

**ASSOCIATION OF CORPORATE COUNSEL**

**Desktop Learning Webcast Transcript  
Trade Secrets in the Digital Environment  
June 14, 2007**

**Faculty:**

**Francis J. Burke**, Partner, Steptoe & Johnson LLP

**Rebecca Edelson**, Partner, Steptoe & Johnson LLP

**Moderator:**

**Joseph F. Murphy**, General Counsel, Shainin LLC

Joseph Murphy: Hello to everyone. My name is Joseph Murphy. I'm with the Intellectual Property Subcommittee – Committee of the ACC Intellectual Property Committee. We have with us today two experts from Steptoe & Johnson, Frank Burke and Bec Edelson. We're going to be talking about trade secrets in a digital environment.

We have a question-and-answer format during the call. When you – if you have a question, please type your question into the box in the lower left-hand side of your screen. You'll be able to see your question. We'll see it also. Please keep

in mind that there are often many questions, and we may not be able to address them all. So please do not feel slighted if we do not get to your question.

Finally, we ask that before you leave the call you click box number or number one, Web Cast Evaluation in the box just above the questions just below the Links box and give your standard speaker evaluation of how you liked the program.

So that takes us to the beginning. We're going to start with a little bit of intro about trade secrets just through slide warm-up, and you'll note that maybe – Bec , maybe you can take us through the definition of a trade secret.

Rebecca Edelson: Sure. First thing I wanted to say was that there is no uniform definition across the country. It's not like the Patent Act, the Copyright Act, et cetera, that – which are uniform because of Federal law. Here, we're dealing with trade secrets, and so there's state-to-state variances, including the definition. But generally, I can say that it has three prongs to the definition. It has to be information. The trade secret holder has to have used reasonable means to keep the information secret, and the information has to have economic derived from its secrecy. So you have to think about if it's not information, try some other form of protection. Similarly, if it's not secret and it's generally known by others, trade secret protection won't help you, and you should just forget it. Similarly, you have to think about the last prong, economic value derived from

secrecy. So if it has value, but it's not because it's secret, and the value is derived from some other aspect, I would not look to trade secret protection.

Joseph Murphy: All right, so – and how long – how long did you say the protection could last?

Frank Burke: I guess I'm going to jump in on that one, Joe. This is Frank Burke for the benefit of the audience so you recognize my voice. There's no strict definition on how long a trade secret can last. The issue of a trade secret is always going to be in the first place is it, in fact, secret? Is it something that's not generally known to the public, and that's always an issue in any trade secret situation. And then secondly, the question is have you taken reasonable steps to preserve its secrecy, and that's often times a problem because as companies deal with outsiders, vendors, manufacturers, suppliers, customers and the like, they often times find that they – something that was secret has not become a secret because it's become known to others, and so you have to look at your trade secret portfolio periodically. You don't want to waste information – money protecting information as if a trade secret if it no longer has value from being kept secret.

Joseph Murphy: All right. Would you like to say something about the Eldorado Stone case? Were you going to bring that up?

Frank Burke: Sure. Bec and I were going to just talk about a few recent cases in the trade secret area because it is a state-by-state area of law. There's not as much importance to presidential value. But we just wanted to give a few examples of some recent cases. This was an Eldorado Stone ...

Joseph Murphy: Give us a survey – give our audience a survey of what's the latest news of trade secret cases, and I've already cued up your slide for Eldorado.

Frank Burke: Sure.

Joseph Murphy: Thank you.

Frank Burke: In the Eldorado case, it was a case where Eldorado Stone won a \$17 million Federal jury verdict for trade secret misappropriation against their rival stone manufacturer, Renaissance Stone. They also get \$3.85 million dollars in punitive damages and attorney fees. So this case demonstrates that, first of all, trade secret cases can mean big money. I think every year or so the National Law General does a survey of the largest jury verdicts rendered that year, and often times trade secret cases are at or near the top of that list. This particular case took years. The dispute arose in 2004 and wasn't resolved until 2007. So it can be a very expensive commitment to pursue a trade secret case.

Thirdly, the case shows that computers—and that's part of the theme of this broadcast—computers are the new favorite method of misappropriation. In this particular case, the defendant – one of the defendants, whose name was (Alvarez), downloaded significant amounts of trade secret information while he was still an employee of Eldorado. So departing employees are a hot bed for misappropriation. The enemy was in is often times more serious than the enemy was out.

Joseph Murphy: I see. I see. So the party employees are often the ones to look for.

There are some other laws to consider, are there not, and could you tell us about some of those?

Frank Burke: Sure. The slide lists a number of items, many of which we don't really have time to cover today in our little one-hour broadcast here. But copyright infringement is obviously very important, The Digital Millennium Copyright Act. Often times with information on the web can be used in combination with some of these other provisions. The Computer Fraud and Abuse Act is a very important weapon, and I want to spend a little time covering that. Electronic Communications Privacy Act is important. The Economic Espionage Act, which is essentially a Federal statute which makes criminal trade secret misappropriation, and then there are trade secret – state trade secret criminal laws that deal with either misappropriation of trade secrets, receipt of stolen property or computer hacking.

