1-1-2017

Understanding the Defend Trade Secrets Act (DTSA): The Federalization of Trade Secrecy

David Green

James Pooley

Elizabeth Rowe

Ryan Calo

SYMPOSIUM

UNDERSTANDING THE DEFEND TRADE SECRETS ACT (DTSA): THE FEDERALIZATION OF TRADE SECRECY[1]

David Green

James Pooley

Elizabeth Rowe

Ryan Calo, moderator

Loyola of Los Angeles Law Review is pleased to inaugurate our "symposium discussion" series in which leading experts are invited to engage in an evening symposium on a new or emerging area of law. The subject of our first evening symposium was the Defend Trade Secrets Act (DTSA), a federal statute signed into law on May 11, 2016[2] that creates a federal civil cause of action for trade-secret misappropriation. The DTSA marks a significant federalization of trade secrecy law, giving companies the opportunity to protect against and remedy misappropriation of propriety information in federal court.

Prior to the DTSA's enactment, companies were essentially forced to bring trade secrecy claims in state court unless there was diversity jurisdiction; such diversity jurisdiction is rare in trade secret cases because, as one of our panelists, Mr. James Pooley notes, trade secret cases tend to have local actors. Because trade secrecy protection was a matter of state law, there has been a lack of uniformity in substantive trade secrecy standards, statutes of limitations, and

1. Please cite as *Symposium, Understanding the Defend Trade Secrets Act (DTSA): The Federalization of Trade Secrecy*, 50 LOY. L.A. L. REV. 331 (2017).

2. Defend Trade Secrets Act, Pub. L. 114-153, § 3(a)(1), May 11, 2016, 130 Stat. 382 (codified as 18 U.S.C. § 1832, et. seq.).

remedies. The DTSA now provides companies the option of filing suit in federal court through a uniform federal statute.

But as with most new law, there are many unsettled issues, disagreements about the likely impact of the law, and much to be developed as the law is tested in court. To shed some light on the DTSA and the increasing importance of trade secrecy protection, the symposium panelists were:

- DAVE H. GREEN – Mr. Green is currently Assistant General Counsel in Microsoft Corporation's Intellectual Property Policy Group, counseling in the areas of copyright, trade secret and intermediary liability. He was previously Assistant General Counsel for Corbis Corp. and, prior to that, Assistant Attorney General to the University of Washington, advising on complex IP and licensing, privacy, and business matters. Mr. Green is a co-founder of several private companies which produce entertainment projects, including McQueen Racing (in partnership with the family of actor Steve McQueen) and Zero Point Ventures (in partnership with the Albert Einstein estate).
- JAMES POOLEY – James Pooley has practiced intellectual property and technology law in Silicon Valley since 1973, with the exception of the period from 2009 to 2014 when he served as Deputy Director-General of the World Intellectual Property Organization (WIPO) in Geneva. Mr. Pooley is the author of the law treatise TRADE SECRETS (1997, 2017) and the book SECRETS: MANAGING INFORMATION ASSETS IN THE AGE OF CYBERESPIONAGE (2015). He testified before the U.S. Senate Judiciary Committee in 2015 on the proposed, and now enacted, DTSA.
- ELIZABETH A. ROWE – Elizabeth Rowe is the Feldman Gale Term Professor in Intellectual Property Law at the University of Florida College of Law, where much of her research addresses the intersection of trade secrets with employment law and/or technology. Professor Rowe is co-author of the first casebook in the United States devoted to trade secret law, ROWE & SANDEEN, CASES AND MATERIALS ON TRADE SECRET LAW (2nd Edition,

2016) as well as the first "nutshell" treatise on the subject. Prior to joining academia, Professor Rowe was a partner at Hale and Dorr LLP (now WilmerHale) in Boston.

And our moderator,

- RYAN CALO – Professor Calo teaches at the University of Washington School of Law, where he is also a faculty co-director of the school's Tech Policy Lab, a unique interdisciplinary research unit. Professor Calo's recent scholarship has appeared in the *California, Columbia, George Washington,* and *Notre Dame Law Reviews.* A founder of the annual "We, Robot" conference that explores social, legal, and policy issues related to robotics, Professor Calo has been named one of the most influential people in the field of robotics by *Business Insider*.

RYAN CALO (MODERATOR): First we are going to hear from Jim. Jim, as Justin said, is intimately involved in this. I know you testified before the Senate just months before this law was promulgated and we would love for you to set us up and give us a sense of what this law does.

