percent of GDP on both sides.

These industries also pay much better than the rest of the sectors. The conclusion to be drawn from these figures is that these industries are formidably important for our respective economies.

There is one figure I haven’t put up because we don’t have a comparison with the United States. IP-intensive industries also correspond to 93 percent of exports of the European Union.

Now, faced with that, let’s look at how much counterfeiting costs us. Counterfeiting is immense. The new study that we issued together with the OECD shows that 3.3 percent of international trade is counterfeit and up to 6.8 percent of imports into the European Union is counterfeit.1

---

These figures are staggering. Some of our main economic sectors are being heavily attacked by illegal practices. So the next question is: How do you fight against counterfeiting and piracy? The first thing that needs to be done is that you have to get together an incredible number of different authorities and stakeholders. Indeed, IP is transversal in the economy and the way our governments are organized. There are indeed specialized bodies in all our countries that deal with IP, but there are also many administrations that deal with the matter without it being their main priority.

You see here a list of national authorities that may have to deal with IP infringements. It might actually not be complete. There may be others that come in also, like health authorities, etc. The list is long and varied.

In the European Union, participants include Europol, Eurojust, EUIPO/Observatory, and European Commission services (TAXUD, OLAF). At the international level, I have only listed those that are directly involved in enforcement: Interpol, the World Customs Organization (WCO), and a series of UN agencies. WIPO is not very active in enforcement because it does not have a mandate for that. If one wants to fight IP crime efficiently, it is necessary for these many different organizations to work together.

In the United States, the U.S. National Intellectual Property Rights Coordination Center (USIPR) brings together all U.S. agencies that have an interest or competence in fighting IP crime. The IPR Center is led by Immigration and Customs Enforcement (USICE). Its role is to coordinate everything that happens in the United States regarding IP infringement. It includes nineteen federal agencies (e.g., USPTO, FBI, USICE) and also it has correspondents from Interpol, Europol, Canada, Mexico, and the United Kingdom. We do not have an equivalent central coordinating body in Europe. I think this is a subject our policymakers will have to think about.

How does transatlantic cooperation function?

First, the USIPR Center and Europol have almost daily contacts. We do have a representative from Europol sitting in Washington who participates in all of USIPR’s monthly meetings. On the other hand, U.S. administrations are represented in Europol by some thirty correspondents (e.g. USICE, USIPR, FBI, DEA, FDA). They follow all areas of crime including IPR infringements. The Royal Canadian Mounted Police also has several correspondents in Europol.

This is how enforcement works. The enforcers send people, who are either called points of contact or liaison officers, who are involved in all the criminal cases that will be of importance also for their country. Once an investigation that is of importance is identified, the points of contact make sure that their administrations back home are informed in detail and rapidly of the case so that they can participate in the enquiries, and eventually in action on the ground, in a coordinated way.

Judicial cooperation is mainly a question of obtaining evidence. The typical case is one in which an inquiry takes place and elements outside the territory are required to be investigated in order to complete the file of the prosecutor. It must be said that cooperation between prosecutors functions well between Europe and the United States. It seems that when our prosecutors contact U.S. prosecutors, they usually get an immediate response of the highest quality. What is usually needed on the EU side are elements related to Internet-based U.S. companies. Since U.S.-based companies are among the leaders in the world in such technologies, it is logical that their help will be key. In this way our prosecutors will be in a position to ask through US prosecutors these companies for information or actions.

The types of interventions which are predominantly requested relate to: requests for data freezing; basic subscriber identification in order to pursue the investigation; and sometimes content detail.

We have an agreement of mutual legal assistance with Canada. However, the
reality is that examples of cooperation with Canada in IP cases are much less common than with the United States. Some prosecutors report that Canada usually requires that an Internet company has been asked to make voluntary freezing of data before the authorities will accept a formal request for mutual legal assistance with the aim of transferring the data to the European Union.

I would like to give you three examples that illustrate the cooperative international enforcement operations. These operations are performed on a regular basis (in principle, every year):

• Operation In Our Sites (IOS) is a joint global recurrent action against illegal domain names. Previously identified sites on which illegal activities are performed, many involving cross-border criminality, are closed down and the domain names are seized. Europol’s Intellectual Property Crime Coordinated Coalition, the USIPR, and law enforcement authorities from twenty-seven EU Member States and third parties, facilitated by Interpol, have seized over 20,500 domain names.

• Another operation, which is well-known internationally, is the Pangea action, which happens every year. It is coordinated by Interpol and the U.S. and European authorities are closely involved. This deals with counterfeit and substandard medicines, which of course is a major problem in the fight against counterfeiting. It has a strong focus on African nations, but there are also many problems with such products in the United States. In Europe, the system of distribution of medicines is more controlled in a number of Member States, but this is still a considerable problem. Trafficking of such products is organized by international crime groups. Without close international cooperation, there could not be a solid response to these threats.

• Another cooperative enforcement operation I want to talk about is Ayurveda, which is a more recent initiative. This involves counterfeit and illicit pharmaceuticals as well. One of the main cases was production in Spain and shipments to Asia, Africa, and the United States of fake medicines. That operation was coordinated between the Spanish Guardia Civil, Europol, and the U.S. Food and Drug Administration. A number of people ended up in jail, so you should know that counterfeiting is not a crime that remains unpunished.

A few conclusions. We all know that the reports show that organized crime is behind counterfeiting and piracy. I should add that we have to deal with organized crime of the worst sort. The criminals who are involved in these activities are usually also dealing in many more crimes like human trafficking, money laundering, sometimes arms or drug sales, etc.

If we want to efficiently fight against IP crime, we need the public and private sectors to work together because only close cooperation will help us to be efficient.

From the national to the international level we have to work together well, and I can say that so far cooperation between the United States and the European Union has functioned really well. There is very good cooperation between countries as well.

The problem with that is that IP is cross-cutting. You not only have to involve people and organizations that have a competence in IP. The World Health Organization has interests when it comes to drugs. A number of cultural sectors have interest even if they do not have a mandate as such to talk about IP. All need to bring their knowledge and competences to ensure that the response of law enforcement is adequate.

Last but not least, central coordination between both sides of the Atlantic is a real asset. Central coordination is already ensured on the U.S. side. The European Union will have to make sure it continues to achieve a good level of coordination even if no strong central structure has been created so far.