Joseph Murphy: That sounds quite a list – quite a list of primes. Can you take that back a little further and take it to the next? You mentioned a CFAA, and tell us why we'd want to use that, please.

Frank Burke: Well, the Computer Fraud and Abuse Act is a law that's been on the Federal books since the 1980s, and I'm continuously surprised about the number of folks that really don't even know it's there. It's a very, very important weapon in the – in the computer environment. It's a Federal statute, which was originally designed to make criminal hacking into computers, but it's been amended several times by Congress. Every time there's a new technological change, Congress goes back and tinkers with the law, as over the years hackers and worms and viruses were interposed.

But the interesting thing about it is it has Federal question jurisdiction, and you can have supplement jurisdiction, obviously, for pendant state – trade secret claims. But it has a civil damage provision in the Computer Fraud and Abuse Act. So it's somewhat – it's been analogized by many to the Federal Racketeering Statute, which has primarily a criminal statute, but which has civil components, and this, I think, is going to be in the computer environment, for many as important a weapon as state trade secret protection and confidentiality agreements, which we'll talk about in a little bit. But it very broadly, the statute covers protected computers against unauthorized access or exceeding

authorized access. Those two terms—unauthorized access or exceeding authorized access—are the core of what this statute is all about.

Joseph Murphy: So even if an employee has access – if he exceeds the authorized access, there are cases that hold that they've done that?

Frank Burke: Yes, if they – if they commit other violations of the statute, such as causing damage or taking information with the intent of defraud.

Joseph Murphy: Now, is that the Shurgard case you're talking about?

Frank Burke: Sure, let me just finish these two points.

Joseph Murphy: Excuse me.

Frank Burke: Protected computers. Is there any computers that are attached to the Internet, and in today's environment that's just about everything. Now, exceeding authorized access, the Shurgard Storage Center's case and the complete site to this is in one of our linked items, which the audience can pick off the little box on the left there and download.

Joseph Murphy: Afterwards – later on after they do number one web cast evaluation, there are other choices with choice information like that.

Frank Burke: Sure, this was a case in the Western District of Washington, and it was a civil action under the Computer Fraud and Abuse Act. That was a case where the defendant embarked on a scheme to hire away key employees of the plaintiff for the purpose of taking their trade secrets. Some of the employees jumped the gun. While they were still working for the plaintiff, they used its computers to send trade secrets to the defendant by email, and in a very critical – analytical passage, the court looked at the restatement of agency and concluded that once the employees began acting as agents for the defendant, when they then used the plaintiffs computers and information in those computers in an improper way, they were acting without authorization, and that concept has been picked up by other cases after that, and we'll talk about a couple if you advance the slide.

Joseph Murphy: All right, please.

Frank Burke: International Airport Centers versus (Citron) was an opinion that came down just last year in the seventh circuit, and this was similar kind of a situation. Prior to leaving the plaintiff to compete with the defendant destroyed laptop data. He simultaneously took information, which was confidential information, and then ran an erasure program to cover up his footprints. So the court found that the taking of the data and running that erasing program damaged the computer and found that a transmission in interstate commerce can occur via a signal from a disk drive, and so the court there decided that his authorization had terminated

when he decided to destroy the files, thereby breaching his duty of loyalty—again, applying the Shurgard test and revisiting the restatement of agency.

Joseph Murphy: I see. I see, and would you like to say anything more about that case, or shall we move to the next. Well ...

Frank Burke: No, I think it was ...

Joseph Murphy: ... my finger slipped. I guess we have.

Frank Burke: The next piece I wanted to talk about was the first circuit decision, EF Cultural Travel BV versus Explorica. The interesting thing about this case is it involved the use of a hacking program, which took information off of a public Internet site, and you couldn't really analyze the data properly without the confidential information in the minds of the departing employees. But the information that they took was freely available on the web site, but they used a scraper program, which went up very, very rapidly and downloaded 60,000 lines of data, which is something like the equivalent of 10 telephone books, and there the court focused on a confidentiality agreement that they had signed with their employer, which prevented them from misusing the employer's information, and because they violated the confidentiality agreement, the court found that their actions exceeded authorized access.

Joseph Murphy: All right, then. So we can move on from there. But that is the key development, would you say, in the statute going from where it was a moribund overlooked statute, like (Rico) once was, to where now that people realize they can use it against the enemy within?

Frank Burke: Exactly. I think that after – over 20 years of jurisprudence, at the beginning most of which were criminal cases, we've now got a fairly defined body of civil law, and we've got several, I think three or four, courts of appeals in the United States, courts of appeals, which is weighed in on this statute, and so we've got a nicely defined body of law, and so people don't have to feel like they're pioneers going to Federal Court using this statute. They've got a very, very powerful weapon, which can be part of their arsenal, along with Trade Secret Law, State ((inaudible) Fiduciary Duty Law, and of course, breach of confidentiality agreements.

