The John Marshall Journal of Information Technology & Privacy Law

Volume 29
Issue 3 *Journal of Computer & Information Law - Spring/Summer 2012*

Article 5

Summer 2012

Session IV: Technology and The Future of Privacy, 29 J. Marshall J. Computer & Info. L. 379 (2012)

David E. Sorkin
John Marshall Law School, 7sorkin@jmls.edu

Ann Bartow

Robert S. Gurwin

Doris E. Long
John Marshall Law School, 7long@jmls.edu

SESSION IV: TECHNOLOGY AND THE FUTURE OF PRIVACY

Moderator:

David E. Sorkin
Associate Professor, The John Marshall Law School

Panelists:

Anne Bartow
Professor, Pace University School of Law

Robert S. Gurwin
Assistant General Counsel, AOL Inc.

Doris Estelle Long
Professor, The John Marshall Law School

PROFESSOR SORKIN: We now move to Session IV, Technology and the Future of Privacy. As Amitai Etzioni and others have noted, technological advances are constantly changing our expectation of privacy. In the *United States v. Jones*, which held that attaching a GPS device to a private vehicle was an unconstitutional search, Justice Scalia and a majority of the Court emphasized property rights as a basis for Fourth Amendment protection rather than relying solely on the reasonable expectation of privacy. Elsewhere Justice Scalia has urged us to be practical about Internet tracking and other minor incursions and focus on protecting more sensitive information.

Over a decade ago we were told that privacy is essentially dead, an exaggeration to be sure, but a warning that technology will continue to threaten our privacy.

But technology can also enhance privacy. Encryption, technological intermediaries and other privacy-enhancing technologies can help us control the information that can be collected and used about us. But privacy still seems to be the long shot in this race.

Our panelists in this session will look at some aspects of technology and privacy and hopefully give us some insights on what the future holds. Our first panelist is Ann Bartow, a professor at Pace Law School. She previously taught at the University of South Carolina School of Law and served as a Fulbright Scholar at Tongji University in Shanghai, China, last year. She teaches and writes in the fields of intellectual property, privacy and technology law, and feminist legal theory. Professor Bartow.

(Applause.)

PROFESSOR BARTOW: Thank you. It's a great job to be here for a lot of reasons, and I especially love seeing David and Doris and Leslie and my John Marshall friends. This is a fabulous law school. I've been coming here for many years for different reasons and it's always a pleasure, so thank you.

What I'm going to talk to you today about is what I think is one of the worst pieces of legislation for women in the last fifteen years. What I'm talking about is Section 230 of the Communications Decency Act. This was passed in 1996 as part of an act, most of which was found unconstitutional, but Section 230 remains. And Section 230 of the Communications Decency Act immunizes online service providers, quite extensively, for any sorts of liability related to what other people do with the network or post on the network.

The Act, that part of the Act, had a name when it was going through Congress. Anyone remember what that was? Nobody?

It was called the Good Samaritan Act. Please keep that in mind, the Good Samaritan Act that I'm actually opposing, and I'm in very much opposition to the current formulation of the Good Samaritan Act because I'm evil. Let me explain why.

So consider this hypothetical. This happens, say, a law school student—law school can be an emotional crucible for a lot of people, a lot of law students—let's say here at John Marshall, not in John Marshall itself but the coffee shops around here – and there's DePaul, there's a lot of studenty kind of coffee shops—and the restaurants and coffee shops around here—one morning you are a law student at John Marshall and you walk into your local coffee shop and you go to the bathroom and you see in the bathroom there are nude photos of you, giving your name and your phone number and saying that you like rough sex and should be approached, that you would enjoy that, you would protest, but that, in fact, you would enjoy rough sex from strangers. And you're just in shock. You're just in shock. You can't even believe this. You don't know when this picture was taken. It's got your name, it's got your contact information, your e-mail address.

Immediately you rip down all the posters and you walk and you find somebody who works at the coffee shop and "What is the meaning of this? How could this happen? Who did this? What is this all about?" And they say "Hmm, we don't know. We have no idea."

And you go to class and you're pretty shaken up. And then on your way home later you stop by the coffee shop and you go in the bathroom again expecting the worst and, in fact, you see the worst. There are copies of the poster again. And you rip them down again and you're beside yourself and you walk into the coffee shop and some strange men start heckling you, touching you, demanding sex with you, and you realize those posters were also in the men's room.

And again, you go to the people who run the coffee shop and you say "This is intolerable. I'm calling the police. I'm suing you. I mean, this can't be, you know, you have to—what is this? How can you allow this?" They say "Not our problem. Not our problem. We're not putting them up, someone else is putting them up."

You say "Well, can you at least, you know, look at your security footage or have somebody monitor the bathrooms and figure out who's doing this?" They say "No." And you consult a lawyer and you say "Surely I have legal action here," and they say "No."

And you call the police, because people are literally assaulting you, and they say "When someone assaults you, we will arrest that person. But we will do nothing about those posters that keep reappearing in the bathroom."

Basically that's the situation the Communications Decency Act formulates online. In real space it might be different. But if a shop refuses to take down or help you figure out who's doing it, do they have an obligation to help in real space? Maybe, maybe not. But online they do not. If you call the police, the police may help you, but probably they won't. I'm going to talk about that more in a minute.

Basically, generally, even people I've represented that have had this happen to them online, the police generally give you a line like "Be more aware of your surroundings." Wow, that's really helpful, right? It's not like women spend every single day of our lives understanding that we might be victims of male violence every day, right?

After 9/11, immediately after 9/11, one of the interesting conversations I had with a bunch of different men was, you know, "We don't know how to live anymore, we don't know how to behave, anything unexpected could happen." I said, "Welcome to the world of being a woman." Right? I mean that's how women live. Don't walk in the dark. Don't walk alone. Right? If you get raped, it might be your fault because you worked late and you didn't get someone to escort you to your car.

This is not new to us. But what's new is the Internet. The case I want to frame my discussion for you is a case called *Barnes v. Yahoo*. *Barnes v. Yahoo* is a bit unusual, because unlike most cases that are brought with the online version of the hypothetical I just told you about, the coffee shop, *Barnes* was the rare plaintiff who got traction. I'm going to tell you why.