I will be very happy to answer any questions. Thank you very much indeed.
PROF. BARTOW: We do have a couple of minutes for questions.
I will start out with a question on medicines. Of course, the idea of counterfeit medicines is very alarming to everyone, but, as other people have pointed out, there is no health impact of a fake purse generally. How do you allocate your priorities? Is it mostly for counterfeit goods that are health-related?

MR. MAIER: No, not mostly. Europol has had operations in a number of sectors. I have here mentioned some in which the United States was also involved. But there are operations also on the luxury goods sector. There was a major international action two years ago in spare parts, which was basically a joint operation made between the European side and South Asian countries where many counterfeit spare parts were seized.

We do not prioritize as such, a priori. If it is determined that it is important to have a cooperative operation, first you need to gather evidence to evaluate the size of the problem in terms of the organized crime groups involved, proceeds obtained by these organized crime groups, and the risks for society as such (which can be health and safety linked, but not solely). It is also important to add that EU-wide or international operations only then are considered. If a crime is manifestly limited to a particular Member State, then it will not be investigated with Europol; the competent national authorities will deal with it on their own.

IPTV was one of the major actions that has been organized recently. Somebody else on the panel may wish to mention details about it later. I can add that further actions on IPTV may be foreseen. These were major. A lot of money was seized. People were jailed. A private plane, several luxury cars, villas, etc., were seized.

So there is no a priori, but we need to have solid evidence before launching launch operations.

PROF. BARTOW: Panelists, any questions?

MS. PHILLIPS: One of the rationales for the involvement of organized crime in IP infringement has been that it is low risk and high rewards compared with other kinds of crime. I wonder if the risk profile for the infringers has changed with the move to online forms of counterfeiting and piracy.

MR. MAIER: Obviously, the online part of it has changed a certain number of things, just as it has changed the legal market as well. This is obvious.

The first reason for IP crime you have mentioned yourself: indeed, there is a lot of money to be made in counterfeiting and piracy. This is why I showed the first figures, the €120 billion of imports.

Secondly, it is still, unfortunately, a quite a low-risk illicit business. If you are caught with a couple of kilograms of cocaine, you go to jail for many years. Punishment is not the same in many countries if you tried to smuggle a couple of containers full of fake shoes and you get caught. So indeed, the reward-and-risk balance is formidably in favor of IP crime.

Organized crime is probably a very big word for some of you here today. Let me give you the example of Italy. In Italy, counterfeiting, and probably piracy as well, has become one of the major ways in which the mafia is financed. Actually, the state of law is at risk because of that. So heavy criminality is behind counterfeiting and piracy.

And these organized crime groups are very opportunistic and, I must say, formidably adaptable. They will do everything they can if they see that there is money to be made. Basically, that is the rule: if there is money to be made with an activity (be it counterfeiting or piracy or any other type of crime), these organized crime groups will engage in the activity.

PROF. BARTOW: Do we have a question from the audience?
QUESTION [Jean-François Boittin, Coalition Pour la Diversité Culturelle]: You said that employment in IP-intensive industries is 28 percent in the European Union and 18 percent in the United States, and in terms of GDP it is 42 percent versus 38 percent?

MR. MAIER: Yes.

QUESTIONER [Mr. Boittin]: Those are either bad numbers or there is a very low level of productivity in Europe.

MR. MAIER: The first thing is that when we speak of IP-intensive industries, we actually mean the entire production industry. Let us take the example of the motor car industry. In the European Union, the cars are still almost entirely produced in Europe because the low-wage new Member States have allowed investment there.

Such is not the case in the United States. Indeed, it seems that U.S. car makers have invested in low-cost countries (e.g. Mexico) in order to maintain their productivity. That makes a dent in your GDP, of course, because the production in these countries will no longer appear in the US GDP.

The fact that the U.S. percentage of GDP is 38 percent whereas they have only 18 percent of employment is not something bad. That simply shows that American companies have kept their investment in high-value jobs in their own territory.

PROF. BARTOW: Thank you very much.

We need to move on to the next speaker, Raymond Dowd, who has the best pocket scarf on the panel so far.

MR. DOWD: I would like to thank Hugh Hansen for hiring a guy with a bomb to throw at me when I end this presentation.

And I’d like to throw a bomb right back at all of you. Three takeaways I hope you get from my presentation: (1) there is a crisis; (2) there is hope; and (3) it is time to act.

The crisis: We have heard in many presentations over these two days about recent statistics showing that 6.5 percent of online television streaming is pirated. That was in late 2017, and I think it is higher than that now. Some of the presentations that I have seen this morning also back that up.

Right now, I can get on the Internet and watch content for free. If I pay a little bit, I can get very steady, good content. I can watch television, I can watch movies, I can watch particularly European content or content from other parts of the world very easily. I can do that by buying a little device, getting an access code that I put into the device, buying a Smart TV, downloading and installing an app, and putting in an access code. That is very easy to do.

As a copyright lawyer, my day job is to appear before the Southern District of New York, considered one of the most sophisticated copyright jurisdictions in the world — at least that’s how we like to think of ourselves.

I think Devlin Hartline was correct when he said that the Digital Millennium Copyright Act (DMCA) Section 512 is broken. We heard a question yesterday about whether Section 1201 was broken — I think it is. One subscriber to a broadcast can rebroadcast it anywhere, and downstream of that the courts have said that the DMCA doesn’t apply.

Try to get injunctive relief post-eBay in the copyright context; doesn’t work. Try to get attorney fees; very unreliable — “Who is the prevailing party? What is the amount

---


of work that the lawyer put in? Was that really warranted?” So, you are spending money on attorney fees that you cannot get back even when you win and you cannot get an injunction.

A hopeless situation? No.

In the materials is a four-page paper on the Federal Communications Act of 1934 — music to content owners’ ears — mandatory attorney fees, statutory damages, without registering anything. So, if you have a foreign broadcaster that hasn’t registered its copyrights in the United States — trademark; what’s a trademark? — you can still get statutory damages and attorney fees.

The Federal Communications Act of 1934 can transform civil litigation into a profit center. How does it do that?

We heard this morning from Michael Mellis how a Major League Baseball broadcast is created [Sunrise Seminar II]. He talked about a broadcast truck. What’s on top of the broadcast truck? A satellite transmitter.