Joseph Murphy: I see, and perhaps if they click in the links, they might be able to access and save some of that information also. So having – and I know we're going to come back to this often overlooked law, but would you like to say something about the – you mentioned the Electronic Communications Privacy Act.

Frank Burke: Sure, this is essentially the Federal Wire Tap Statute, and it comes up with some frequency when folks hack into other people's web sites, and there was a – and it sometimes can backfire. It can be a legitimate company which is trying to track down a person which has misused or stolen or misappropriated confidential information. But if you hack into somebody else's web site and then download information from there, you can easily run a file of the Electronic Communications Privacy Act.

We had a scenario where, in one case I was in, where I should say a prior counsel used passwords that departing employees had used internally. They left the company and were setting up a competing business, and the employer used their passwords to enter their new web site. I guess you could call that the what we now know is pretexting from the Hewlett Packard case. But in that case, they took information from the new web site, got a lot of business plans, used them to get a temporary restraining order, and then when the other side came in, they said, look, this information was on a protected web site. They hacked into it using our passwords without our permission, and they thereby violated the Electronic Communications Privacy Act, and that backfired on the employer, and their injunction was dissolved, and they pretty much lost all impetus on the case, all momentum in the case.

Joseph Murphy: Well, we had ((inaudible)) things like, but we wondered on the idea of injunctions and getting a handle on that. Bec Edelson was going to say a few

words about that, and she had a choice case picked out, which we'd like to share with you. And Bec , are you – are you there?

Rebecca Edelson: Yes, I am.

Joseph Murphy: All right. Well, please lead away with your Wal-Mart ex parte (TRO).

This sounds like something else.

Rebecca Edelson: Sure. It's not a case I was involved in. In fact, it's not even a published (paste) or anything like that. I just happened to see a blurb about it in the news, and I thought it was interesting. It's from, I guess, April. Wal-Mart apparently went to a judge at night to get a completely ex parte (PARO) against one of its former employees for misappropriation of trade secrets, and all of the documents were sealed. They went to the judge's house at night, and it just struck me as an interesting case because that would be incredibly unusual here in Los Angeles, if not extraordinary. In any event, Wal-Mart filed the case against a former security employee, and that sort of raises the issue of you really can't trust anyone, because if this person was responsible for protecting Wal-Mart's trade secrets, and here Wal-Mart is going after the security employee, and we're not talking about a security guard. We're talking about someone who is actually responsible at a higher level for security of information.

So you really need to have some sort of backup plan in case your security employee sort of runs amok.

Joseph Murphy: It's who watches the watchers kind of thing.

Rebecca Edelson: Right, exactly. It may not be feasible for a lot of businesses because they're not the size of Wal-Mart, but it is just something to think about. I think in this case this was actually true in the Renaissance Eldorado case that Frank described earlier. Again, we were dealing with someone who was responsible for protecting the trade secrets of the company.

The other aspect of the Wal-Mart case that I found interesting was the judge just sealed the pleadings in connection with the (TRO) application, and sealing means that the court will make an order such that the public cannot access those court files, and that's pretty important in a trade secret case because you're sort of caught in this catch 22 situation. Here you want to protect your trade secrets from further misappropriation, but you don't want to have to file your trade secrets in a public record to do so, and you would think that, well, of course the judges should just seal the records, but there's also a countervailing public policy in favor of public access to court files that you'll run up against, and for ...

Joseph Murphy: Is that a threshold issue, then, that you have to deal with with your clients when they say, Bec , we want to sue our trade secrets, but do we have to file them?

Rebecca Edelson: Definitely. You have to warn your client, not just in sealing but in the litigation generally, you're up – you know, remember you're upset that this guy has your trade secrets. Well, if you file litigation, chances are they'll get even more of your trade secrets in the course of discovery, and it just really depends on the judge you pull. Some of them take a more practical approach. Of course, you can have these documents sealed. They're trade secrets. How could you file a trade secret case without having the ability to seal? But other judges who aren't used to trade secret cases just think everything should be presumptively public, and so you'll have to take the time to convince them that you need a sealing order on this case.

Joseph Murphy: All right. So you have that – on the one side, the judges that are a little skeptical and maybe a little restrained in their use of judicial power, but you also were going to give us an example of a judge that was not shy to swing his or her gavel, aren't you?

Rebecca Edelson: Yes, it's true. The other thing too, remember in (TRO) proceedings, a lot of times you need to get a confidentiality protective order in place very quickly, and sometimes that is given short shrift, and you'll just take an old form

that you have from another case and, you know, submit it. But that's not a good thing to do because you have to live with that protective order throughout the case, and it's a pretty important document just to do it in five minutes.

Joseph Murphy: All right. Didn't mean to jump the gun there. Yes, but I just went through a case where I had to live with something like that, and ...

Rebecca Edelson: It comes back to haunt you.

Joseph Murphy: Pardon?

Rebecca Edelson: It comes back to haunt you, often.