Most of the people who wind up in that coffee shop hypothetical, which basically online means dating sites, blogs, online sites, women, a lot of women, are having nude pictures posted of them, their contact information posted, and then men showing up at their homes and showing up at their place of work demanding rough anonymous sex because that's what it says they want, believing this, and then women calling the police, contacting the ISP.

The police maybe, in some cases there were men convicted of rape for this, because they actually were raping these women saying "But she wanted it, she said online that she was going to pretend she doesn't want it and she wants it." Men willing to believe this, taking the action, would be arrested for their consequences.

But as far as the online postings, the ISP is unwilling to do anything about the postings, right, or repostings after these things happen.

The unique thing about *Barnes* was that Cecilia Barnes, when this started happening to her, she understood that she probably didn't have a legal remedy, she understood the police were not going to help her, but she was unusually feisty and had an unusual level of resources, she leveraged the media. She actually leveraged the media and got a news

show that was going to broadcast her plight when people were showing up at her workplace demanding rough sex. And she got a news show to do a segment about this.

As part of this segment, they called Yahoo to get Yahoo's perspective. And Yahoo freaked out and said, "Oh, no, no. No story here. We're going to take the postings down." And they told Cecilia and they told the newspeople, "We're going to take the postings down." But they didn't.

They represented they would take them down to quash the news show, nothing to see here, but they left the postings up and the harassment continued. Unlike a huge string of cases that have been brought that were dismissed on summary judgment, basis 230—and that also happened to her, by the way, in the district court when she got to the Ninth Circuit—because I told you she was unusually feisty, had an unusual amount of resources—when she lost in the district court on summary judgment 230 immunity, she appealed to the Ninth Circuit who said, "Okay, maybe you have an argument for promissory estoppel, maybe you have an argument for detrimental reliance. We will at least give you a chance to convince a court of that and we'll overturn the summary judgment."

That's where it stands. It's not clear at all if she would win on the merits, or will win on the merits, but that's where it stands right now. She had to go through all that just to get into court to make a claim on the merits.

Where did this all come from? Who is the very first 230 victim? That actually was a man. Some of you, at least, will be familiar with his name. His name is Ken Zaren. This was the first case that established the breathtaking breadth of 230 immunity.

And recently, about a year ago, at Santa Clara, he, for the very first time in about almost fifteen years, broke his silence about what happened to him, appeared at a conference organized by Eric Goldman, you can see his statement online, talking about what happened to him and about his feelings, as you might imagine what they are, about 230. Ken Zeran was a person who, after the Oklahoma city bombings, somebody went on AOL and posted all these things about Ken Zeran's selling naughty Oklahoma Murrah Building bombing tees, that were the most disgusting, tasteless mocking of the victims of the bombing you could imagine, posted his name and his contact information.

So what happened? People legitimately thought, because it was on AOL, it was on the Internet, it must be true, mocking the victims and trying to make money from mocking the victims by selling these tasteless T-shirts. And they started calling him and yelling at him, lambasting and, of course, threatening him with death. It reached a point where he was getting one death threat every two minutes.

This was serious enough and deemed serious enough and he was well connected enough that the FBI got involved. But meanwhile, while the FBI was getting involved, a local radio station picked up the story, what a scumbag Ken Zeran was, and ramped it up to a new level with all his listeners, "Call Ken Zeran. Tell him what you think of his disgusting T-shirts."

Finally, finally, a newspaper picked up this story, reported that Ken was being victimized, the radio station realized it was a hoax, apologized to Ken and started telling people, "Stop calling him. This is a hoax."

AOL, unlike the newspaper, unlike the radio station, did nothing. No removal of the postings, no retraction of the postings, no help in identifying this culprit who has never been identified to this day, no screening of future postings. They were allowed to just let the abuse continue, continue, continue.

230. He went to court, he sued, and the court said under 230 they do not have to help, they do not have to remove, they do not have to retract, they don't have to identify the culprit, and they don't have to do any screening. Do you remember what that Act was called?

The Good Samaritan Act. Why is this called the Good Samaritan Act? Well, I guess, so that AOL is not afraid to help. Because if they get it wrong, they can't be sued. But the reality is they're not just afraid not to help; not helping is where the money is. When people log in to excoriate Ken Zeran, AOL gets eyeballs, AOL gets browser clicks, AOL gets advertising money. That's where all the money is.

Now, I spent last year in China, which has a very different set of privacy laws and privacy norms, which I'm actually studying and writing about at this moment. In China, there was—well, one of the things you have to understand about China, if you haven't spent a lot of time there, is there is very little freedom of the press. The press is controlled by the Communist Party. All right. There are some social networking things that are happening that are interesting, but, by and large, the press is controlled by the Communist Party. The Communist Party publicizes certain things as a certain social control mechanism.

There was a judge known as the Nanjing Judge who decided a case. There was a case where someone was injured, some stranger stopped to help him. And then, when they were trying to figure out who the wrongdoer was who had injured the person who was injured in the first place, the judge said, "Well, it must be the Good Samaritan." Why? Why is it the Good Samaritan? He said, "I'm completely innocent, I just stopped to help."

And the judge said, "No one would just stop to help. You must have injured him in the first place and were trying to help him to avoid liabil-

ity. But we're on to you, because no one would just randomly stop and help a stranger."

This was widely, widely publicized throughout China. It had two effects. One is that people who were reluctant to be Good Samaritans were even more reluctant to be Good Samaritans in China, which was maybe an unintended consequence, but certainly a strong consequence. The other, though, is it was a story for Chinese citizens to tell themselves about why they didn't stop and help. It's okay not to stop and help. The Nanjing Judge has given you a reason, a reasonable reason to feel okay about not stopping to help strangers.

And again, the press is all controlled, so these stories that appear, this is some sort of policy. I couldn't begin to tell you who thought of this and what the end game is, but I watched this play out the year that I was there.