I would like to read from page 4 of my presentation some “magic words.” We as civil litigators like magic words from a judge that we can drive a truck through. Here are the magic words:

I conclude that the third sentence of Section 605(a) does not require pleading or proof that the defendant intercepted a satellite transmission or other radio communication. The statute reaches the unauthorized retransmission of a signal that originated as a satellite transmission even when it is thereafter received or transmitted over the Internet.4

If we creative lawyers can find a satellite transmission anywhere in the way that the content gets to the consumer, we can drive a truck through that language.

How are we doing that? We are going after the folks who are putting up these pirated sites; we are seeing the vast amount of income that they have; and we are taking them down.

How are we getting it? Through local payment processors. Consumers are using credit cards, PayPal, and other payment processors. You can get at them and you can get a lot of that money back.

I suggest that the Motion Picture Association ought to rethink its naming strategy and call itself the Satellite Content Providers Association, because copyright doesn’t have really strong, easy, effective enforcement mechanisms the way the Federal Communications Act of 1934 does.

Why is that? In copyright we have this whole weighing and balancing of the rights of authors. I wrote a book called Copyright Litigation Handbook.5 I have a blog called Copyright Litigation Blog.6 I am a big believer that copyright should have solved these problems.

In the broadcast context, it really is at its core just stealing. If you can show that somebody is taking your content and copying it — so we don’t run into “Well, is there ‘substantial similarity’; is there any freedom of speech?” — no, you are taking someone’s

---

radio or satellite communications, you are copying them, and you are reoffering them wholesale to the public. It is really just pure pirated content.

That is what we are facing now. Is the eighteen-to-twenty-five-year-old market in the United States going to pay for Netflix when they can get it for free?

If you are a European living in the United States and you want to watch a soccer game, how are you going to find it? You are going to go on the Internet, you are going to not pay very much, or you’re going to pay a pirate, and you are going to watch the broadcast, because you can’t find it easily otherwise. I know that some of the broadcasters have said the contrary, but this is what I’m hearing from people.

There is a crisis. There is hope. It is time to act.

PROF. BARTOW: Nice job keeping on time too. We have five minutes for conversation.

I will ask the first question: What kind of statutory damages would you expect to get, in what kind of context, and who would pay them?

MR. DOWD: It depends on who you are going after. I know a lot of consumer-friendly content providers are not going to want to go after the grandmother whose grandchild takes something off the Internet. Violations range from $1,000 to $10,000 per violation; for a device it’s $10,000 to $150,000. That’s pretty good money.

And again, let me emphasize, because it’s really music to my ears, that there are mandatory attorney fees. The case law is that it has to be what the attorney expended and that the attorney is supposed to get the money back, which is not the balancing factors that you have under copyright law.

PROF. BARTOW: Panelists?

MS. WONG: I guess it’s my turn to say something. I keep wondering why I’m on the panel. It’s not so much a question or a comment on your or Paul’s presentations, but just to follow up on what seems to be the rising tide of the crisis and the consent.

At the Internet Corporation for Assigned Names and Numbers (ICANN), we are certainly seeing that as an observer, but also we are seeing a lot more conversations happening within the domain name industry because of the players, because of the path of traffic, and various things.

It always sounds a little bit defensive for me to sit here or at any other panel and say, “ICANN doesn’t do content regulation.” We don’t, but we dive in a little bit deeper.

Essentially, our remit is very narrow and very technical. We sometimes find that folks come to ICANN and say, “Can you help us take this site down or take this domain down?” or “What can we do if there’s all this counterfeiting traffic and all this illegal content?”

There is sometimes a fundamental misunderstanding of what we can and cannot do. We do have contracts with the registrars that sell domain names, for example, and they are obligated to cooperate with law enforcement.

Paul, you mentioned operation in our sites. That is the role of law enforcement, but it is not like we can turn over a whole bunch of registrant names and domain names to anyone who asks, whether they are content owners, rights holders, or law enforcement.

While there are things that we can do, it is within a limited remit that is constrained by the extent of the contracts we have with the industry folks who sell the domain names.

The main point I also wanted to make is that we certainly are seeing these conversations. We are seeing quite a lot of blog posts and other things saying, “ICANN is getting drawn into content regulation and helping law enforcement.” I know that this audience doesn’t have that misconception. But this is really something that we are watching quite closely.

Thank you.
PROF. BARTOW: Do we have questions from the audience or other panelists?

MS. PHILLIPS: I want to make an observation. I think the two presentations that we’ve heard so far show an interesting dichotomy, one approach going after the source of the infringing content and the other targeting the end-user. There are two different approaches to enforcement: do you stop it at its source, or do you stop it at its destination? There has been a really interesting evolution in approaches to piracy and counterfeiting.

MR. DOWD: Remember Napster? The music industry sat on its hands for a number of years and then, really when it was too late, started overreacting and going after consumers. I think that’s history. What we are seeing now is we are a few years into a Napster-like attack on these content owners, and they are not really stepping up to the plate in terms of boots-on-the-ground enforcement.

MR. MAIER: I think that enforcement is only one of the things that you should do in copyright, and in the intellectual property world in general, if you want intellectual property rights to be protected efficiently.

What you first need, of course, is good laws, right? Without good laws you are nowhere. That’s the first thing.

The second thing is — and that’s what I was talking about — you have to fight as efficiently as possible against the real pirates, the real counterfeiters, the traffickers, the criminals. You have to do that. This is where Europol comes in. This is criminal law. You are also expecting more civil damages and other legal remedies.

The third thing is that consumers, and policymakers and judges as well, must be made aware of the importance of IP. They have to be aware of the fact that this is not a victimless crime. We must make sure that people know what they do.

We work a lot on education. The EU Council of Ministers introduced in our key competencies for lifelong learning developing key elements to be included in the curricula of all pupils in the European Union, a series of elements that relate to IP: respect of the law, the importance of creativity and entrepreneurship. This is long term, but the idea is that we need to invest in such notions in order to make Europeans aware of the importance of these issues.

The last thing is, if you want to fight, you also have to have legal offers available. Without one of these four elements you will not fight efficiently and effectively against infringements of IP.

PROF. BARTOW: Our next speaker is Susan Scafidi. She is the pioneer of fashion law generally and founder of the Fashion Law Institute at Fordham. She has been a friend for a long time, and she is always a great presenter, so I am excited to be moderating this session.

PROF. SCAFIDI: Thank you, Ann.