Joseph Murphy: It does. It does, and it's – it does. Now, my slideshows are many. Did I skip a slide there, or are ...

Rebecca Edelson: No. I'm going to talk about that one next. That was another case.

The last one was out of Arkansas. This one was out of North Carolina, the Arminius versus Design Industrial case, and that one is from, I guess, March, and again, this was something I just saw a little blurb in the news about, and I found it interesting because usually the (TRO) you'll get is something to the effect don't use those trade secrets, don't disclose them. But here, the judge ended up closing down the defendant's facilities, and I thought that was really interesting,

and apparently there is some background to that rather harsh order. When the court issued the (TRO), it also ordered that the plaintiff should be able to go into the defendant's facilities and inspect the computers, and when they went to do that ...

Joseph Murphy: They found them shut ...

Rebecca Edelson: ... they found that the defendant had sort of closed shop, so to speak, and so when the judge went to enter the preliminary injunction, he ...

Joseph Murphy: Maintained the status quo, so to speak?

Rebecca Edelson: So to speak. I was just going to say I shouldn't say he. I don't know if the judge was a man or a woman. And so that was pretty extraordinary and interesting.

Joseph Murphy: So basically, then the plaintiff had examination had its ledger, then.

Rebecca Edelson: Exactly. The other interesting thing about this case I found was it was sort of – there was footprinting in reverse. Footprinting is when a trade secret holder uses some clever means to monitor for misappropriation, for instance. If you're dealing with a customer list, you put your dog's name on the

customer list to see if your dog gets any mail, and so it's a way of tracking misuse of your customer list from – by people who have access to it.

Here, the defendant was ...

Joseph Murphy: I'd say because they cannot say via some other source got your three-year-old's misspelled name or the dog's.

Rebecca Edelson: Right, exactly, and here, what the defendant did was apparently the defendant was concerned that the plaintiff would notice if one of the usual suspects was receiving information or that sort of thing. So they asked one of the plaintiff's employee's mother to send a laptop to the defendant filled with trade secret information, and so it just goes to show that misappropriators are getting cleverer and cleverer, and they're aware that people are watching, so to speak. So it's just something to think about.

Joseph Murphy: Well, and that's something. That is something. That goes back to, I think, INSV, the International News Service or something, and – but this is a long way from that. Do you happen to know the outcome offhand of that case?

Rebecca Edelson: No, I mean it was pretty early on. I just saw the news ...

Joseph Murphy: I'd say it's ...

Rebecca Edelson: ... but I'm sure, you know, unless it's settled quickly, who knows?

Joseph Murphy: Yes, it will take a while to figure out. What about when you have – well, not mothers or three-year-olds, but what about when you have partners that go awry?

Rebecca Edelson: That brings us to our next case, the (James vs. Watson) case, and that was out of Texas, and I did check the docket recently, and it looked like it had settled in August, but I found it an interesting case because apparently it's not just departing employees you have to worry about; sometimes you have to be concerned about your own partner, and in that case, the plaintiff alleged that his partner had allegedly caused the web site, which it was a web site which allowed customers to create their own web sites.

Anyway, the plaintiff alleged that he and the other partners claimed to own the web site which allowed you to create other web sites, and the defendant, after they got into a dispute about renegotiating their agreement, made the web site inaccessible to the other partners, and he took it and was using it for his own private business. He diverted the partnership deposits through the web site to his own bank account, and the reason this is a trade secret case, although it has lots of other aspects, is that he allegedly appropriated the web site customerless for his own benefit. So that's what made it a trade secret case.

In any event, the court denied some rejudgment of the trade secret claim on the grounds that there were triable issues as to who owned the copyrights. In other words, if they owned it, it wouldn't be improper to take it, et cetera, et cetera. But the message I think you should take away from this case is that things can go sour. You really need to think ahead about what's going to happen when things go sour with whether it's your partners or joint ventures or anybody you're dealing with, even if it's a vendor or something like that, and you want – you want to make sure you have an exit plan.

Joseph Murphy: Have an exit plan for?

Rebecca Edelson: When the relationship breaks down, you don't want the other person to be in a position to steal your bank deposits, you don't want them to be able to sort of take over the web site, you know, that sort of thing.

Joseph Murphy: Yes, I see.

Rebecca Edelson: You just sort of want to think ahead.

Joseph Murphy: Sort of an ejection plan as well as a ...

Rebecca Edelson: Right.

Joseph Murphy: I see, and Bec , one thing that we hear that when people do become disrespectful of trade secrets and do decide that they want to sing like a canary, that they wrap themselves in, if not the flag, the First Amendment, and can that ever get brought into these kind of cases?

Rebecca Edelson: Yes, they can. The First Amendment rights is actually a fascinating issue within trade secret law, and it's not often raised, but every once in a while somebody will raise it in the case. For instance, in the – when someone seeks an injunction, that will be the defense to the injunction against disclosing trade secrets. They'll say they have a right to disclose the trade secrets under the First Amendment, and if you look on the screen, you'll see a couple of those cases. The most recent one, I think, which is of importance is one out of California in 2003. Apparently, there was an indictment of the whole Trade Secret Act and protection and not of the whole Act, but of the biggest weapon under it, the ability to get an injunction, and so that actually went up to the California Supreme Court, and people were really looking to see what the Supreme Court would say, because this is obviously a really important aspect to protect business information, trade secret protection.

