4-9-2021 11:10 AM

7D Competition & Four Concurrent Sessions. Trade Secrets

Jan-Diederik Lindemans

Richard Arnold

Courtney Cox

Victoria A. Cundiff

Sharon K. Sandeen

Emily C. & John E. Hansen Intellectual Property Institute

TWENTY-EIGHTH ANNUAL CONFERENCE INTERNATIONAL INTELLECTUAL PROPERTY LAW & POLICY

Friday, April 9, 2021 – 11:10 a.m.

SESSION 7: COMPETITION & FOUR CONCURRENT SESSIONS

7D. Trade Secrets

Moderator:
Jan-Diederik Lindemans
Crowell & Moring LLP, Brussels

***Speakers*:**

Richard Arnold
UK Court of Appeal, London
Trade Secrets and Conflicts of Laws under the Trade Secrets Directive

Courtney Cox
Fordham University School of Law, New York
Deceptive Precautions

***Panelists*:**
Victoria A. Cundiff
Paul Hastings, LLP, New York

Sharon K. Sandeen
Mitchell Hamline School of Law, Saint Paul

* * *

JAN-DIEDERIK LINDEMANS: Welcome everyone, on my behalf, to the trade secrets session of this year's conference. My name is Jan but if you want to make it very complicated, you can call me Jan-Diederik, and if you want to make it very simple, you can just refer to me as JD. Besides being an IP and trade secrets litigator at Crowell & Moring in Brussels, I will also be your host for today's session as well as the moderator of our very esteemed speakers and panelists that we have here with us today.

Unfortunately, I have failed to figure out in time what the exact order is in which I need to present my panel to comply with international protocol and

etiquette, so I won't complicate things and just go as they are mentioned on the program.

First, we'll have the pleasure of listening to Lord Justice Richard Arnold, who has been the IP judge in the UK Court of Appeal for about a year-and-a-half if my information is correct. Prior to that, Lord Justice Arnold was, among many other things, the judge in charge of the Patents Court. Lord Justice Arnold's talk is based on a ruling that was handed down quite recently in the UK, in the case, Celgard v. Shenzhen Senior Technology Material. That would be the UK decision. For the people that are unaware, there's also a US chapter that I assume will be discussed by some of our other panelists. In the UK decision, the courts took an interesting approach on the choice of law in trade secret proceedings under the Trade Secrets Directive.

Next, we'll have Courtney Cox, who is an associate professor at — and I've seen that Hugh is here so — she's an associate professor at "the best law school in the world." Her research focuses on the intersection between IP and philosophy, and in the past years, in particular, she has focused on the use of misrepresentations to mitigate trade secrets laws. At the risk of over-simplifying the topic that she will be discussing today, she will actually be addressing something that my children do all the time, and that is lying as a reasonable measure to keep something secret.

The audience today, as explained, should not hesitate to use the Q&A section or to raise their hands in true Fordham style to interact with the panel. I'm also hoping that our other panelists will be frank and share their views about what will be discussed. If I take into account the warming-up exercise that we've been doing the past couple of days via email, then I'm convinced that this will be the case.

Those of you that have attended the Trade Secrets session in prior years will know Victoria Cundiff very well. She's a well-informed, well-versed litigator who heads the trade secrets practice over at Paul Hastings. I was about to say "Here in New York," but obviously, she might be in New York, but I'm stuck behind my computer in Brussels.

Last but not least, it is a pleasure to introduce Professor Sharon Sandeen. She's the director of the IP Institute at the Mitchell Hamline School of Law in Minnesota, who also, not so accidentally, actually happens to be an international authority on trade secrets.

I believe with that, my five minutes that I have are used up and I would like to invite Lord Justice Arnold to take the virtual floor.

RICHARD ARNOLD: Good morning everybody, or good afternoon depending on where you are. As Jan said, I'm talking about this case, *Celgard LLC v Shenzhen Senior Technology Material Co Ltd* [2020] EWCA Civ 1293.[1] Just a quick skim through the facts. Celgard, incorporated in Delaware and based in North Carolina, manufactured dry batteries separators used in lithium-ion batteries for use in electric vehicles. They had an employee called Dr. Zhang from 2005 to 2016, who was said to have had access to a large body of trade secrets concerning these separators.