In an act of shameless self-promotion for Fordham, I want to note that Fordham Law School just published the first fashion law issue of the Intellectual Property Law Journal, and Ann was actually our featured author. Lovely to have Ann with us. Thank you.

It is wonderful to be here this morning. Thanks to all of you, and thanks to Hugh.

I was just charged by one of my fellow panelists, Richard, with addressing our distinguished moderator’s comment about fake handbags.

Of course, Ann is well aware that they are damaging to your moral fiber (at least I would argue), but actually, with respect to toxicity, the U.S. State Department is planning a study on that now. So, we will find out. Probably not as dangerous as fake pharmaceuticals, but maybe not as clean as we thought.

My topic for today — Hugh-approved of course — is “Oxymoronic Infringement: Do ‘Legal Fakes’ Exist?”

How many of you have heard of legal fakes?
[Show of hands]
A handful. It is a concept that is developing in the popular press, and I’ll talk to you about the vector through which that is happening.
How many of you recognize this logo?
[Show of hands]
I guarantee you, if we had a roomful of eighteen-to-twenty-five-year-old young men, or of teenage boys, in fact every hand would have been raised.
Supreme is a U.S. streetwear brand that has been absolutely sweeping the globe. It started in 1994 as a tiny downtown skate shop in New York — very cool, very edgy, very under the radar — and has grown dramatically. Vogue magazine recently had a feature article on Supreme.

Think about Supreme, and the way it has grown so dramatically by staying small — one shop; then a handful in Japan; recently some shops in Europe.
It has drops once a week. Limited, exclusive product. Every Thursday — and almost every day of the year, in fact — there are lines around the block of people waiting to buy product. In fact, the Thursday drops have become so popular that you have to enter a lottery to get in line to hopefully buy product at the Thursday drops.

The most coveted merchandise of all is their box logo merchandise; that is to say the merchandise with its red box logo with the word “Supreme” written on it.
James Jebbia, the founder of Supreme — again very secretive, under the radar, seldom speaks to press — did admit in 2009 that he didn’t even have a trademark on Supreme, for a couple of reasons. He says, “It’s a good name, but it’s a difficult one to trademark” — in part, because in the United States there was another owner of the mark SUPREME for menswear; but also because there is some concern about whether “Supreme” is merely descriptive of the goods, a concern that exists now in Europe.7
As an aside, Supreme has gotten some pushback about its logo. Some of you may be familiar with the artist Barbara Kruger, who uses these red boxes and this Futura Oblique font on the vast majority of her work, and Supreme has been accused of stealing that style. More recently, she commented on this issue. I won’t read it aloud. It’s a little rude. When Supreme was suing another streetwear brand, she referred to them as “totally uncool jokers,” among other things, because much of her work is anti-consumerist. And artists never know the difference between copyright and trademark, but that’s another story.
That aside, Supreme has been so successful that it has moved into the mainstream, maintaining its exclusivity but expanding via a series of collaborations. I think the one that many fashion people first noticed was the collaboration with Comme des Garçons in 2012; and then, in 2017, the collaboration between Supreme and Louis Vuitton — so popular that they ended up having to cancel the drops in a number of Vuitton stores for crowd control reasons, which is quite interesting.

With that much interest in a brand, you can assume that there will be some copyists and perhaps some trademark squatters, or maybe both.
The phenomenon that we have seen arise appears to be traceable to a company called International Brand Firm out of the United Kingdom actually registering “Supreme Italia” in San Marino and Italy and subsequently in Spain. Alongside the iconic Supreme red box logo they use a yellow hangtag that is somewhat different, and they do business as Supreme Italia.

7 See generally From the Name to the Box Logo: The War Over Supreme, THE FASHION LAW (Feb. 22, 2018), https://www.thefashionlaw.com/from-the-name-to-the-box-logo-the-war-over-supreme/.
They have actually gotten so much traction and sold so much product — because they are not interested in small, limited-edition drops; they are interested in making money very quickly — that they actually induced Samsung to do a collaboration with them. Samsung last year announced a huge collaboration with Supreme, had a big event in Asia, trotted out two people whom they said were the CEOs of Supreme onto the stage, only to realize a few days later they had the wrong Supreme, at which point that collaboration was canceled.

Of course Supreme, the original U.S. company, is fighting this around the world. They have come out from behind the curtain to do so. But the website “Supreme Italia” is still up.

In the press coverage of this issue around Supreme, there has been a lot of conversation around the concept of “legal fakes.” In fact, there was an adverse ruling in a court in Trani in southern Italy that had originally impounded these websites and seized a lot of merchandise, but then re-released it because it reasoned that since there was a registration, the sites and goods must be legal. In the press coverage of this issue around Supreme, there has been a lot of conversation around the concept of “legal fakes.” In fact, there was an adverse ruling in a court in Trani in southern Italy that had originally impounded these websites and seized a lot of merchandise, but then re-released it because it reasoned that since there was a registration, the sites and goods must be legal.8

Here’s a picture of the opening of the Supreme Italia store in Shanghai, again using the iconic Supreme red box logo, and Supreme Italia has announced the planned opening of about seventy more stores.

From a legal perspective, don’t we have this covered? Isn’t this a famous marks problem? Don’t we have the Paris Convention and TRIPs to help us out on this?

And don’t we have lots of cases in the past on well-known marks? “Mc-anything” anywhere in the world is likely to receive a cease-and-desist from McDonald’s. We have also had famous marks cases in the United States having to do with mere dilution.

However, this old problem of famous marks or well-known marks is re-emerging now in a new context, sparked by the perfect combination of Internet-driven brand awareness globally, the move to e-commerce, and things like limited-edition merchandise, much of which is traded on the resale market. Because certain streetwear drops are so limited and so desirable, there are active resale platforms that have arisen around it.

There is also the additional concern about this new rhetoric that even most people in this room haven’t heard, and that is the concept of “legal fakes.” After all, Supreme Italia was operating under color of law; they received registrations for SUPREME in Italy. During the period when that registration was on the books, before the court said otherwise, all of this merchandise appeared to be legal. So lots of unsuspecting third-party distributors, landlords, resellers, and resale platforms actually bought into this concept of “legal fakes.”