And so it went up, and interestingly, the Supreme Court of California said the First Amendment does apply, and you have to do an analysis, but the bottom line is that it's not that difficult to pass constitutional muster, so to speak. The

injunction has to be tailored to protecting trade secrets. Other courts, like for instance, there's the (Ford) case listing under it ...

Joseph Murphy: OK, we're going to have to – we're going to have to hit – if you'd touch on that briefly, we're going to have to speed it up a little. We're actually one-third of the way through the slides and one-half of the way through the time.

Rebecca Edelson: No, I know. I was actually. That was all I was going to say. There were other cases ...

Joseph Murphy: Excuse me.

Rebecca Edelson: ... coming out the other way.

Joseph Murphy: Forgive us, folks. We're not professionals at this, so classes – cases the other way that they can look online for, rather on the links that are provided to the left here.

We had something about – our title's about digital, and Frank's telling us how we could really use this digital law. But is it safer if you have it in paper? I mean what else can you do if you only have digital? I see you've made a good list, and if you'd take us through that.

Rebecca Edelson: Sure. The way I see it, there are three basic ways you can maintain trade secret information. You can just store it in your head, you can have it in digital form and you can have it in hardcopy, and by that I just mean old fashioned paper, and there are pros and cons to each storage method.

For instance, in storing something in your head is not really practical if you're dealing with voluminous complicated detailed information, and ordinarily, in this day and age, trade secret information needs to be shared with others in order to exploit its value. If you keep it in your head, you're not going to be able to do that. Similarly, you know, what if the one person who has the trade secret information is hit by a bus, so although it's really safe from misappropriation, it's really not that practical just to have one person keep the information in their head.

The other way you can store it is digital form, and that's very practical if you're dealing with voluminous complicated information, and it certainly is easy to share the information with others who need a legitimate access to it. On the other hand, that's why – one of the reasons we're having this program today is because it's so easy to forward digital files with trade secret information, and it makes the risk of misappropriation all the greater, and that's, you know, it's not a reason not to do it. You just have to think about it, you have to use the appropriate technology that will reduce the risk of misappropriation—firewalls, passwords, watermarking, you can try and prohibit downloading and printing.

There's lots of technology, and the reason to use digital is that it actually leaves a trail of misappropriation if it is misappropriated. For instance, if you have it in hardcopy, that's not going to be the case. There's not necessarily going to be something you can track in terms of if someone hands over a piece of paper to another person.

Joseph Murphy: Oh, I see.

Rebecca Edelson: So, I mean the bottom line here is you shouldn't just let the form of your trade secret information be decided by default or inaction. You should think about it and make sure it's the right decision for your type of business and information.

Joseph Murphy: All right. Well, even assuming that you've done it all right, you've kept your trade secrets, and it was mentioned at the very beginning that one of the basics is you have to keep it secret to get that special status. What happens if the disgruntled employee, the hacker or the whoever gets your trade secrets and just publishes them on the Internet? Can you get the cat back in the bag?  
Frank, I know you had some views on this, and ...

Frank Burke: Well, the answer is a solid maybe.

Joseph Murphy: OK.

Frank Burke: The – as long ago as 1974, the U.S. Supreme Court, and I think we may have a slide on this, indicated that once information is disclosed, whether it's inadvertent, accidental, malicious or otherwise, that it ceases to be a trade secret and loses the benefit of trade secret protection. But over the years, that can make for some fairly harsh circumstances because you find some cases where you have highly disgruntled employees, who put the information on the web essentially for completely malicious purposes.

There's been a series of cases – a whole series of cases involving the Church of Scientology. There have been a series of cases which involved the DVD hacker protection, the method by which DVDs are encrypted so that you can't freely copy them, and people about 10 years ago started posting the ability to remove that copy protection, and so the courts have had to grapple with scenarios, with if an employer, an entity had taken all the reasonable steps to preserve the secrecy and somebody maliciously tried to destroy the trade secret status, would that be fair to leave them with no remedy, and the courts have kind of come down all over the place, unfortunately. Some of them have found that as long as you act quickly, try to get an injunction rapidly, remove the information from the web as quickly as you can through injunctive relief, then you shouldn't lose trade secret status, and others have said, no, once the cat's out of the bag it's gone.

Joseph Murphy: I see. I see, and so that's evolving – that's just kind of involving, I suppose a – at least ...

Frank Burke: The last bullet on the – on the slide, “Be Careful What You Put on Your Web Site”, is a word to the – word to the wise. Many times you've got counsel over there working very diligently, trying to make sure that they maintain intellectual property protection for other trade secrets. Well, on the other side of the house, the marketing people are working away on the web site, and we've had cases where somebody has actually sued to try to enjoin the release of a customer list or some confidential formula, and you go on their web site, and there's a list of customers freely available for anybody to see or the formula is right there on the web. So be careful what's out there. Sometimes it can be inadvertent as well as malicious.