The Internet can be a tool of abuse. And let me tell you, I do not hate anonymity or anonymous speech and I don't hate the First Amendment. What I do hate is a law that facilitates the monetization of Internet harassment. I've made this case in a law review article that was published in 2009 in the Harvard Journal of Law and Gender. If anyone is interested afterwards, I can give you the citation.

But the bottom line is ISPs won't help you, the police often won't help you either. Once in a while the police will help, but it usually takes extreme violence over a period of years before the police will take action and try to help you track down the culprit.

If you can afford it, search engine optimizers and the like may also help. But then, again, maybe they won't. Because even if you're willing to pay them money, if the harasser is motivated, or an SEO client, not even money would help if someone else was leveraging an SEO against you and had better resources or more resources or was just more persistent.

Barnes was unique in that she may get a hearing. Probably there's been a settlement, or will be a settlement. Why? Because Yahoo didn't want the publicity in the first place, remember. They're probably not going to want any more publicity. And ISPs don't want publicity of cases like this because it might lead to legal reform that they don't want.

And you know who helps them a lot, the libertarian organizations helped them a lot, the ACLU, EFF, even Epic. Marc Rotenberg was here yesterday, that's something he and I have a lot of disagreement about. Why?

Because they're afraid that all 230 would be upended, right, they don't want 230 removed. And neither do I. But there can be a middle ground. I really think that legislatively we can just put some limits, just ask the ISPs to put a little bit of limitation, a little bit of responsibility in

terms of helping find the culprit, in terms of maybe after, someone who is getting like people showing up at their house threatening them with violence, maybe a little bit of help in terms of taking things down or getting the message out there that this is unsolicited and false representation.

One of the effects of the Barnes' case, I mean she got incredible pushback, terrible pushback, I told you she was feisty, she has to be, from all these libertarian organizations and all their resources, that she was excoriated in the press. She, she was excoriated in the press, because some of these organizations said, "Now, no one, like Yahoo, now that Yahoo has been punished for offering to help and not following through, no one will offer to help and not follow through." And that's a bad thing apparently, right?

My question is: Why is this Barnes' problem? Barnes is suffering. Barnes is looking for help. Is it her responsibility to create a climate where ISPs might voluntarily help someone in the future? Possibly. Some fictional person in the future, even though it's against their economic self-interest. I don't know.

What I do know is that a lot of people who identify as feminists view this 230 absolutism line, and I just don't understand it. Victims of harassment in cyberspace are often victims of harassment in real space, real rape, real attack, assault and intimidation. They are often told by the popular press and by some of these libertarian organizations that they must have done something to deserve it. Why were you naked? Why were you naked with your boyfriend? Why did you let your boyfriend take a naked picture? You slut. Right? That this is a problem.

In real space, most feminists have rejected this argument. But in cyberspace they've been largely coopted by civil libertarian organizations when the same dynamic appears in cyberspace. What we need is legal reform. If we don't have legal reform of 230, women in cyberspace are left with what they have in real space. What is that? The police. Sometimes the police will help you and sometimes they won't.

When the police do help you, it's usually not the most cost-effective thing. All right? There's one case where a woman in New Orleans got help. The police were on the case. They had to drive to Maine to find the guy. They spent months and tens of thousands of dollars to help her, because she was such an extreme victim and an extreme factual—it was like Barnes times a thousand. It took three years before the police would take her seriously, okay, and help her. And they finally did help her, but it cost a lot of money to help one person, not really cost-effective.

And what else happens with the police? Now, I'm not down on the police. But the criminal people in the audience, people who study criminal law, know that when the police get involved you have a market basket of things that happen, not always good. We know that there's

evidence that police may act in a racist way, right, that people of color may be prosecuted more, or more harshly, for the same crimes. And we know there's a market basket of difficulties definitely in terms of when police refuse to act.

I want to conclude by talking very briefly about a couple of things. The first one or two is Kate Middleton's breasts. Is everyone aware of the publicity about Kate Middleton's breasts? Okay. Kate's just one signifier of something called creep show photography and revenge porn. Kate Middleton did everything she could to have some privacy with her husband. She took her top off. And now the pushback is, Well, why did she do that? We might as well ask, Why did she have breasts? Because women seem to have this obligation to be sexually available all the time, not just when we want to be. And Internet targeting of Kate's breasts is just one more example of that fact, that you have no autonomy, that you have no real privacy rights.

Another example is a woman named Nadya Suleman. Do you remember her? There were people who called her octomom. She was in desperate financial straits. Pornographers bought her house because she was defaulting on her mortgage and threatened to evict her if she did not agree to perform in pornography and strip clubs. And eventually she broke down and she felt like she had to do that. When you talk about this—and she openly said, "I did not want to do this. I was forced by my economic constraints. They bought my mortgage and were threatening to evict me"—people criticize me and say "But she's showing agency. She wants to be sexual. How dare you sledgehammer her for using her sexuality."

And I have another question for you. I don't know why that happens, and it's not really a lot of fun, but I also want to know why do so many people want to see Kate Middleton's breasts or Nadya Suleman naked? There are a lot of naked people on the Internet, there are a lot of breasts on the Internet. There is something about slut-shaming Nadya Suleman or slut-shaming Kate Middleton that's especially provocative and attractive to a certain kind of audience.

The problem—this happens in real space, this is nothing new, this predated the Internet – the problem is the Internet takes this dynamic and brings it to every woman, every single woman—and men, right, Ken Zeran was a man—but to women especially. And the numbers bear this out, that this happens to women in disproportionate numbers and we are disproportionately victimized by Section 230. Thank you.

(Applause.)

PROFESSOR SORKIN: Thank you, Ann.

Our next panelist is Robert Gurwin, Assistant General Counsel at AOL, Inc., in Dulles, Virginia. In his work, Bob addresses a wide variety of issues including intellectual property, licensing, privacy, advertising and many others. He also serves as an adjunct professor for the Center for Information Technology and Privacy Law at John Marshall and is a graduate of John Marshall's LLM program in information technology and privacy law. Bob.

(Applause.)

MR. GURWIN: Thank you, David. It is always a real privilege to come back to John Marshall and also to be invited to come back and be part of the fantastic programming that goes on at this law school. I cannot begin to tell you how much the LLM program here at John Marshall changed my life and my professional career.