[1] Shenzen Senior Technology Material Co Ltd v Celgard LLC [2020] EWCA (Civ) 1293 (Eng.).

They had a competitor called Senior located in China, in the separator market. When Dr. Zhang left Celgard, he told them that he was going to work for GE in California in a completely different field, but in fact, he went to join Senior in China in 2017 and worked under a false name. Interestingly, that was common ground. What was not common ground was that, according to Celgard, when they found this out and asked him what he was doing, he told them that he was working on different technology, and that was untrue.

At the point where the litigation started, Celgard thought it was on the point of concluding a contract with a UK manufacturer of batteries, and it discovered that the UK customer might be starting to evaluate the suitability of separator film manufactured by Senior. They therefore issued a claim for misuse of trade secrets in England.

They applied for two things, firstly, permission to serve the claim form on Senior outside the jurisdiction, because of course, Senior is in China, and they therefore needed the permission of the court to do that. Secondly, they asked for an interim injunction, a temporary injunction, to restrain Senior from importing the battery separator film in question that they were offering to the UK customer into the UK or marketing it here.

Pending an effective hearing of the applications, they obtained a temporary order. There was an interesting aspect of the litigation there, because there was some misleading correspondence about the shipment from Senior. It subsequently transpired that the film had already been delivered to the UK customer before the order was granted and therefore it wouldn't have been subject to the order, but happily, the UK customer agreed to deliver it into the custody of Celgard's lawyers, so no harm was done.

Now the principal claim that was advanced by Celgard in this case was that Senior was liable for importing into and marketing, or threatening to market, in the UK battery separators whose design, characteristics, functioning and/or production processes benefited significantly from Celgard’s trade secrets, which Senior had unlawfully acquired and used.

The judge at first instance granted Celgard permission to serve out of the jurisdiction and he granted an interim injunction. There was then an appeal to the Court of Appeal. One of the key points on appeal was that Senior argued that the judge was wrong to conclude that the applicable law was English law, and he should have held that the applicable law was Chinese law. The Court of Appeal dismissed the appeal, holding that it was probable that the applicable law was English law.

Now, we need to look at two European pieces of legislation here. First of all, the relatively new Trade Secrets Directive.[2] This contains various definitions in Article 2,[3] one of which is this definition of infringing goods on the slide. It means “goods, the design, characteristics, functioning, production process, or marketing of which significantly benefits from trade secrets unlawfully acquired, used, or disclosed.” Note that word, “unlawfully”.

[2] Directive 2016/943, 2016 O.J. (L 157) 1 (EC).
[3] Directive 2016/943, art. 2, 2016 O.J. (L 157) 1 (EC).

Then in Article 4,[4] we've got various substantive provisions of which the key ones for present purposes are paragraphs three and five. Three says that the use of a trade secret shall be considered unlawful where the person in question has acquired the trade secret unlawfully. Again, note that word, "unlawfully."

Then paragraph five says that the production offering or placing on the market of infringing goods or the importation, export, or storage of infringing goods for those purposes shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew or ought, under the circumstances, to have known that the trade secret was used unlawfully within the meaning of paragraph three. This is a really interesting provision because it's an intellectual property-type provision in a trade secrets law.

The other piece of legislation we need to look at is the EU legislation which regulates conflicts of laws, and this is the Rome II Regulation.[5] We start with Article 6[6] that tells us that the law applicable to an act of unfair competition shall be the law of the country where the competitive relations are likely to be affected. Trade secret misuse is an act of unfair competition, so we're within Article 6, but then paragraph two of Article 6 says that where it affects exclusively the interest of a specific competitor, then you apply Article 4[7] and we're in that scenario. Article 4, paragraph one says that the law applicable to a non-contractual obligation arising out of a tort shall be the country in which the damage occurs.

Those are the two pieces of legislation we have to apply to this situation when answering the question, "What is the applicable law?"

Celgard's case was to say that Article 4 (1) of Rome II led to English law being the applicable law because the direct damage caused by the wrongdoing it complained of had occurred and would, if not restrained, continue to occur in the UK, that being the country into which the infringing goods, namely the shipment to the UK customer and any future shipments of the same separator, had been and would be imported, causing damage to Celgard's market here in the UK.