Joseph Murphy: I see, so you have to be careful either way and – we gleaned from all of these examples that these things seem to be really fast and furious, and strange things happen, and all of a sudden you find out your information has been compromised, and I can say that – I can say that's one of my – one of the joys of being moderator on this call is that, of course, one gets to ask the questions, which is easier than providing the answers, and I wanted to thank Bec for – well, for sending me a copy of and for writing her book, which is linked in your materials on your screen. It's a good listing of practical examples and tips and what-ifs, and the book's entitle “Trade Secret Litigation and Protection in

California” published by the State Bar there in 2005. As you can see, a lot of cases come out of California. That book will contain more practical tips than we can go through today, but we’re going to go through a few more of them from them now, and Bec, did you want to hit a few of them now?

Rebecca Edelson: Well, actually, before – I think Frank’s up next, but before we left out, I wanted to thank you for plugging my book, and it actually didn’t make it up onto the link how to order it, but I’ll just tell people they can just go to the State Bar of California’s web site, and they should be able to figure it out.

Joseph Murphy: All right.

Frank Burke: Yes, Joe, if we could go through the next few slides very rapidly, I think I can hit some of these points.

What we first wanted to do was go through some of the traditional methods of preserving protection, trade secret protection, and then take some of those concepts and apply them to digital media, and since the theme of the program is the digital media, I would like to try to go through the next five or six slides very rapidly, and they’ll be available for folks to read afterwards. If we could just go to the next slide.

Joseph Murphy: OK, we'll go to the next slide. But something occurred to me, as in in-house, if you'll permit this one conceit, it's not a – it's not a book, but whenever you have people coming into your companies, everyone on the call, have them sign a form when they enter, a logbook, to get their visitor's badge, and include some sort of language that they're signing could seem inoffensive that at least let's you establish that they were there and they know they were not there for a free information-gathering session, and but, again, refer to Beck's book for many more.

This is our next slide, then, for you there, Frank.

Frank Burke: Sure. Let me give you the nutshell version of the next 20 minutes.

Joseph Murphy: OK.

Frank Burke: You can lock the front door of your building, you can make people sign in, you can keep everything under lock and key. If you don't make any effort to stop people from sending things out onto the Internet using email or instant messages, you have the equivalent of the backdoor of your company being wide open, and so it's important to do these kinds of things in terms of security, but if you haven't implemented digital security, then you've – in today's environment, you're only halfway there. You've got the front door locked and the backdoor wide open.

So I'm going to flip through six slides very rapidly here, and people obviously have these available, and I think most of the audience members probably already know most of these. Obviously, marking documents confidential and confidentiality policies are important.

Next slide.

Joseph Murphy: All right. Prudent efforts.

Frank Burke: Having employees sign forms at their date of hire, and then annually and at the time of every promotion under various states' laws. If you don't redo these when people are promoted they become ineffective. They need to acknowledge that they're using trade secrets. They have to sign confidentiality agreements. They have to understand that they're working with trade secrets.

Next slide.

Joseph Murphy: I see, and you do that at promotions, right, for when the proverbial versus promoted from the mailroom, and then when he leaves as CEO they learned he never signed a disclosure agreement because he was hired as (plunkin).

Frank Burke: OK, confidentiality in India agreements are an incredibly critical component in terms of an overall trade secret protection program. As I mentioned at the outset, it's very hard to prove that something is a trade secret in the first place and that it kept its trade secret status throughout, and often times you may go into a case with a 20 things that you think are trade secrets and only find out by the time you're done that only five or 10 of them were actually trade secrets because they were – either weren't confidential at the outset or it was lost.

So the – one of the most important weapons to be able to preserve all 20 of the items in my hypothetical example is through a confidentiality or a nondisclosure agreement. These need to be used very broadly. As Joe said, have people actually sign them when they come into your plant. You can design a little two-part form, where the upper portion is actually a confidentiality agreement that goes right, and the bottom portion is the badge that they're going to wear when they're in the site. Obviously, employees – any kind of contractors, licensees, joint venturers are – there are many cases where joint venturers wind up being the thieves. They probably don't consider themselves thieves, but they – to the person who's lost their confidential information, they might as well have been a burglar. Consultants, outsources, other vendors—these persons often times themselves will be, on your behalf, dealing with third parties, and you need a program by which this first line of contractors and vendors are required to get the (patrons) with whom they deal on your behalf to sign (NDA) agreements.

There have been some great cases where something was found not to be a trade secret but was found to be confidential information within the meaning of the nondisclosure agreement, and very effective injunctive or damage relief was secured. You have to remember that one form doesn't fit all. Sometimes you can – this can backfire if you try to imply that everything that you have is confidential and it really isn't. So sometimes you want to have limited purposes on disclosure agreements, and these should be maintained by the legal department. Next.