Before becoming an information technology and privacy professional, I was a general practitioner for ten years and came into this program at the end of 1999. It was very cutting edge. It was the only program that was doing what it does at the time and continues to do it better than anyone else.

(Applause.)

Much has changed since I was an LLM student here, and I'm not just talking about the beautiful enhancements to the building downstairs and the new State Street entrance or this magnificent courtroom. When I was here, you have to put it in perspective, that the commercial Internet, as we know it, had only existed for about seven years. Mosaic, the first commercial web browser, launched January 23, 1993. So it was in its infancy.

The first Blackberry devices came out in 1999. And those initial devices weren't even Web-enabled devices, they were simply using Blackberry servers to transmit text data back and forth to deliver what was essentially business and corporate e-mail. And of course, until the iPhones went on sale in June of 2007, changing the mobile space, this has all evolved really, really quickly.

So what I'm going to talk about is a landscape that has changed dramatically in such a very short period of time, but it's something that we deal with at AOL every day. It's one of the exciting things that I get to deal with. In my current role I am actually the legal lead assigned to the AOL consumer mail product, the AOL mobile team, and our AOL paid services teams. So I am there, essentially, mini GC, I am their teaming attorney, and I work with them on their product pipeline. I work with them on roadmap. And as they're developing initiatives and working on

things, it's my job to make sure that we're flagging and doing things that are going to offer the best possible experience for our customers. And staying on top of privacy is really important, which is why AOL also employs a team of dedicated privacy professionals who I work with on a daily basis in doing this stuff. So here is a quick shot of the landscape.

And this is just a handful of the many things that are happening here. Consumers have migrated. Whereas, you know, ten-fifteen years ago, people were tied to a desktop, that isn't the case anymore. And more and more consumers' touch points with the Internet are with mobile devices, whether it be a laptop, a netbook, a tablet or even a smartphone.

So the amount of versatility and the way people are using their devices and interacting has changed. And at the same time, social media has increased the amount of information that's being shared, as was noted by several of the previous speakers this morning.

So we battle with the big question of industry self-regulation as opposed to legislation on this. And again, the previous panel addressed both sides of the coin on that and there are things to be said. It's very true that with industry self-regulation there is seemingly an inherent conflict between doing right by consumers and doing things that, you know, we should be doing, taking our medicine, as President Obama says, eating our peas, and the idea that some of these things may not be in the financial self-interest of companies who rely on monetization from Internet advertising or mobile Web advertising. And then on the flip side, legislation is always tricky because you're trusting legislators to get it right, and frequently you have people who are responding to public concerns and aren't necessarily equipped with the right background either in technology or in privacy to really understand the heart of it, and it's just as easy for them to get it very wrong. And bad legislation is worse than no legislation.

So let's talk about some of the things that we deal with and that impact us from an Internet media company like AOL and certainly certain other companies that are similarly situated. Professor Swire talked about Do Not Track. I'm going to touch on it briefly here, again because my time is limited. But again, Do Not Track is something that's been kicked around and worked on in an attempt to allow consumers the ability to choose whether or not the devices that they are using to surf the Web will be able to provide third parties with data about where they visit and things that are of interest to them.

The slide that I'm showing here shows the Mozilla Firefox browser, which actually had this functionality baked into it for quite some time. The interesting thing about it is that Do Not Track by itself is not a content blocker and it doesn't mechanically impede cookies. It simply passes certain information to the source that is serving the content, tell-

ing them of the end user's preferences. And also, you know, in theory, if the website that the person is visiting participates, will allow them to manage in accordance with his preferences.

So this isn't a new idea. Again, consumers have been concerned about privacy, Web users and users of mobile devices have gotten more sophisticated. And while the average user doesn't necessarily understand all of the things that are going on behind the scenes, all they see is what's on their screen, their expectation has changed.

And more and more there is a consumer expectation that, or at least an understanding, that their devices are capable of recording things, of tracking things, and it becomes very apparent to users when they're interacting with the website and all of a sudden they start seeing advertising for some other site that they had visited maybe yesterday or an hour ago.

Mozilla, which is the organization that produces and ships Firefox, has included it, but again, this Do Not Tracking has largely been ignored. The only two companies that recognize that Do Not Track preference currently are Yahoo and Twitter. In May of this year Microsoft announced that when it ships IE10, when it releases Windows 8, that it will effectively be turning that on by default, which has raised a lot of concerns within the Internet advertising industry.

In May of this year, the UK took a very drastic step in their directive that requires websites to give users very, very blatant notice if their site collects cookies. We went through an exercise, as did all of our brethren that provide Web services in the UK, to make sure that we're in compliance. And the worldwide Web consortium, which is the official standards lobby, has this technical working group to try to work on this. But it's not an ideal solution, it's far from perfect, but it's just one of the many things that are going on in this space.

Again, it's voluntary. There's no requirement to participate. And again, there's the question of risks associated with it. So it will be interesting to see where Do Not Track legislation goes and if it takes this a step further and actually turns it into a binding and a meaningful requirement, or whether the industry in the meantime will step up and do things on its own initiative that satisfy the consumer public's concerns and desires to have more control about information that's collected about them.

The states' AGs and the FTC are getting much more aggressive at dealing with privacy issues. California took a very bold step in February of this year and entered into essentially a consent decree with six major providers of mobile platforms concerning notice and consent that requires these companies to deliver, that before the app is actually downloaded and installed they have to display the privacy policy.

The three screen shots that are here just show instances where Apple has required that mobile apps are giving notice and consent when certain third-party apps are accessing contacts, the camera, the geolocator on the device. These are all really positive steps towards it being very clear to the user: This app is going to access this information or do this functionality. So that there's no question later, yes, you agreed to, this is certainly within the expectation of what you wanted this app to do.