By contrast, Senior said that Chinese law applied because confidential information, and trade secrets are a species of confidential information, was intangible property, and damage to intangible property was located at the time and place it became irreversible. One of the arguments they put forward in favor of that analysis is that it gives you a single applicable law.

The Court of Appeal rejected Senior's argument for a number of reasons including the following. Firstly, confidential information was not property. Secondly, there was no need to locate the direct damage in a single country because the explanatory memorandum that was promulgated by the Commission when the Trade Secrets Directive was proposed envisaged the distributive application of the laws of each country where direct damage was sustained.

Next, the act of unfair competition was the importation into and marketing in the UK of infringing goods. The fact that they were manufactured in China was immaterial, and Senior's argument would favor the application of laws of countries

[4] Directive 2016/943, art. 4, 2016 O.J. (L 157) 1 (EC).
[5] Commission Regulation 864/2007, 2007 O.J. (L 199) 40.
[6] Commission Regulation 864/2007, art. 6, 2007 O.J. (L 199) 40.
[7] Commission Regulation 864/2007, art. 4, 2007 O.J. (L 199) 40.

with weak trade secrets protection, contrary to the purpose of the Directive. However, the court asked the parties a question, which they hadn't thought about themselves, which is, what about Article 4(5)? What law do we apply under Article 4(5) of the Trade Secrets Directive to determine whether the secret was acquired unlawfully?

When we asked that question, we got quite different answers from the parties. Senior said, "Well, look, it talks about where the trade secret was unlawfully acquired. That must involve application of the law of the place where the trade secret was allegedly acquired, here China, because that's where Dr. Zhang was, and it was therefore an implicit choice of law rule."

Celgard said, "Well, there's two possibilities. Either it must be an autonomous interpretation of the Directive, and that leads to EU law being the relevant law or alternatively, if it's got to be some national law, then you apply the law under Rome II."

The provisional view taken by the court, on which it wasn't necessary to reach a final decision, was that the applicable law was the one indicated by the third of those answers, namely, it's the law you determine applying the Rome II Regulation. In favor of that were really three main reasons. Firstly, there was nothing in the Trade Secrets Directive to indicate it was intended to include a choice of law rule, whereas that was the function of the Regulation.

Secondly, it was doubtful that the applicable law was EU law, because EU law wouldn't really give you a complete answer. You need a national law, and the Directive is full of references to national law. Lastly, it was doubtful that it was consistent with the objectives of the Directive to apply the law of the country of acquisition if that was different to the law determined by the Rome II regulation.

That's a whistle-stop tour through that decision. I hope to take some questions.

JAN-DIEDERIK LINDEMANS: Thank you, Lord Justice. I see that in the Q&A there's no questions, so let me make a small observation as an introduction to maybe some feedback that we might get from our panelists.

In the ‘confidentiality club’ that we created these past few days among ourselves, I admitted that I never read Article 4(5) of the Directive in relation to the choice of law discussion. For me, it was always a provision that the European lawmakers included to give some extra punching power to the trade secrets holder, to which then Professor Sandeen candidly replied that she actually saw the exact same provision as the cradle of what, according to her, was “a new wrong” in European trade secret matters. I found that very interesting and I thought if she maybe could share that view of hers with the public, which might then trigger some questions.

SHARON SANDEEN: Thank you very much. It was noticeable to me that it's a new wrong because historically, looking at trade secret law through the lens of US law, which of course has since been used as the driver of international harmonization efforts, what we've traditionally thought about as wrongs under trade secret law are wrongful acquisition, wrongful disclosure and wrongful use. What you have now is a list of other things that could be wrongful under Article 4(5) of

the Trade Secrets Directive, including wrongful production, offering for sale, placing for sale, importation, exportation, and storage.

When you read Article 4(5), I think one of the big questions is: "What is the requisite state of mind of the defendant when they're engaging in any of those behaviors?" It seems to point back to the other provisions of that particular article, particularly I think Article 4(4). We have to consider what the defendant needed to know and when they needed to know it.

I think that's a problematic issue, not just in interpreting that provision, but also from a policy point of view because what I'm concerned about is shopkeepers, as I called them in our exchange, becoming liable for trade secret misappropriation just because they get a cease-and-desist letter, even though they weren't actually involved in any act of what we would consider trade secret misappropriation.