In addressing this new iteration of the famous marks issue, which has revived and is continuing to expand under the misleading moniker of “legal fakes,” we might consider a few options:

• Updating the protection of well-known marks in general, because I think this is a vector that has affected not only streetwear via Supreme but will affect lots of other areas.
• Additional harmonization, such as eliminating the local use requirements for the recognition of famous marks that exist in some jurisdictions.
• Clarifying the requirements for what constitutes a famous or well-known mark.
• Perhaps a fast-track for cancellation in the way we have a fast-track for registration in the Madrid Protocol.

And, of course, increased public awareness around the idea of “legal fakes” and why that would be a misnomer, potentially an expensive one for unsuspecting third parties. I am over my time. The bomb has gone off.

PROF. BARTOW: Nice job. Thank you.

PARTICIPANT [Massimo Sterpi, Gianni, Origoni, Grippi, Cappelli & Partners, Rome]: I have some first-hand information for you.

We acted in another case, Noah clothing — same phenomenon, identical — and we won the case. We got an interlocutory injunction against these people based on the international reputation of the trademark, at least in the relevant circles. Based on the number of accesses to the website of our clients and the reputation of the trademark in Italy based on a few articles in the press, even if it was a very niche brand, we got an injunction even if there was no registration in Italy and limited sales. I will be happy to share this decision with you because it is very well-written and also informative.

We researched the subject a bit more. Actually, this phenomenon of “legal fakes” originated in a small town in Apulia called Barletta. There, many different companies — probably inspired by a single mastermind — registered twelve or thirteen different brands, all of them streetwear brands from the United States, that they have more or less the same pattern: they become famous in a very small social group in the United States and then immediately get worldwide recognition. But the fame is faster than the trademark registrations, so the companies in Barletta decided to fill this void and get the registrations first.

The Supreme case is particularly telling. The Supreme people, because they lacked registration and they had a few problems related to the potential lack of distinctive character of “Supreme,” acted in both the criminal and civil courts. But the other side did not stop their activities, so what is pending is a real war being fought on many different fronts.

PROF. SCAFIDI: Thank you so much, and I would love to hear more about that. My research turned up a number of cases traceable to Barletta. It’s lucky that in Italy there is no physical local use requirement, no local sale requirement for the recognition of famous marks. But in a number of countries there is, and that is another great concern looming on the horizon.

PROF. BARTOW: I have a question. You didn’t really get a chance to talk about the solution. I’m suspicious and nervous that the solution is going to sound a lot like secondar meaning in the making.

PROF. SCAFIDI: Could be, yes, though in the Supreme case secondary meaning already existed and simply hadn’t been recognized by the relevant trademark authorities via a registration. The ultimate solution is something that I haven’t truly arrived at yet so today I offer suggestions for consideration.

But, yes, I think that we need to start thinking this through, at the very least to eliminate the physical local use requirements that are incredibly anachronistic in the era of the Internet and e-commerce. Maybe we could agree on that while we talk through the rest of what might be beneficial.

PROF. BARTOW: Panelists?

MS. WONG: Again just an observation from the domain name side. I did a quick search while you were talking. The website www.supreme.com resolves to Perry Ellis, which, as far as I know, has no collaboration or relationship with the streetwear Supreme. However, the website www.supremestreetwear.com resolves to a German e-commerce site, and it is very difficult to tell whether the merchandise on that site is counterfeit or genuine. So there is a trademark and a branding problem here.

PROF. SCAFIDI: Supremestreetwear.com, I believe, was registered by International Brand Firm, the same company that is doing business as Supreme Italia. It also
Session 7A

has a German registration, so maybe that’s why there is a German website along with www.supremeitalia.it.

MS. PHILLIPS: This is probably more a matter of personal rather than professional interest. People who know me know that I’m an absolute shoe obsessive and the cupboards in my playroom are filled with shoes, not children’s toys.

PROF. SCAFIDI: My sister!

MS. PHILLIPS: Is the issue that you are talking about more a manifestation of how poorly intellectual property serves the fashion industry? It is a huge issue. If you are a brand, how do you go about protecting your work?

PROF. SCAFIDI: From your lips to the ears of intellectual property offices all around the world. My time is up, though.

PROF. BARTOW: Yes, it is. Thank you so much, Susan.

Next up we have Gareth Dickson.

MS. WONG: Maybe I can just add something while Gareth is getting ready. This is a lead-in for him. Trying to figure out who was behind supreme.com and supremestreetwear.com I did a WHOIS look-up search. I cannot figure out who the registrant is because all of that information has been redacted.

PROF. BARTOW: On that note, Mr. Dickson.

MR. DICKSON: Thank you.

I am going to spend a few minutes today looking at the EU General Data Protection Regulation (GDPR). We’ve heard about counterfeits, crises, clothing, and now we are going to hear about a bit of confusion.

The GDPR came into effect on May 25, 2018, shortly after the last Fordham Conference. We now have had an opportunity to look back at its impact with specific reference to the Uniform Domain-Name Dispute-Resolution Policy (UDRP), online trademark infringement, and trademark enforcement generally.

I have split the talk unto three sections. First, we will look at why the UDRP has been so successful in helping to tackle online trademark infringement. Second, we will look at the immediate impact as of today’s date of the GDPR on the UDRP. Third, look at what the longer-term impact of it might be — not just in online trademark enforcement, but on the resolution of online disputes surrounding IP more generally.

I think there are three issues that we can look at to understand the success of the UDRP.

The first, of course, is that it is a global remedy. Rights holders do not have to go to jurisdiction after jurisdiction to secure expensive and time-consuming injunctions. They can go to one service provider and be granted a reward that is enforceable immediately and takes effect worldwide.

For that service you are also looking at remarkable speed and cost savings when compared to injunctions because the UDRP is very narrowly focused; it is really only to be used for clear-cut cases of cybersquatting. If your evidence needs to be tested, if witnesses need to be cross-examined, if there is going to be a lot of discovery or disclosure, then the UDRP is not the appropriate forum for your dispute.

WIPO, as the principal provider of the UDRP, employs panels of experts who know all about trademarks and how the Internet works, so that the decisions that are being made are informed and they have legitimacy. That has built up a body of jurisprudence over the twenty years since we’ve had the UDRP that WIPO has consolidated into a series of overviews.