In California, again, Amazon, Apple, Google, HP, Microsoft and RIM all entered into this agreement. Big step forward because, again, it does require that the privacy policy be displayed before there is an opportunity to download and install. It's still incumbent upon end users to take the step of actually reading it. And as you know, it's a catch-22. My esteemed colleague, Mr. Francois, pointed out, if you bombard people with too much, they're not going to read it. So it's really important to keep it simple, tell them what they really need to know, because otherwise they're not going to pay any attention to it. If they see that popup screen, "Facebook wants to access the contacts in your phone," I think everybody understands what this means. Whereas if they get presented with a privacy policy where they have to sit there and scroll through ten screens of information, they're going to get lost, they're not going to read it, and it's not meaningful, it's not really a meaningful consent.

The FTC just last week published a guide to help mobile app developers observe truth in advertising in privacy principles. And these bullet points are all included in the booklet. It's a really, really good roadmap. And it's the type of information that's helpful for someone in a role like I have, because it's concise, it's to the point and it's clear and this is the kind of thing that I can share with my Web and my mobile app developers and go through it with them so that they understand when they're building things, these are the kinds of things we, as a company, need to be conscious of, telling our customers what the app can do, what it accesses, what functionality, how to turn certain features on or off. Make those things easy to find. And then when we are relying on our privacy policy, making sure that we keep those promises. Making sure that if we're marketing anything to children under the age of thirteen that we're complying with the COPPA requirements, only collecting data that we absolutely need and nothing more. If we don't need it, there is no reason we should be collecting it. Keeping sensitive information only with consent and making sure that we're doing everything we need to be doing to keep it secure.

These are a few resources. And again, my understanding is these slides will be available to you, but there are some really good basic resources. The first one is a link to the privacy guide that the FTC just put out, as well as a link to their information on children's privacy, and then

the California Office of Privacy Protection has a very robust and comprehensive site of laws, regulations, and other information not unique to California. There's California-specific but then there's also national and more widespread things there that are very, very helpful.

In my day-to-day, the best thing that I can do when I'm working with my teams is to make sure that when they're building new experiences that they just have these things in the back of their head, that it's not some foreign concept that, hey, if we're going to take a twenty second video of somebody as part of an interactive game, we need to make sure they understand what's going to happen with that video and where it can be shared and where it will end up and give them the ability to opt out of that if they don't want to share it with other people other than the person they're playing with. So that's the global framework. We're talking about something that's very, very significant.

This is this morning's Wall Street Journal, and there is an article in the Business Marketplace page talking about a U.S. ad spent an estimated, for 2012, in just mobile advertising, $166 billion. So the information that is gathered and collected from mobile devices, it's a lot of money and it's very significant. So all the more reason why we need to make sure that we're being conscious of these things and building experiences that will enhance consumer trust and want them to choose our experience over somebody else's. Thank you.

(Applause.)

PROFESSOR SORKIN: I think I should explain for some of the younger members of our audience, the high-tech device that Bob is referring to in his hand is called a newspaper. And Bob, if you want to say the name of the app that you were alluding to there, please feel free.

MR. GURWIN: Oh, wow.

PROFESSOR SORKIN: He said he wasn't going to plug the latest app.

MR. GURWIN: I wasn't going to plug our new app, but our mobile team launched a really, really fun new game for iPhone yesterday called Clucks. And it's a social media version of, basically, charades, where you record a twenty second video to try to get your friend to guess a word, but you can't say the word that they're trying to guess. And it exchanges the videos back and forth and it's actually quite fun.

PROFESSOR SORKIN: And I'm sure there were no privacy implications there.

MR. GURWIN: Absolutely none.

PROFESSOR SORKIN: All right. Well, our final panelist, last and certainly not least, you know, I saved the fun panel for myself, our final panelist is Doris Long, another colleague of mine here at The John Marshall Law School and chair of the law school's intellectual property, information technology and privacy group. Doris specializes in international intellectual property law. She's taught in nine countries including China where she served as a Fulbright scholar at Jiao Tung University in Shanghai. Please welcome Professor Doris Long.

(Applause.)

PROFESSOR LONG: Thank you. I have to confess when I started teaching at John Marshall back in 1994, I had said, "I teach intellectual property, it's over here; you guys deal with privacy, it's over there." No problem.

Well, given that already the Internet was becoming an area of E-commerce, it is not only not this far apart, sometimes it's like this (indicating). And sometimes it's actually colliding with each other, because we have two separate laws with two separate policies that don't always combine well.

To make that worse, because the Internet is global, you also have to worry about privacy and copyright from other countries as well. And what I wanted to focus on is basically the disparate treatment that we appear to have when copyright and privacy collide in the digital environment, particularly in connection with enforcement of copyright. And I wanted to focus primarily on the United States and the EU, because they seem to be at different loggerheads when it comes to both views of copyright and when it comes both to views of privacy as well.

And in order to make some sense out of this, I had the opportunity in June, I was at a conference in Hawaii, and I got to see the transit of Venus. The transit of Venus across the sun is really interesting for a couple of reasons. First of all, it happens every 100 years, and then there's a twelve and an eight year interval, and then there's another 100 year gap. So it gives you a chance to figure out back in the eighteenth century how can we measure the distance of Venus from the sun. And in order to do that, they sent explorers out in various places, including Captain Cook who was on Tahiti, taking measurements to try and figure out how far Venus was actually from the sun.

One of the problems they didn't completely count on was the difference of the parallax view. This is not a parallax view photo, but it sort of demonstrates what you see depends on where you sit and what you're looking for. As you look at that picture, it's either a saxophone player or

a woman's face. And to a certain extent the privacy and copyright intersections depend on where you sit. And what I want to do is take the parallax view and try and come to a measured distance, because I think in the limited area of enforcement of intellectual property rights on the Internet we may not be as far apart as we appear to be in other areas. And in the interest of time, I'm going to do a lot of summarization. I've got a longer PowerPoint that's going to be made available, it has a lot of quotes and case cites, but I want to sort of bring things together and sort of take you through the measures of, first of all, where we are, but the points are. Obviously, when you talk about copyright and privacy and public policy, I think we're on the righthand side of the slide right now. I think it's all wheeling around each other and trying to take the measure of each other, sometimes unsuccessfully. One of the difficulties is copyright has admittedly had an ugly birth, okay, censorship, but it has been about communication and regulation of communication. Privacy had a very limited role in the early days when it came to copyright. Privacy was more or less: I don't want people to know who I am, either because I want to avoid censorship or I want to avoid the embarrassment of being engaged in something that women aren't supposed to do. So that you have a lot of anonymous writing by women then.