JAMES POOLEY: Ok. Thank you. I have a few slides a little later on when we dive into several of the detailed provisions that I think are most important, but for right now what I want to do is set the stage. We need to look back a little bit in order to know where we have come from and how the Defend Trade Secrets Act (DTSA) compares to what we had before. As most of you appreciate, the law on trade secrets in the U.S. was created by the courts.[3] It's part of our common law. That was true here and in Britain. Up until 1939, we really just had a collection of trade secrecy cases. In 1939 we got the first Restatement of Torts[4] and it included trade secrets as part of the provision on torts—part of the section that dealt with torts.[5] No one was very clear about where trade secrecy really fit, but that's where they put it at the time. When it came time to address the law in the Second Restatement

3. *See* Vickery v. Welch, 36 Mass. 523 (1837) (acknowledging the first known common law cause of action for the modern concept of trade secret law in the United States).

4. RESTATEMENT OF TORTS § 757 (AM. LAW INST. 1934).

5. *Id.*

of Torts,[6] they couldn't come to a decision, and so it wasn't covered in the second Restatement. Eventually it was in the third.[7]

But in the meantime, because people were concerned that the law wasn't moving forward and it needed a different approach than had existed in the 1939 Restatement, there was a push to create a uniform state law. So the commissioners on uniform state laws got a bunch of experts together and in 1979 they put out the first version of the Uniform Trade Secrets Act.[8] There was a second version in 1985,[9] which portended some changes that we would see coming later in the DTSA. But that was the state of play in the late 1970s.

I started practicing in the early 1970s and started doing trade secret cases because that's what there was to do in Silicon Valley as it was growing. The cases were local. And the issues were laid out on paper. In fact, it was through paper that you got access to information and you usually carried that information away by using the company's photocopier at night when you weren't supposed to be there, generating hundreds of copies and putting them in a box and going down the street to a new start-up. That was the typical way in which these cases played out.

Keep in mind that again, this practice was all state law-based. There wasn't so much a push for a federal law as there was a concern that following the end of the Cold War a bunch of government spies, particularly in Eastern Europe, had just been released into the system and were available for industrial espionage. And so there was a discussion about creating a law that would address this at the federal level and in the context of the criminal system. And that's what led us to the Economic Espionage Act of 1996.[10] That was the first federal law on trade secrets, regulating the behavior of people outside the government (there had been section 1905 of the *Trade Secrets Act*,[11] which basically made it a crime for any federal employee to release something that shouldn't be released).[12] That statute has existed for

6. RESTATEMENT (SECOND) OF TORTS (AM. LAW INST. 1965).

7. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (AM. LAW INST. 1995).

8. UNIF. TRADE SECRETS ACT (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1979) (amended 1985).

9. UNIF. TRADE SECRETS ACT (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1985).

10. Economic Espionage Act, 18 U.S.C. §§ 1831–39 (2012).

11. Trade Secrets Act, 18 U.S.C. § 1905 (2012).

12. *Id.*

the last 20 years. Now, there was a discussion at the time that perhaps there should be a civil cause of action added into that legislation, but it was all done very, very quickly in the summer of 1996. There wasn't enough time for the idea of a civil cause of action to be thoroughly vetted and discussed, so it went forward just as a criminal statute.

What's happened since then? Everything that used to be on paper is now digital and everything that used to be local—or many things that used to be local—are now cross-border. So over the last 20 years one of the things that we've seen, certainly industry has seen, is the increasing insecurity in the integrity of information that drives business. That insecurity is played out in fears about information being transmitted through networks on the Internet or in very small electronic devices that make that transportation of data very, very easy. And the actors that are involved in these kinds of activities come not just from down the street; they are often from other states and other countries. So, over time, the concern about the threat environment for information grew just as the value of information itself was growing. Owners of that information decided that the laws that we had and the procedures that we had to protect that information against theft and to pursue claims of misappropriation were basically inadequate. Why? In part because the state interpretation of the Uniform Act, by anybody's measure who actually went in and started reading and comparing state statutes, was not really very uniform.[13] At a certain level it was. There were concepts that were all the same. And most states got most of it the same as they enacted it, but it doesn't enjoy anything close to the uniformity of the Uniform Commercial Code.[14] And so, there were different rules. Substantive rules. Then you layer on top of that different procedural rules. If you had actors in one of