JAN-DIEDERIK LINDEMANS: Thank you, professor. You will understand that even though I work for an American law firm, when I heard your concerns, you actually, in my view, had a quite conservative view of what the extraterritorial application of US laws should be or the international jurisdiction of US courts. I understood from Vicky that the answer is more nuanced than my view. Maybe, as you enlightened me, Vicky, you could also explain a little bit to our public what your more nuanced opinion is there.

VICTORIA CUNDIFF: Sure, thank you. I think this whole dispute does underscore the importance that trade secret owners who face misappropriation in international markets may need to be pursuing lawsuits in multiple jurisdictions. What is quite interesting is that the same parties plus some additional ones have been involved in two lawsuits in the United States relating to essentially the same facts as Justice Arnold noted in his presentation.

Celgard is based in North Carolina and at least part of their argument was that the lead individual defendant had acquired trade secrets in North Carolina, which he then dispersed allegedly through subterfuge back to China where they were used to produce goods that were exported throughout the world.

In the United States, there would be a couple of routes to potentially remedy the wrongdoing. One is under the Defend Trade Secrets Act,[8] which does provide the possibility of substantive claims in the United States under the US law for acts of misappropriation that took place primarily abroad, so long as acts in furtherance took place within the United States. However, there is still a need to secure jurisdiction over all of the defendants.

In the California case, some of the goods had made their way to shopkeepers, as Sharon would refer to them, and the pleadings were rejected. The case was dismissed because, at least as to the shopkeepers, there were no plausible allegations that they knew or should've known of some misappropriation, or that the corporate defendant had in fact directed that those goods go to particular sellers in California.

I think I would disagree actually with Professor Sandeen's observation that Section 4(5) is a new wrong, and we can discuss that in due course. But under US law, one possibility would be the assertion of an [inaudible] trade commission, which is an *in rem* claim against the importation of goods into the United States

[8] Defend Trade Secrets Act, 18 U.S.C. § 1836 (2016).

made through acts of misappropriation that, under US law, would be found violative of US law.

In fact, even if US law may conflict with, for example, the law of China, an importation order can be entered in the US. The problem is that because of the labor intensity of bringing such proceedings, only about ten of them that deal solely with trade secrets have been brought each year in recent years. They can be extraordinarily powerful remedies, however.

JAN-DIEDERIK LINDEMANS: The basic understanding is that you can also combine them with patent claims, if need be, to make them more efficient?

VICTORIA CUNDIFF: Yes. Courtney's back, so Courtney.

COURTNEY COX: I'm so thrilled to be here. For this project, or part of it, one of the early hooks that I found for a suspicion that I had was actually in one of Vicky's papers. It's a niche issue, but it's growing.

There's lots of case law about the use of lies by trade secret defendants. We saw some of that in Lord Justice Arnold's talk about defendants who misrepresented who they are at some point in the process and used that kind of subterfuge in order to gain access to trade secrets. There's been a lot of really interesting philosophical work lately on lying, on the wrongs that are associated with lying, and also on conceptual questions about what lies are.

Some of that got me thinking, "Well, gee, as Jan-Diederik, suggested, what about using a lie to protect information that you don't want to share?" Maybe it's your kids who are lying to each other or an overly inquisitive mother-in-law. When you're asked directly, what can you do about protecting it?

Within trade secrets law, there's this reasonable precaution requirement under American law. It appears in the UTSA,[9] and it appears in the DTSA as part of the definition for what it is to be a trade secret. The requirement is simply that a trade secret owner have taken reasonable precautions in order to protect their trade secret. For those who are out there who are litigators, it's a case-by-case, fact-specific kind of inquiry.

Sometimes it involves cost-benefit analysis. It's rarely decided as a matter of law except for certain kinds of precautions that have become really standard like nondisclosure agreements. Now with everything moving online or technical, passwords are another thing that we're seeing in the case law where you'll be found to have failed to satisfy that requirement if you didn't at least take those basic precautions.

Usually, it's more about a suite of precautions, so the nondisclosure agreements plus certain kinds of access controls, both physical and technological. To a certain extent, certain kinds of notice that you might provide to employees or collaborators, that "ubiquitous, confidential, or proprietary information" that we see stamped on a lot of things.