When you talk about the conundrum itself, it is this privacy intersection. And what I want to do is focus in on this definition of privacy. There are a lot of different ways to define privacy. For my purposes I am really looking at two different types of privacy that are combined in this question of the protection of copyright.

The first is going to be anonymous speech and anonymous acts. What's interesting about the Internet is, as opposed to shield my identity for my writings or my posters, it has become shield my identity for my acts as well. I'm not saying they don't qualify necessarily as speech, but it's a much broader demand that's put on privacy in connection with copyright than you had before. The other issues that you have, where the real challenge seems to be coming in, is the identification of personal data—name, rank, serial number—and anything else that will help me determine who you are and who is speaking.

And I think when you take that particular ontology and you look at it, that's where you start to see, at the outer edges, the true differences. Because at least in connection with privacy on the Internet in connection with posting and activities, one of the alleged distinctions is you have the money and commoditization on the right. And any time you talk about privacy and you talk to people from Europe about privacy, they are appalled at what we allow people to do. They are appalled that companies are allowed to gather information, they're allowed to sell it, they're allowed to monetize it in various and sundry different ways.

I posted, and I don't have time to play the link, but the European Privacy Commission actually posted a video on what online activity means to your privacy and, cut to the chase, the minute you go online they are concerned that you are in essence walking around naked. You have lost all of your clothes, because everybody can find out everything you have to do. Consequently we need stronger regulations. So you start with almost polar opposites.

If you move down through the thumbnail sketch of the EU and the U.S., you'll see that a lot of EU privacy deals with a lot of directives that are actually privacy directives, that deal with protection of the right of privacy, that deal with the protection of transfer of data, that deal with the fundamental right of consent and rectification of your data and your personal information, as opposed to in the environment that I'm talking about, which is the collision between copyright enforcement and privacy rights, you end up with a couple of statutes and a lot of it is push the button and simply say that you agree or don't. Come on the service, or opt out after a very complicated process. It's a very different approach to this area.

And when you look at the more specific areas where there is a conflict between the two, end-user identity disclosure, the need for ISPs to monitor to discover infringing conduct and remove it or avoid access to such infringing conduct, and even the grant of injunctive relief to prevent future infringing conduct, if you look at those as points along the parallax spectrum, those are the points at which we start taking the distances to see where the intersections might lie and how far apart they are.

And while as you go through them they appear to be at two different ends of the spectrum, I think if you take a deeper look, I think as we measure it, there is some interesting intersections that should allow us to proceed forward and come up with some sort of harmonized standards or policies so that we can start adding a little more predictability.

And very quickly, if you look at privacy under copyright, and I'm assuming most here are familiar with the Digital Millennium Copyright Act, it is the act that basically says in the intersection between ISPs and copyright we're going to create safe harbors, we're going to provide what they call a 512(c), basically, request for information of identity, it's based on good faith belief that there's infringing conduct.

We then, when the court stepped back and said that only applies for Web-hosting services, if you're a conduit one, you have to actually ask for a subpoena. If you look at all of the cases that have arisen that deal with a request for end-user disclosure, what you see over time is although the focus has been on making certain that there is a greater demand, in the demand there's greater proof that there's actually infringement, show me that there's not a fair use. Most of the debates are over fair use. You

don't see a lot of privacy language in copyright cases in the United States about the disclosure of end-user data. You see a little bit about expectations of privacy. But to be perfectly honest, when you look at what's going on here, you take a look at Sony Music, and it basically said, look at the terms of service, you've already said they could collect all of this information, don't tell us you have any interest in privacy moving on.

So the approach has been more or less copyright-centric focus, the focus has been on assuring that you have access to Internet service providers. And beyond that it's been, we really think you kind of gave up your privacy when you stepped into this, and we're done.

So you don't see a lot of privacy concerns. When it comes to the question of monitoring, however, we do have 512(m)(1), which basically says, and I like the title, it's from the statute, Protection of Privacy—thank you—there's finally a mention in the DMCA of privacy there. And it says you can't necessarily impose a monitoring requirement. But notice what it says: Nothing shall be construed to condition the applicability of your safe harbors to a monitoring, except to the extent consistent with a standard technical measure. On the one hand you don't have to monitor, we love privacy; on the other hand, there's that cute little exception that's hanging out there. So when it comes to end-user identity disclosure, as long as you can prove sufficient infringement, it seems to be a slam dunk, you get it.

When you move to the markers of the European Union, if you look at all those various directives, one of the challenges they have is half of those are privacy directives that don't mention copyright and the other half deal with intellectual property and don't necessarily mention privacy. Welcome to juggle the balls in the air and figure out which one bounces on your head to figure out where you're going to come out.

From an outsider's view, that's what it looks like is going on. Once you get into the cases though, there is some consistency. There are some points of attachment that make sense.

First of all, the easiest one. The issue that is the easiest to find in the United States, prove up the infringement, prove you need to have the end-user's identity, and you get it subject to some concerns about fair use. And we're done. It becomes a battleground here simply because the European Court of Justice, when it looked at all those various directives, said, you know, none of them have to do with civil procedures. And they're right. Welcome to God help you when they draft a directive in 1995. TRIPS just got signed in '94, nobody is thinking TRIPS. Two different hands talking about two different things. And out of the database privacy, the only exceptions they allow for monitoring and disclosure of information are for criminal prosecutions and investigations, and that's a constant.

So one of the issues that they have had to deal with is on the one hand I have privacy that says exceptions for national security, exceptions for criminal prosecutions, but it doesn't say that you have a right to monitor and disclose for civil actions. Yet you also have the enforcement directive which says, hello, we're supposed to provide effective enforcement.