Joseph Murphy: All right. So, yes, maintain them by the Legal Department, and next slide. We have more on prudent efforts.

Frank Burke: Yes, you want to try to keep records of persons who had access to the trade and secret information. Use a checkout system. Next.

Joseph Murphy: Yes, and if I could just interrupt for a moment, Frank, and to all of our listeners, we're coming up on about 12 minutes before the end of the call. So in about five minutes, we're going to start taking questions. If you have question, please take the time to type it into the box at the lower left-hand of the screen and click "Send", and I'll be reading them off, and we'll throw them to the panel.

Please – Frank, please continue, and would you like the next slide already?

Frank Burke: Yes.

Joseph Murphy: OK.

Frank Burke: Putting restrictive legends, having a good security – physical security system, sign-in procedures, badges, restricted access, locks and passwords.  
Next.

Joseph Murphy: All right. All right. Continuing. The exit interviews?

Frank Burke: Exit interviews, obviously when you have people leaving you want to remind them of their continuing obligation to maintain secrecy. You need to collect all of the information that they have and send them a follow-up letter reminding them of their obligations. Next.

Joseph Murphy: All right, so keep them straight. Where else can you emphasize the trade secrets to the employees?

Frank Burke: You can have codes of conduct. Sometimes there have been situations where companies have slipped up and didn't get the trade secret agreement signed by the employee, but they put it in the Code of Conduct or an Employee Manual, and that was signed by the employee. So sometimes those can be the

belt and suspenders. So you have employment agreements, trade secret agreements, you have codes of conduct and you have employee handbooks, all of which are good ways to remind people of their obligations.

Joseph Murphy: All right, and thanks for those tips. Now, we would be remiss if we didn't address email in the two minutes or so before we take some questions, and Bec Edelson has some thoughts on practical tips.

Rebecca Edelson: Sure.

Joseph Murphy: What would some practical tips be to protect trade secrets in email documents?

Rebecca Edelson: Well, misuse of email is a bigger topic than we can possibly cover here. It's the bane of every lawyer's existence at this point, and you'd be surprised what people will put in emails. The problem is people don't think before they push that send button. A few tips which you can address vis-à-vis trade secrets information and the protection is you need to educate your employees as to the proper use and the improper use of email. They need to understand what they should send by email and what they should not send by email, and one of the things that is also problematic as far as trade secret litigation is concerned is that people do not keep records of emails that people send to them. They just sort of feel like it's a conversation, and if someone sent

an email rather than a letter, it wouldn't necessarily make it into the file. So they need to understand an email is a record that they should maintain if it's worth maintaining.

You can have a blanket rule—don't send trade secret information by email. The reasons for this is it's too easy to forward to the world, it's easy to hack into, and less proper technologies use. There's also human mistakes such as sending it to the wrong addressee, so to speak. It's probably – well, it may be unrealistic in this day and age to tell people they can't send things by email, but if you do allow emailing, you need to make sure you're using appropriate technologies such as encryption, anti-hacking technology, firewalls, passwords and that sort of thing.

Joseph Murphy: Yes, but Bec, I notice you have a number of those covered in some of your materials and the books. Are you ready for your next slide?

Rebecca Edelson: Sure, let's go to the next slide.

Joseph Murphy: Unless you need – we covered confidentiality notices enough.

Rebecca Edelson: No, I mean there are pros and cons to using them. It alerts people if they get something by accident it may have something of value in it; otherwise, people may just delete it and not think about it. On the other hand, it is a reasonable means to protect confidentiality to tell people to return it.

Joseph Murphy: OK.

Rebecca Edelson: So let's go to the next slide.

Joseph Murphy: All right, and that's an email policy.

Rebecca Edelson: One of the things you want to consider is not allowing employees to send confidential information to their home email accounts. The reason for this is because the company can't monitor for misuse if it's in the home email account. The reason to let them do it is for convenience. It's just something to think about it. If you're going to allow employees to email trade secret documents, you may want to consider employing a cleaning tool, and there's a site on the slides as to a possible one you might be interested in.

Joseph Murphy: I see, and that's the remove hidden data tool that removes the so-called metadata from the Microsoft Word documents that we all send to our friends and opponents alike.

Rebecca Edelson: Exactly. Exactly.

Joseph Murphy: And it's free, and that's a – that's a good tip too. With just – with just seven minutes left, I'm going to take the liberty of interstitially asking some of the

questions as we go along here. I'm getting a number of questions here, and I'd like to throw it out to Bec and Frank about, "What do you mean by don't overreach on when your various (NDAs), and what is the risk of not marking everything confidential?"

Frank Burke: I think, Joe, that some of those points, you had a very recent experience with in an – in an arbitration, and I think we added a few of those points as words to the wise from your unpleasant experience with some arbitrators, who wound up effectively negating many of your (NDA) agreements because they found that they were overbroad. Maybe you could kick in some information on that.