There's some theoretical disagreement among scholars about exactly what role this is supposed to play, but certainly, it serves many useful functions. It's evidence that the information was treated as a secret, that it was taken by improper means, and that it had some value because effort was taken and maybe some evidence of what exactly that value was as a function of the security precautions.

[9] Unif. Trade Secrets Act. 14 U.L.A. 433 (1985).

Recent scholarship has really been focusing on the notice function of it, in so far as we're thinking of trade secrets as a proprietary interest.

My work began by asking, "Well, what about a lie?" When I started asking people about it, it's interesting, you've got polarized reactions. But one of the dominant ones was, "Oh, that's fraud. You obviously can't lie in order to protect your proprietary information." I thought, "No, no, no. Of course, a court's not going to call it that. They're going to use a different term."

When you start thinking about it that way, the examples pop up. Deception has a long history in IP both in this country and elsewhere: the use of mountweazels and data sets, fake data in a data set in order to catch somebody that has copied your data set, fake doors, code names for projects, and canary traps of a more traditional kind. Those have been increasingly used in cyberspace.

If I could show you my slide, I could show you some of the great headlines in advertising, because not only is this gaining traction, but actually, it's being rebranded as deception technology. There was a headline in an industry mag back in September, "MITRE Shield Shows Why Deception Is the Next Big Thing in Security." Some of the cybersecurity companies that are building some of this deception technology — a company called "Illusive" boats of over 75 deceptive techniques that you can use to identify both internal and external would-be-misappropriators on your network in order to catch them and watch them. You fill out the form and learn more about how deception can help you protect your company's information.

Most of this is using different kinds of honeypots, so a decoy computer network or a network system designed to attract hackers that's isolated from the main system. Some of the more sophisticated kinds of laying traps throughout the actual internal system, this is what Illusive and MITRE and other companies in this space at least represent that they're doing, by leaving fake trails of information. The passwords that might be inadvertently saved by your web browser, they plant fake passwords.

This is all very interesting but what does it have to do with lawyers? Well, it's starting to appear in case law. We're starting to have some early harbinger cases here in the US. One big one — all right, it's not so big — is SolarCity v. Pure Solar Company.[10] It was in the US District Court for the Central District of California. There, you see it talks a little bit in the denial of the motion to dismiss, but if you dig into the pleadings, what happened to SolarCity was they had an internal employee that they believed was selling customer information to a competitor. In the process of investigating this, they built a honeypot, they built a decoy system.

When the internal employee was trying to take the information, the system would give them a decoy phone number. He was then passing along these decoy phone numbers to Pure Solar. Pure Solar representatives were making calls to these customers on the decoy phone lines, and there was a setup receiving line to receive these calls and then basically pretend to be these customers so they could pump out as much information about who Pure Solar was and try to figure out exactly why they were getting these phone calls.

[10] SolarCity Corporation v. Pure Solar Co., No. CV 16-01814-BRO (DTBx), 2016 WL 11019989 (C.D. Dec. 27, 2016).

In the pleadings, the company explained this use of the decoy phone numbers and then in the causes of action under the DTSA and UTSA identify the development of the system as satisfying the reasonable precaution requirement under both the California UTSA and the Defend Trade Secrets Act. Then the court in ruling on the motion to dismiss — the satisfaction of the RPR[11] wasn't really challenged — the court accepted it and the parties seemed to both accept that some of these measures were obviously sufficient, but the court did find it quite useful evidentiary.

In some of the same functions that I talked about the RPR just a second ago, it found that they established misappropriation during the requisite time for application of the DTSA, so the honeypot was really useful for establishing that timeline. They also found it as establishing loss, as establishing the cost of creating this honeypot as establishing a measure of the value of the trade secrets that were taken, not just for the trade secret causes of action, but also for the application of the CFAA,[12] which has a minimum amount in controversy of $5,000 in the court.

This is limited, this is an early case. I anticipate, although I'd be interested in hearing what my fellow panelists have to say, that this may be an increasing phenomenon. It doesn't particularly serve the notice function of the reasonable precaution requirement as we were discussing by email, and I'd love to get into that a little more. But it does seem to serve all of these other evidentiary purposes of the reasonable precaution requirement as well as other elements for related causes of action that might arise in these cases. I'll leave it there. I see the time that has gone, and we can discuss some of the other implications in the conversation.