The scary thing when you look at the recent cases that have come down is they have said there is no obligation under the directives to allow identity disclosure in civil procedures. So you can't look to the directives to say you have the right to get the name of the end user who is posting your copyrighted works, but it doesn't prohibit it either. So it leaves you to go to every one of the twenty-seven countries of the European Union and find out what their law says. If their national law says you're allowed to get the identity, and most of them do in some way, shape or form, you're not off the hook yet. You then go back into the privacy concerns and ask yourself, have you really demonstrated a strong enough need, have you balanced privacy interests against enforcement interests?

Now, ultimately as long as you have, it appears right now, strong evidence of infringement, and you really can't get the identity any further way and you have a good case for winning, you can most likely get the end-user disclosure, but you're going to have to really prove up. The ones that the courts have reviewed have been clear evidence of infringement. So it's not just the, gee, we think it might be infringing, they're really raising the bar because of the privacy concerns. So we don't have a directive that says that you get it.

For internationalists, the scary thing about all of this is they said that TRIPS does not require disclosure of user identity for effective enforcement. Fortunately, that hasn't been taken up to the WTO yet. But you could hear the sea quake on my side, on the IP side, going, "Oh, my God, are they serious?" And yet the privacy is going, "Absolutely, have you seen how much abuse is out there, from content owners trying to get content down that they shouldn't?"

So at least what we do see between the U.S. and the EU, I think, is some convergence. There is a recognition that it's not going to be the carte blanche, gee, I'd kind of like to know the identification. You are going to have to step forth and give some information and demonstrate that you do have a legitimate concern over copyright. It's going to be a privacy balance in the EU. It's going to be a fair use balance in the United States. And that there is no other easy way to get your hands on it.

So at least when it comes to end-user identity, I think we have some intersections we can actually work with. The one that gets really inter-

esting is when you talk about injunctions and the alternative side, which is monitoring. Because most of the injunctive relief against allowing future infringing contact, future posts of infringing information—under the DMCA we don't really deal with injunctions, we have notice and takedown, and we don't really go after injunctions quite as hard. So you don't have this monitoring issue going on. Because we do have the general prohibition against it.

In the EU, injunctions get knocked down, if they are to prevent future conduct, nine times out of ten, because you're asking the ISP to monitor personal information, because they have to find out who is posting it and how they're posting it in order to block it. And what you end up with is generally in two cases that both deal with a collective rights organization, the concern here, first of all, just because you're enforcing copyright doesn't mean privacy slides off the hook. We've already known that. You have to balance the two.

Second of all, to the extent that you ask for any monitoring activities to prevent future infringement, including access, you have to be concerned about the fact that you're asking them to monitor personal data, and the European Court of Justice has basically said, "You can still get an injunction, but you can't monitor everybody who is in the data stream." So when it comes to getting any sort of a block of future conduct through the privacy lens, the European Union has said, "That ain't going to happen. Not allowed." They're not talking fair use here, they're talking privacy. It's two different languages that we're talking about. When we talk fair use, we're talking free speech. They're not talking anonymous speech per se, they're talking a right to privacy and to prevent the access.

Now, what we do have in looking at the two is a new case that is out of the UK, it has not gone up to the European Court of Justice yet, that basically says, look, if it is a specific injunction that is aimed at specific conduct that does not require the identification of the end user, you can have the injunction. And it's relatively limited.

But interestingly, in Newzbin it dealt with an injunction that didn't block on the basis of the end users, it blocked on the basis of whether they were accessing exterior conduct that had not triggered the clean feed technology that they had. So the purpose of the injunction was to tell the ISP to monitor, in essence, the incoming traffic as opposed to the outgoing users. That's a narrow base, but it is a base to get an injunction. So people would say, "oh, my God, you can't even get an injunction to enjoin future conduct because of privacy concerns." Not necessarily true.

When you look at the parallax view, because I do a lot in law, I actually think it's helpful to have discussions about intersections and where we differ and where we disagree. I also think it's unfortunate that at

least currently when it comes to international models, we're all huddled in different corners and we're not talking to each other, because it's too complex, we can't understand it, we throw rhetoric at each other, as opposed to sitting down and actually trying to see the points of intersection and actually coming up with some international standards or harmonization standards.

Some people have said that it's impractical to come up with international harmonization standards based on how different our views between the U.S. and the European Union are insofar as privacy is concerned. Well, anybody who sat down and looked at the European views and the United States views on copyright, we're just as far apart. And we still can agree on certain harmonized concepts about who has the rights and what some of those rights should look like.

And the reason I say we're so far apart is, anybody hear the term "moral rights"? We are known over in Europe as the country that doesn't have moral rights. Largely true. And also known as the country that lets you sell your reputation. Little harsh.

So even if we're told to be the country that doesn't protect privacy, that's not true either. And I think if we take the rhetoric down, I think the future is that if we start talking now at points of convergence, if we start looking at the parallax view and start setting the standards, then we might actually come up with a framework that protects privacy as well as enforcement without being drowned in some of the rhetoric that's there now. Because now if you mention privacy and the Internet and copyright enforcement, you are part of the evil empire. And I think we need to end that and start talking so that we have a better boundary. And with that, I will stop. Thank you.

(Applause.)

PROFESSOR SORKIN: I'd like to thank all of our panelists, among other things, for complying with my requests, polite requests, as to time. That does leave us time for some questions.

I will start that off with a brief one of my own, picking up on Doris's last point, the future. We have heard from panelists about some of the dangers, some of the harms, the risks to our privacy. And we've heard from some folks about how challenging it is to deal with that and how technology makes that even more of a challenge. What do you see in the future? Is technology going to further injure privacy? Is privacy gasping its last breath? Or are we going to be able to harness this in some way such that technology, or otherwise, we'll get our privacy back? Ann, do you want to start?

PROFESSOR BARTOW: Sure. Well, I guess my issue is not unique to any particular technology, that any technology can be harnessed. I did think though when I talked about the police being not cost-effective, it's because it's actually fairly inexpensive to police your Internet. In other words, when Ken Zeran had the situation, AOL could have just written a program finding references to his name. It would have been a lot cheaper and more efficient if they wanted to do that. They didn't want to do it. They didn't want to spend the money to do it, and they also were making a lot of money because of his harassment, but that's not unique to the technology.