The most recent is Version 3, which was released a couple of years ago. That looks at all the key questions that are likely to arise in the online enforcement of trademarks via the UDRP and what the panelists’ consensus is on those issues. So you have a roadmap
when you go to prepare your complaint. That makes it easier to develop a template. It makes it easier to reuse your precedents. It also means that you can use automated processes in many instances to combine the likely arguments with the results of your trademark monitoring services and your watch services.

But we also know that the enforcement of IP has to be balanced against the protection of other fundamental rights, including privacy, freedom of speech, and data protection, and that is really where the GDPR comes into its own. It has pitted these rights against one another and brought this tension to the fore.

It does so in an environment where the essential participants — namely, the registrars who hold information about who has registered a domain name — do not want to participate. Their essential function is completed by the time a dispute arises. They have supplied somebody with a domain name and they have been paid for it; as far as they’re concerned, that is the end of the transaction.

IP owners ask the registrars to disclose information to them, but now, in the GDPR era, those registrars are at risk of significant fines if they unlawfully process that personal data. So what they do is they adopt the path of least resistance.

We have looked at this over the last number of years at Fordham and we have always been looking forward: what do we think the likely impact of the GDPR is going to be?

The most obvious impact was that the WHOIS, the database that identifies who is the owner of a domain name, was going to go dark, so the personally identifiable information that it supplied and published was going to be removed and redacted and could only be accessed if the registrar agreed to it.

That was an obvious prediction to make. But we also thought that this, in turn, was going to make it more difficult and more time-consuming and costly for rightsholders to enforce their rights. In turn, it would make it easier for bad actors to infringe and may in the end lead to a stronger focus on intermediary responsibilities.

WIPO has published some statistics about UDRP cases in 2018. If you look at the bars on the graph, you will see that in 2018 there was a significant increase in the number of cases that were brought before WIPO.

At the same time, there was a significant decrease in the number of domain names at issue in those cases because rightsholders are not able to consolidate complaints against multiple domain names registered by a single registrant in the GDPR era. So they are investing more for less return.

What is also clear from the statistics is the number of industries that are being targeted by cybersquatting has remained remarkably consistent over the last four years. If you try to identify and follow through the different industries, the top seven haven’t really changed in the last four years: it’s fashion; it’s biotech and pharma; banking and financial services; Internet and IT. That raises some real consumer protection issues. This is not really just an issue about branding; this is an issue about protecting consumers.

ICANN is struggling to find a consensus among various factions to identify a way forward. How are we going to grant access to the WHOIS information to those who have a need to see it? I think there is going to need to be some external force to burst the ICANN bubble, to put some pressure on those parties to come to an agreement themselves.

The National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce sent a letter to ICANN on April 4, 2019, a couple of weeks ago, that says: “without clear and meaningful progress on alternative solutions, calls for domestic legislation will only intensify and be considered.”
The United Kingdom is also looking at some measures to hold social media companies and their officers accountable. Again, it’s a slightly different process. What we can see is a patchwork of national regulation taking the place of the UDRP.

As we move forward it would be nice to think that the parties will sit down together and talk about online IP infringement. If they do, then perhaps we should learn some of the lessons from the UDRP and what makes it work so well and move it on from just the assessment of disputes involving trademarks and domain names and ask it to look at trademark and copyright issues on websites. It’s a good model that we could use.

In conclusion, the GDPR has been a bit of a boon for infringers, but a compromise needs to be made; otherwise we are going to end up with a patchwork of national regulations which benefits nobody but the infringers.

The IP community is very creative, and perhaps together we can identify a resolution.

Thank you.

PROF. BARTOW: Terrific. Great job.

MR. DICKSON: There is a lot of discussion about ICANN and its role within this confusion around the GDPR, but none of that should be understood to be a criticism of the endeavors that anybody at ICANN or within the community are doing to try to find a way forward. This is an incredibly difficult topic and it has really delayed progress in a number of other areas because it is so important. But everybody is working very hard to resolve it.

PROF. BARTOW: I think Mary Wong may have a comment.

MS. WONG: Thanks, Gareth. I think those of you who have come to Fordham for the past few years know that Gareth and I are often on the panel where GDPR has been discussed. This is a conversation that we continue to have.

I want to make a comment for those who haven’t been following this — and you probably don’t need to because it goes deep into the trenches. There are a few folks in the audience today who are very active participants in the ICANN community. Policies about domain name dispute resolution, and certainly policies about the WHOIS directory of registrant data, are made by stakeholders and as ICANN staff we facilitate that.

Those of you who were at the Sunrise Seminar this morning on ICANN and rights protection mechanisms probably thought that working group reviewing the UDRP and associated rights protection mechanisms for trademark owners was exciting. You haven’t heard about the one on GDPR and WHOIS.

Without going into detail, as Gareth has already mentioned, it is a very difficult topic. There is a lot of work to be done. I think even those of you who don’t deal in the domain name space but have had to deal with the effects of the GDPR, as well as other legislation coming up around the world that is either modeled on GDPR or very similar to it, are working with your clients and your colleagues on what is necessary to comply with the GDPR.

In the domain name space, as Gareth said, the reaction, which is probably understandable, among many of the registrars, who are the ones who hold the registrant data, has been to essentially redact that data; hence, my quip earlier.

There was a temporary fix, if you like, that ICANN put into place because there is no question that what used to be no longer is. This sounds like a line from Game of Thrones. I just hope it doesn’t end as bloodily.

In the past, as many folks in the room know, you could just look up a registrant’s name, maybe an email address, contact information, by doing a lookup of the domain name. As you just saw, I couldn’t do that for supreme.com because I don’t know who is behind that. By going to the website, I guess I can see it’s Perry Ellis and do a lookup. So there are ways you can find information, but it’s a lot harder now.
We have also heard from law enforcement that it is very, very difficult for them to do their jobs because this tool that used to be freely available now no longer is because of the GDPR.

There is a lot of ongoing policy work, but it will come as no surprise to this audience that it is difficult because of the multiple interests — Gareth described that in his earlier slide — and the work is proceeding in phases. We just completed Phase 1 in the record time for ICANN of one year. I think for some of the participants it probably took ten years of their lives and their time, or it feels like it.

I will end on one point and then pass it back to Ann and everybody else on the panel. One of the most contentious and difficult discussions has been around: What is a “lawful purpose,” what is a “legitimate interest,” in order for there to be a policy to allow third-party access to what is personal data?

We did not conclude that discussion in Phase 1. We are starting up Phase 2, so I suppose this time next year I will come back and report on how well we are doing.