13. *See* Andrew Campbell, *The Federal Defend Trade Secrets Act*, TENN. BAR ASS'N, (June 1, 2017, 12:00 AM), http://www.tba.org/journal/the-federal-defend-trade-secrets-act ("Since its publication in 1979 and its amendment in 1985, primary protections have been found in the Uniform Trade Secrets Act (UTSA) as adopted by 48 states (all but New York and Massachusetts). But even among those 48 states, variations and nuances in the UTSA are common.") (footnote omitted); *cf.* Charles Tait Graves & Elizabeth Tippett, *UTSA Preemption and the Public Domain: How Courts Have Overlooked Patent Preemption of State Law Claims Alleging Employee Wrongdoing*, 65 RUTGERS L. REV. 59, 65 (2012) ("Notwithstanding its title, the UTSA has not resulted in uniform rulings when it comes to deciding whether the state UTSA preempts common law claims arising from the same conduct.") (footnote omitted).

14. *See* Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1649–50 (1998) ("[U]nlike the Uniform Commercial Code, the UTSA never won the support of all of the states, and even the states that did adopt the UTSA modified it, sometimes substantially, before enactment.") (footnotes omitted).

these misappropriation dramas living in other states, in order to get discovery (and that's very important in trade secret cases), you had to get letters rogatory issued from one court to another state and it took weeks sometimes to get the kind of information that you needed. And sometimes the level of inquiry that you were allowed would differ from one jurisdiction to the next. All this was a problem. You have an issue that has a nationwide, and often now, international scope, and state courts that were not really well suited to handle these kinds of cases. At least those that had that kind of characteristic.

Why not the EEA? The Economic Espionage Act was no panacea because it is a criminal statute.[15] On average, only seven to eight cases were filed per year over its 20-year history. Trying to get the government actually interested in taking on these cases was always a little bit difficult. I had that happen in my own experience—calling on somebody who was part of the high-tech crime unit for the Department of Justice, describing to them a case that seemed to me to be very compelling and the response being, "Well, have you looked at your civil options." So, even in cases where you wanted the government to get involved, you had to deal with their decision to take it on or not. And these cases are complicated. They're difficult to win. So sometimes they just wouldn't do it. And when they did, you had to give up control in order for your case to be handled.

So industry came to the conclusion there was, there is a simple answer to all of this: add a civil cause of action to the existing structure and framework of the Economic Espionage Act.[16] That's where the DTSA came in. It was introduced after some tries that didn't work. In the 114th Congress, in the summer of 2015, identical bills were introduced into the Senate and House adding a civil claim to EEA,[17] and, basically taking the position that there should be a choice. This shouldn't be a replacement. So, Congress is not really willing to address whether or not it made the most sense to preempt state law. Just proposed an addition to state law by making it an option for a trade secret owner, who has a claim, that might affect inter-state commerce in some way, to be able to bring it to federal court without

15. Economic Espionage Act, 18 U.S.C. §§ 1831–39 (2012).

16. *See* Robert B. Milligan, *U.S. Senate Passes Bill Creating a Civil Cause of Action in Federal Court for Trade Secret Misappropriation*, TRADING SECRETS, (April 5, 2016), http://www.tradesecretslaw.com/2016/04/articles/dtsa/new-year-new-progress-2016-update-on-defend-trade-secrets-act-eu-directive/.

17. H.R. 3326, 114th Cong. (2015); S. 1890, 114th Cong. (2015).

having to rely on diversity jurisdiction. And when you think about it, that's a fairly difficult limitation in trade secret cases because you so often have local actors involved in this, making it very difficult to create diversity. At least full diversity. So, we have this, additional cause of action there, there was some controversy around it.

Most of what was objected to in the statute had to do with ex parte seizure provisions that were written into the new law,[18] borrowed from the Lanham Act, where we had, for some time, and had some experience with the use of ex parte seizure as a way to grab onto counterfeit goods. It wasn't a really good fit for something as inchoate as trade secret rights, but there it was, and they wanted to do it, and they wanted to do it for a particular reason. And that is that companies wanted to have the ability, in a case where they knew ahead of time that something was either going to be taken out of jurisdiction, out of the country perhaps, or destroyed. To be able to go to court and get an order where the marshals could come in and seize the container for the information, or whatever it was, the disc drive, or what have you. And that had been a prospect in more than one case, not many, but enough so that it was deemed an important additional tool to have. Well, we spent most of our time debating whether that was an appropriate thing to have and whether or not the statute had enough protections built into it to prevent misuse of any type of ex parte seizure. At the end of the day, meaning where we are now, many months later, I, I think we can see that the provision, although its been requested a few times, it has not been invoked except in two cases,[19] one of which remains entirely under seal.[20] So, in the real world it has not had as much of an impact as we thought. At least not at this stage.