PROFESSOR SORKIN: Bob? As far as I know, Bob had nothing to do with it.

MR. GURWIN: For the record, AOL has a separate law enforcement unit that deals with such matters, and I can't comment on that one. In any event, I think what's happening and what we're going to see on a go-forward is as time goes forward consumers are becoming more savvy and understanding in new ways of what technology can do and consequently their own expectations have changed and, ultimately, I think that helps foster privacy protections. Because, again, like Marcy Syms used to say in the old TV commercials: An educated consumer is our best customer.

That's true with anything. And with mobile and Web, people that understand at least a threshold level of what the technology can do, enough to demand that the companies that are providing give them options, give them notice, give them opportunity to opt out or, you know, in a perfect scenario ask that they opt in before doing certain things, it's all going to help.

And the technology is not going to go away. It's simply how we, as a society, choose to manage it. And again, as we go further and further from 1993 when Mozilla hit everybody's screens and everybody was like, wow, this is so cool, but nobody knew what the heck was going on in the background, people are waking up. It's taking time and it's taking a generation, but people know, even if they're not savvy, they're starting to know enough to ask: Is there something more I should be doing and know about here?

PROFESSOR SORKIN: Doris.

PROFESSOR LONG: There was an interesting, as part of the draft privacy regulation coming out of the EU, there was a study that was done by Eurobarometer, and it's interesting because one of the questions they asked is: How much privacy do you expect on the Internet and are you getting it? And it's intriguing to me how much privacy is expected

and yet at the same time they recognize they don't have as much as they think they're entitled to.

What I think is real interesting is our definition of "expectations of privacy." I know, I teach an IP digital class, and when Facebook graciously gave all of its users access to that wonder, timeline, of guess what we've been saving for you and here it all is, expectations were extremely different. And I do think maybe consent as an opt-in at each step to let you know when you can pull out of it is amazing.

The other thing I've been impressed with is my students who say: If I post it for X reasons, it shouldn't be used for Y. And the world doesn't operate that way. So I think we all assume that we're sophisticated consumers. I'm not sure, unless those forms get a lot easier, if we really are. And I think as opposed to technology, we need much—you know, the European Union may not be wrong in its strict consent, be-real-clear policy, as an ultimate goal.

PROFESSOR SORKIN: Thanks. I think we have time for one maybe two questions.

FROM THE FLOOR: I have a question for Ms. Bartow. In terms of the immunity that is provided under Section 230, where does stuff like defamation or invasion of privacy or public disclosure of the Privacy Act fit?

MS. BARTOW: Absolutely immunity.

PROFESSOR SORKIN: The question was: Where does defamation and invasion of privacy fit into immunity under Section 230 of the CDA?

PROFESSOR BARTOW: The only limits on the immunity are related basically to child pornography or intellectual property

FROM THE FLOOR: In other words, not a form of attack?

PROFESSOR BARTOW: Nothing. There is no absolute immunity for third-party postings. They can't post it themselves.

FROM THE FLOOR: So a general question for everyone, which is, if we were to craft a regulation or a law that allows companies or actually forces companies to remove harmful content, however way harmful it is, as defined, how would each of our panelists approach and shape the contour of this law? And I think for Professor Doris Long, I know in copyright we have a lot of mechanisms for taking down things that

apparently is not translated over there. So any kind of parallax synergy there is appreciated.

PROFESSOR SORKIN: If I can summarize the question, if there were a law requiring removal of harmful content, perhaps analogous to what we do for copyright infringements under the notice and takedown procedures in the DMCA, what would or could that look like?

PROFESSOR BARTOW: Well, I mean, the notice and takedown under the DMCA is certainly not perfect, there is a lot of room for criticism. Ironically, Fred von Lohmann who used to be with EFF said it, but it works pretty well. This is the same guy that absolutely said we couldn't possibly do it for any of the speech torts. So make of that what you will. I mean, we're humans. Anything we're doing would be flawed and there would be some problems, but I think we could take a stab at something, something that allowed for notice and takedown for pretty severe acts that were encouraging violence.

MR. GURWIN: From my perspective and contrary to information that Ann is conveying, our company actually does quite a bit in the space. Wherever we have end user-generated content, there's a report that's filed. And there is a team. Basically our consumer action team looks at that stuff and they tend to take down first and ask questions later, at least from my experience and my understanding. So again, nothing is perfect, but again I think that where you have an opportunity to click a "report this" where you think that there's something, and at least engage somebody who is trained to screen it and take a look at it and decide whether it should be referred to law enforcement, whether it should simply just be removed to stop the swirl or something else, at least if there's some human element there.

PROFESSOR BARTOW: In my experience the ISPs do not do this and certainly don't do it in a timely way.

PROFESSOR SORKIN: Doris, do you think that we Internet privacy people have anything to learn from the copyright folks?

PROFESSOR LONG: You know, it's funny, because Ann mentioned the notice and takedown, and she and I have been at conferences where it was just criticized, ridiculed. It's so nice how much difference a bad term suddenly makes, and it's like that's not such a bad idea after all, because in other settings it works.

Although Canada just opted for notice and notice. I think one of the most tough things that's floating around there right now is the European

Union draft regulation of the right to be forgotten, which poses yet another level of notice and takedown, because now it's not just harmful speech but can I actually send a notice that says, you know, I'm really embarrassed by those drunken photos of me in high school, I want them to be forgotten, go out and take then down, poses all kinds of interesting issues in so far as how do you actually reach. Somebody told me there is actually an ISP that's threatening to be up in space as soon as they can figure out how to launch a satellite and pay for it.

MR. GURWIN: It's not AOL.

PROFESSOR LONG: So it poses a lot of interesting questions. But I do think notice and takedown with some tweaks could be applied in a lot more interesting ways to deal with all different kinds of harmful speech.

PROFESSOR SORKIN: I think we need to stop here. That concludes our session. I'd like to thank our panelists for their interesting and provocative remarks and our audience for sticking with us throughout the symposium. We're going to move on to a dedication of this courtroom at noon and then a convocation with Justice Scalia later this afternoon. Thank you for coming.

(Whereupon a recess was taken.)