PROF. BARTOW: I look forward to that.

Is there a question?

QUESTION [Mr. Sterpi]: Very briefly, I think the situation is that IP lawyers were turned into “Ghost Busters,” because now they are chasing ghosts. Now if you find an infringing website, you do not know who to attack, which is completely against any minimal level of reasonableness. Clearly, that must be changed.

Second, it is completely absurd that you can draw a right from your registration of a domain name, which is similar to a trademark right, but, on the other hand, you can remain incognito; so you can enforce your right against any third parties, but the third party cannot attack you because they do not know who you are, which is completely unfair.

Third, I think there was a complete paranoia about the application of GDPR and people completely misunderstood and confused personal data with other data. Data about corporations are, of course, not personal data. So the registrars scrapped everything, but 90 percent of the data that they scrapped were not correctly scrapped.

Finally, my proposal is that the balance should be, of course, pending on the legality side. Clearly, when someone is unreachable or incognito, there should be a kind of a UDRP proceeding to cancel the domain name registration. If you don’t want to be caught, probably you have something to hide; you better get your domain registration canceled.

MR. DICKSON: One of the key issues in the UDRP, and one of its successes, is the ability to consolidate complaints. I think the largest ever complaint was 3,000 domain names in a single complaint. You can imagine in this area if you can’t aggregate those domain names, you are going to have many multiples. It is still cheaper than getting an injunction.

PROF. BARTOW: Thank you very much.

Our final featured speaker is Richard Pfohl from Music Canada.

MR. PFOHL: Much has been made of the EU Copyright in the Digital Single Market Directive, particularly Article 17 (nee 13). As you know, its adoption by the European Council eleven days ago:

- Broke the Internet
- Is causing global civilization to descend into chaos

---

• And, as any Canadian will tell you, this was clearly heralded by the crashing out in the first round of the Stanley Cup playoffs in four straight games of the Tampa Bay Lightning.

Fortunately, we had a panel yesterday\(^\text{10}\) that talked about the Digital Single Market (DSM) Directive in a lot of detail, so I’m not going to depress you with the world descending into chaos right now. In fact, my point here, NHL evidence notwithstanding, is going to be exactly the opposite: The EU Directive is not an outlier. It is in fact not even ahead of the curve. It is part of a broad worldwide wave of statutory and case law developments that are adapting copyright enforcement tools to new digital challenges, just as the WIPO Treaties did twenty-two years ago. Call it WIPO 2.0 if you will.

Maria Martin-Prat, who will correct me if I misquote her, spoke yesterday about how we seem to be moving into a post-multilateral IP treaty world, and wondered whether we are moving toward convergence or managed diversity or even divergence.\(^\text{11}\)

I would argue that in the realm of online copyright enforcement, we at least seem to have best practices globally emerging, and they seem to be centered around a common theme, and that is platform accountability.

What are the challenges? I think you’re probably all well aware of these. I will just highlight the second two.

Whack-a-mole is actually being played on three different levels. It’s sort of like playing Star Trek Chess: There is constantly refreshing infringing content (the moment you take it down it goes back up again) and there is also jurisdiction and domain hopping.

We also have, as Justin Hughes told us yesterday, safe harbor laws that were premised on the concept of the Internet as “profoundly dumb.” Unfortunately, those safe harbor laws are sheltering companies that are not dumb; they’re quite smart. As an example, the one that EU Article 17 targeted, YouTube: 80 percent of the music that’s accessed on YouTube is either curated or recommended by YouTube. Query whether that’s really a “passive intermediary”?

How has the world been evolving? I will quickly take you through some key developments and recent responses.

Dynamic website blocking orders have been around for a few years. The difference is that we now have dynamic website blocking orders to deal with the domain name hoppers. In Singapore and Italy in the last year we had courts issuing dynamic orders. Contrast that with Greece, where a new authority that was created issued a website-blocking order, but they declined to make it dynamic: they said it was a bit too vague to do so. What happened as a result was the infringers went online, told their users precisely where to migrate, everyone migrated to those sites, and they are now infringing again. So I would predict that you may see Greece moving in the direction of Singapore and Italy in the next year.

We have globally reaching orders. I will just quickly mention two. The *Equustek* case\(^\text{12}\) in Canada was actually a trade secret case, but it applied to Google on a global basis. Similarly, in the *ZIRA* case\(^\text{13}\) in Israel: same actor, same effect — global.

\(^{10}\) See Session 3C: EU Copyright Reform, EMILY C. & JOHN E. HANSEN INTELL. PROP. INST. FORDHAM L. SCH. (2019).

\(^{11}\) See Session 1C: Government Leaders’ Perspectives on IP, EMILY C. & JOHN E. HANSEN INTELL. PROP. INST. FORDHAM L. SCH. (2019).


\(^{13}\) ZIRA (Copyright in the Internet) Inc. v. Anonymous, and others, [2015] Civil Case 37039-05-15 (Isr.).
We have notice and stay down. The DSM Directive requires that user-uploaded content (UUC) services use best efforts to make sure that material once taken down stays down. Interestingly enough, Italy did not approve the treaty, but nonetheless they actually went beyond that in two instances in the past year. They adopted new amendments to their AGCOM\textsuperscript{14} regulation that require stay down. They also have the Reti Televisive Italiane SpA v. Yahoo! Inc. case,\textsuperscript{15} which came out just last month, again requiring stay down.

Similarly, we have UUC services (or, as the European Union clumsily calls them, OCSSPs\textsuperscript{16}).

Of course we have the DSM Directive.

Again, the Italian Supreme Court went even further than that. They didn’t put in any conditions about best efforts; they simply said: 

If you are effectively operating a site that is hosting, then you’re going to be liable.

We also have liability for linking and merging.

Again, Italy seems to be a good actor. The Court of Rome, in a case involving Facebook, found liability for hosting links to unlicensed content.\textsuperscript{17}

Similarly, Israel enacted Copyright Act amendments this year that provide for primary (i.e., direct) liability for profit-motivated facilitation of access — or, if you will, linking.

A final example: search engines.

Our panelist Fiona Phillips can talk a bit more about the Australian statute, but in November 2018 website blocking requirements were extended to search engines.

Similarly, again, in the ZIRA case in Israel, the district court issued an ex parte global order effectively requiring a search engine to take actions to make sure that they did not link to infringing sites.