Joseph Murphy: Well, OK, I'll bare my soul here. I almost thought we couldn't talk about this straw, but sadly we can. Briefly, my company had two cofounders leave, take information, violate their non-competes, violate their confidentiality agreements and so on. I have said to many people they are – these agreements were drafted in the past, and they were layered upon by non-lawyers with more and more penalties. They were very draconian, they were very heinous, they were – they were offensive to read. They were – they were an affront, and the court was progressively in dismay by that, and even though it saw that the defendants had not been choirboys and had done some sneaky things to avoid the agreements, they found the agreements so horrible that they declined even to blue pencil them, and they rather felt that they should just set them free, that they'd suffered enough in the year-and-a-half they'd been under the litigation.

So I guess, questioner that is the danger. If you put too much, you look like the boy who cried wolf, and another thing that looks confidential, and also, you end up generating sympathy for the thief. So it's almost like brutalizing a witness on the stand. I guess you – Bec and you trial lawyers I know will have to sometimes pull your bunches.

Rebecca Edelson: Yes, a lot of times, you'll see an agreement. Everything you possible come into in contact in connection with your employing is confidential and you're not allowed to use it. I mean there's a lot of public information you come into a contact, and so instead of enumerating what the truly confidential information is, people will just say everything, and you'll have a judge, an arbitrator, whoever is the fact finder, finding that is just overreaching, and I'm not going to enforce that. It's against public policy to not let people talk about things that are perfectly public.

Joseph Murphy: All right, and I've learned that all too well, and the scars are still healing. One of the things I'm sure we all know, that in ACC we're all here for each other. To those of you on the call who have not yet joined ACC or the IP committee, I encourage you to join because then, you know, Frank and Bec and myself have shoulders to cry on when things go wrong. And on the – on the subject of being laws ourselves, we have a question as to whether there have been any cases in these areas – any of these areas that involved a law firm?

Someone running amok. I think we once said one of the tobacco companies sued informants was a law firm, but are these frequent involving law firms, or is there at least that last bastion of decency?

Rebecca Edelson: No, I mean there are cases with law firms. I think you'll recall a case where a paralegal of a law firm emailed information that he or she shouldn't have to opposing counselor, or something like that. I can't remember what it was. But certainly, law firms know all about the need for confidentiality. In fact, often you're not dealing with trade secret information; you're just dealing with confidential information of your client for reasons having nothing to do with trade secret protection.

Joseph Murphy: If it's a real secret, you know he's late for his appointment because his mistress kept him over, or what not.

Frank Burke: Hey, Joe, there's one point I wanted to make before we – it looks like we're down to the last minute or two, which is the instant message point.

Joseph Murphy: Oh, yes, please. This is very good. Frank read out a point that was news to a lot of us, including myself, and that is that unlike email, which has embedded in it addresses and headers and ways to track where it has gone, where it's been, IMs don't have that. Say, please, a few words about that, Frank.

Frank Burke: Yes, if you are in a situation, a company environment, where you have the need to protect your trade secrets, and part of the aspect of closing the backdoor as well as the front door is to strongly consider blocking the use of instant messages—Google, AOL, IM – AIM and the like. The problem is that these things come in like a cloud and go out like a cloud. They don't leave any footprints, and the securities industry has had to deal with this because they're required to keep records of communications, all communications with customers for three years, and a category of software has risen to try recognizing that in some environments it may be impossible or impractical to block the use of IMs. It is actually possible to manage them, and there are software environments which will track and manage and keep a record of instant messages coming in and going out. If you – if you don't use one of those methods, either blocking or tracking, you run a grave risk because an instant message is an electronic container ...

Joseph Murphy: And so you're saying that if I – if I can remember the end there, people can risk attaching the file to their instant message and sending it out. Even if you've prevented that with emails, they can do it with their IM.

With like two minutes left, I'm going to have to grab the microphone and just remind everyone thank you for attending and thank you for your questions. We won't be getting to anymore questions, I believe. But I do want you to know that there are more materials on this subject that Steptoe & Johnson has prepared,

very helpful, that are available on the links on your screen. I want to give you a brief overview of what they are. There are more lists about practical tips that you can use to protect your trade secrets when using web sites. Bec Edelson has compiled a number of those on slides, and Frank has also given a good list of what protections can be used with computer and digital information, your classic shrink wraps to more exotic methods.

Frank has also told us some protections that can be used with private chat rooms and blogs, which is a whole other area of nightmare that could probably take a conversation in and of itself, and I think, among the most citable things is – the slides also – Frank has added some more details on the CFAA. This looks like it could be a secret weapon for some of us that are out there with these thieves, because no matter how esoteric—was it secret, was it not—did they use a computer, you know. How did they get it, and you can hang them on that.

So with that – with that rush closing, I'm so sorry we have to say adio for the day. We thank you for joining this web cast. We encourage you to enjoy the (AACCIP) Committee, and we especially want to thank Steptoe & Johnson for providing us with Rebecca Edelson and Frank Burke and their expertise to speak with us today on this topic.

Thank you.

END