JAN-DIEDERIK LINDEMANS: Thank you, Courtney, also for respecting the time. That actually was not just an original talk, but also quite inspirational for me as a litigator to go into some of those techniques. While you were talking, I saw that Professor Sandeen was nodding a lot, and I don't know whether that was because she wanted to say something or react to something that you said or whatever she was preparing to rebut to something that Victoria said earlier. I'll leave it up to her to surprise us with what she would like to say.

SHARON SANDEEN: Yes. First of all, let me thank Courtney for her paper and her presentation. I think I can speak for Vicky too to say that as people who've been engaging in trade secret scholarship for decades now, we are very excited to see a lot of newer scholars enter the field with such interesting, new ideas. My response, however, would be this: It's not so much about trade secrets, per se, but it's about how companies and information technology people and information security people look at information differently from how lawyers look at it. This is exactly why lawyers need to be involved in advising companies about information security.

What happens in information security is the focus is on actual security, absolute security. This is what would be the ideal for anybody trying to protect information held by a company, whether it's a trade secret or not. Then the next

[11] Reasonable precaution requirement.

[12] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).

focus is on having reasonable security to meet GDPR[13] requirements and similar laws on a privacy front. But these efforts may not suffice for trade secret misappropriation purposes for the reasons you indicate, Courtney, because there is this very important notice function of the reasonable efforts requirement.

The way I like to describe it is: imagine if you take the three requirements of trade secrecy that exist in the US, and now in the EU and that aren't set forth in the TRIPS agreement,[14] and you ask your question, "Okay, the information has to be secret, not generally known or readily ascertainable. It has to have commercial value because it is secret. And then there's this third requirement of reasonable effort. If the information is already secret and already has value, why do we have a third requirement?"

I think the most powerful argument is because the efforts have to put on notice the person and companies that you want to be under an obligation to maintain the secrecy and confidentiality of that information. I will add that that's particularly important in the United States, and in other countries that are under pressure from the United States, notably, for instance, Canada, who just changed their laws, where there's an imposition of criminal responsibility for trade secret misappropriation.

I for one do not want a law where I can go to prison, federal prison, and never be told what it is that I'm supposed to keep confidential and secret. That's why I tend to highlight that particular requirement at least when it comes to trade secrecy. Thank you.

VICTORIA CUNDIFF: I would make a couple of observations including one literal observation, which is that my apartment is right across from Fordham Law School. I am seeing the beautiful magnolia tree and full bloom that we have often gathered under in the past and hope to in the future. This discussion is provocative, and I think that we might profitably divide it into two parts. One is, as Sharon notes, the actual desire to protect the trade secrets, that's the "lock" aspect. If you lock it up, people aren't going to be acquiring it.

It sounds like some of the procedures that were utilized in the SolarCity case that you described were directed to that end about, "We know somebody is trying to ex-filtrate our trade secrets, let's make sure that he's not able to do it." But to prove misappropriation, as Sharon notes, you must present that the person knew or should have known that the information was intended to be kept secret.

I think the notice function, I'm not familiar with the full details of that case, but presumably, the evidence would have shown that the defendant knew that the information was intended to be secret. That's why, in fact, they were trying to acquire it, rather than by searching for it on the internet or by going to the owner of the information. It's almost like a sting operation that was set up because the defendant knew the information was information that he shouldn't be trying to develop. The company was using stealth help to ensure that he didn't.

---

[13] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[14] The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Apr. 15, 1994, 1869 U.N.T.S. 300.

We've talked about other situations. It turns out there are apparently multiple scenarios where a company's source code has been somehow stolen and then is being offered on the internet in a very sketchy way that it's like, "Oh, here's the source code to pick your favorite major thing." To try to remedy that problem, sometimes the proprietor of the actual source code may flood the market with other sketchy offers about, “Oh, get your stolen software here.” All of the people who are trying to access it think they're getting stolen software, and maybe they are not because it's been able to be camouflaged.

Nonetheless, at the end of the day, to prove the case, the plaintiff will have to show that as to the original misappropriator, that they knew or should have known that the information was secret. A remedial measure of trying to camouflage what has happened may be useful, but it doesn't substitute for establishing liability on the part of the first misappropriator.