That was similar to what was provided for in Canada in the Equustek case, again a trade secret case, but nonetheless a global de-indexing order.

Previously search engines seemed to fly under the radar screen. We now realize that is actually the way that people get to infringing material.

One example of a copyright enforcement mechanism that dates back two decades, but has been invoked in the past year, is a U.S. provision to ensure that ISPs take appropriate actions to enforce against copyright infringement that they are notified of on their networks. In the United States ISP safe harbors enacted as part of the DMCA have always included copyright enforcement requirements that ISPs have to meet in order to qualify for the safe harbor protection. Specifically, they are required to have an effective repeat infringer policy in place.

In two recent cases, U.S. courts have found that ISPs that did not have an effective repeat infringer policy did not qualify for the ISP safe harbor. In 2018, the Fourth Circuit, in \textit{BMG v. Cox},\textsuperscript{18} and, similarly, in March 2019, the District Court for the Western District of Texas, in \textit{UMG Recordings v. Grande Communications Networks},\textsuperscript{19} refused to extend safe harbor protections to an ISP on these grounds. Compare Canada, where ISPs get a safe harbor without such a requirement.

In conclusion, I will leave it to you to decide one of two things:

\textsuperscript{14} Autorità per le Garanzie nelle Comunicazioni (AGCOM) is the Italian Communication Regulatory Authority.

\textsuperscript{15} Reti Televisive Italiane SpA v Yahoo! Inc., [2019] 7708/19 (It.).

\textsuperscript{16} Online Content Sharing Service Provider

\textsuperscript{17} Reti Televisive Italiane SpA v. Facebook Inc., [2019] 3512/2019 (It.).

\textsuperscript{18} 881 F.3d 293 (4th Cir. 2018).

• Either we are starting to sort this out through best practices globally; or
• The Broken Internet End Time is upon us.

PROF. BARTOW: Great job. Thanks.

Fiona, do you have a comment or a question?

MS. PHILLIPS: Essentially, I think what Richard described really very much reflects the situation in Australia. Courtesy of our free trade agreement with the United States, we have a version of DMCA Section 512\textsuperscript{20} with a couple of differences.

• We have no code of conduct underlying it, so there is no cooperation between rightsholders and service providers, which makes it largely ineffectual.

• Our definition of service provider is quite narrow. It was recently extended, but it does not include platforms like Google, Facebook, etc., despite their best efforts. So that doesn’t work.

The debate has shifted, and we now have had site blocking since 2015, which has been used very effectively. As Richard said, coming out of a review that was done last year, those provisions have now been amended so that it is now clear that the Federal Court has the power to make dynamic orders.

Justice Arnold spoke yesterday\textsuperscript{21} about the conditions for making site-blocking orders. For the “primary purpose” test in Australia the bar has been lowered. Also, now online search is included within the parameters of site blocking.

We have yet to launch the first case. The legislation only came into force at the beginning of this year. If Equustek is anything to go by, I think Google is unlikely to take it lying down. But it will be interesting to watch what happens.

The other interesting development in Australia is in terms of the shift to focusing on the role of digital platforms. There was a discussion very early this morning in Sunrise Seminar II on streaming. Our competition regulator is currently conducting an inquiry into the role of digital platforms, looking at the competition issues but also looking at the copyright issues.

Despite what Bill Patry said yesterday about Google not making money off content,\textsuperscript{22} our competition regulator’s preliminary report has suggested otherwise. So we now have the competition regulator suggesting that it should play a role in the safe-harbor environment.

As I mentioned in the early panel this morning,\textsuperscript{23} I think that in our part of the world, the live streaming of the terrorist incident in Christchurch has really focused people’s attention on how you regulate digital platforms.

That very much is where the focus is in Australia at the moment.

PROF. BARTOW: Mary?

MS. WONG: I have a question for Richard, and maybe some of our other speakers can chime in.

Paul mentioned education in one of his comments earlier. ICANN is often asked to do training. I do not do that because I am not technical, so my technical colleagues do that. Sometimes we cooperate with law enforcement. We do workshops.

\textsuperscript{20} 17 U.S.C. § 512.


\textsuperscript{22} See Session 3B: DMCA: 20 Years Later, EMILY C. & JOHN E. HANSEN INTELL. PROP. INST. FORDHAM L. SCH. (2019).

One of the things I’m told by my technical colleagues that they hear when they are on the road is that in terms of drafting the orders, whether it’s an order for a domain seizure or any kind of other judicial order, some of it is not done very well, some of it is certainly not done very accurately, and that makes the job hard for a judge who may or may not be educated in the niceties of how the domain name system works.

You have the same sorts of issues surfacing with legislators, for example, in terms of legislation that is either very remedy-specific or that targets a specific type of technology.

I wonder if anybody has any thoughts or observations based on your in-the-field experience.

MR. DOWD: I do from a local perspective. Our initial applications to judges are getting longer and more complicated. Really the big job is to break the technology down to about a sixth-grade level; and if it’s not that clear and it’s not that simple, you are not going to get the relief you need.

The judges are nervous about technology they don’t understand. They don’t want to be issuing injunctions that are not clearly warranted. What that means for the client is a big up-front investment. Just as they say first impressions are most of what people are left with, when you go into court your first impression is likely to remain for a really long time. That has been a frustration, I think, for many rights owners who go to a court to try to get relief.

MR. PFOHL: The one thing I would add is those are hotly litigated issues, I think, like the breadth of an order. If you get it wrong, the service provider or intermediary to whom it is going to apply is certainly going to contest it and is going to say, “No, that’s inapt for the following reasons.” I do think that gets sorted out.

But you are right, Raymond, that it requires some up-front investment in terms of making the case and being precise in terms of what you are asking for.

MR. DOWD: And the judges are looking to the lawyers actually to help them not do something that’s crazy, right? You usually go in and say, “We want to ask for everything we can get.” Dialing it down and showing how you are being reasonable and that what you are asking for is fair is advocacy that really has to happen right at the outset.

MR. MAIER: We in the EUIPO try to help judges understand how it functions. We had another training session for forty judges last week where we explained how the Internet functions. They are often more aware of what they need to know than we may think. This being said, further awareness raising and explaining is important, and we will continue to offer these sessions.

PROF. BARTOW: Thank you very much for a great session.