RICHARD ARNOLD: I just wanted to add two more dimensions to this discussion because I agree with what Sharon and Victoria have both said. But two distinctions I would introduce at this point are, first of all, when we're talking about reasonable precautions, I completely agree about this having a notice function. Of course, we mustn't forget that, in trade secrets cases, there are typically two scenarios. One is misuse by the employee or the ex-employee. You're trying to give notice to your employees and future ex-employees as to what they must regard as company property, as distinct from their own skill and knowledge, which they can take elsewhere. But then there's the external hackers. Of course, the role of reasonable precautions there is much less about notice in that sense, although it does have some function, it's more about why should the law help those who don't help themselves?

Then the other distinction I'd like to bring into this discussion is between what you're doing to create a protectable trade secret in the first place and then what you're trying to do by way of evidence gathering in circumstances where you suspect there's been misappropriation. It seems to me that a lot of what Courtney's talking about, and I'd be interested in her response, is really about evidence gathering rather than about how you create a protectable trade secret in the first place.

JAN-DIEDERIK LINDEMANS: [unintelligible] something and maybe we can have a conclusive remark. Very often in trade secrets litigation, submitting convincing proof is the biggest issue. When I heard you talking, I felt like there are some interesting ideas there to get access to proof.

COURTNEY COX: Yes, there are a few thoughts. The first is what function might these deceptions provide or serve? I agree with Vicky that one of them is the lock, keeping and identifying intruders and cornering them off into what looks like the system, but isn't actually a system. One of the interesting things about the use of them is they don't only serve the lock function, they also serve a safeguard function, recognizing that you have been breached, recognizing that further measures might need to be taken — this investigative purpose that Lord Justice Arnold is raising.

In the cases at issue here, the notice function is in some ways served by other precautions. I don't know if it makes sense to think of the deception as being,

"All you have to do is lie and your trade secrets are protected." No, this is part of a larger package of, “Have you done something reasonable?” It can evidence misuse by both the employee, the ex-employee and the external, that they were going in the facility where they weren't supposed to. That's part of this idea of leaving the trail of password data in — altering passwords, leaving fake passwords and logons that Illusive and some of the others claim to be doing.

It can also be used as basic training for your employees. While I was working on this, I received a lovely birthday present from Fordham IT in the form of a phishing simulation. “Dear, Professor Cox, your package has been delivered,” I’m like, “Oh, no, this looks like spam.” I reported it and they said, "Oh, thank you, nothing to worry about here." I was like, "What do you mean nothing to worry about here?" and they said, "Oh, well, it's just a simulation."

Sharon, I think I saw you tweeted out about something similar that happened at your university. As these become more common, I think there's a question of, if your entity failed to take even these basic ones, have you done enough to protect — have you even taken bare bones minimum reasonable requirements to prevent things from falling into the public domain as needed to satisfy some of these requirements?

JAN-DIEDERIK LINDEMANS: I actually agree. Training is probably one of the most efficient, reasonable measures you can take to keep your secrets safe.

COURTNEY COX: But it requires lying to your employees in this new context. Sharon, I think you said you had gotten in trouble when you notified your colleagues?

SHARON SANDEEN: What happened is my school hired a consultant to help us stop phishing attacks and they advised us to send out phony phishing requests. I got in trouble because I was supposed to click a button that said it's a phishing attempt rather than what I did, which was to notify all my colleagues, "Don't click on this because it's a phishing attempt," which was an interesting information security process, because they're basically socializing us to click a button rather than advise the whole entity, which I thought was totally bizarre, but anyway.

VICTORIA CUNDIFF: That way, they can assess whether it's a genuine threat or not. We have that button too. Sometimes you get these emails from people you don't know, and you're not sure. Then they can look at it through various scanning devices and report, "Yes, it's malicious software,” or, “No, it seems okay, but still be careful."

COURTNEY COX: I think they handled some of that problem at Fordham. There were multiple different kinds of this phishing email that went out. Even if I had shared it with the rest of the faculty, that wouldn’t have destroyed the simulation for everyone. But I would have thought notifying people is also helpful.

JAN-DIEDERIK LINDEMANS: Speaking of destruction, you may have noticed that unlike in a ‘live setting’ at Fordham, there are no bombs here that go off when we go over time. The previous panel went well over time. We're doing the exact same. I know that there's a virtual lunch break scheduled now. We've eaten some of that time already. I would like to thank all of you for a very interesting pre-discussion and discussion today.