There are three other provisions of the statute that I wanted to cover here. One of these three issues I want to talk to you about is the whistleblower protection issue. This came up long after the statute was introduced into Congress. And actually after I had testified and while

18. *See* Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 WASH. & LEE L. REV. 284, 286 (2015).

19. Paul M. Mersino, *The DTSA's Ex Parte Seizure Order: The "Ex" Stands for "Extraordinary" (Guest Blog Post)*, TECH. & MKTG. LAW BLOG, (Feb. 1, 2017), http://blog.ericgoldman.org/archives/2017/02/the-dtsas-ex-parte-seizure-order-the-ex-stands-for-extraordinary-guest-blog-post.htm ("The first was issued by the Southern District of New York in *Mission Capital Advisors, LLC v. Romaka*, No. 1:16-cv-05878-LLS (S.D.N.Y. July 29, 2016).").

20. *Id.* ("It has also come to the author's attention that an application for ex parte seizure was granted by a federal court in Florida in October 2016. To date, unfortunately, all information has been held under seal and is not yet public.").

they were considering amendments. An article that had been written by Professor Peter Menell from Berkeley, on the sad state of protection for whistleblowers that exists under current trade secret law,[21] influenced the senators who were working on this statute to draft a provision that would address the problem of the employee who works at a place under confidentiality restrictions but finds evidence that a crime might be, be committed, or some other wrongdoing happening, and wants to be able to report it to law enforcement.[22] You may be surprised to learn that there never has been any very specific protection in trade secret law that would cover that kind of behavior and exempt it. A few courts had talked about it as a public interest kind of thing,[23] but it hadn't been made explicit enough that employees in that position, whistleblowers, would have been able to rely on it without fear of being sued for breach of their non-disclosure obligations. And so, the provisions around the whistleblower immunity, which are now in section 1833(b),[24] were crafted to provide that sort of protection. What's interesting here is that this is the only preemptive provision of the DTSA. Preemption is not something that this Congress takes on lightly. I'm not even sure that anyone even noticed as the statute went through, but there it is. Immunity is granted under any state or federal trade secret law to anyone who has information under an obligation of confidence and wishes to disclose it to law enforcement or to a court in confidence or to their lawyer in confidence for that purpose—for that sole purpose.[25] So, the immunity was established and the statute requires, in order to make sure that employees knew about this, that all nondisclosure agreements that were drafted after the date the

21. Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CAL. L. REV. 1 (2017).

22. James Pooley, *The Myth of the Trade Secret Troll: Why the Defend Trade Secrets Act Improves the Protection of Commercial Information*, 23 GEO. MASON L. REV. 1045, 1076 (2016) ("[Menell's] article appeared early in the process of Senate consideration of the [DTSA]. Senate staff reached out to Professor Menell to help craft appropriate language.").

23. *See* Menell, *supra* note 21, at 31–32; *see also* United States *ex rel.* Ruhe v. Masimo Corp., 929 F. Supp. 2d 1033, 1039 (C.D. Cal. 2012) (holding publication of documents evidencing fraud in contravention of a nondisclosure agreement was not wrongful for public policy reasons); United States *ex rel.* Grandeau v. Cancer Treatment Ctrs. of Am., 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004) (holding that there is a "strong policy of protecting whistleblowers who report fraud against the government").

24. 18 U.S.C. § 1833(b) (Supp. IV 2017).

25. *Id.*

provision came into effect, May 11 of last year, would have a notice of this kind of provision.[26]

The second major provision, which is found in section 1836,[27] on injunctions, bears some discussion. And that's the provision that corresponds to section 2 of the Uniform Trade Secrets Act.[28] It is very familiar language that tells judges you can issue injunctions on either actual or threatened misappropriations. And that makes sense, of course. Judges need to be able to stop something wrongful happening before it happens, if they can. And the objection, the original language in the DTSA, just took what was in the Uniform Trade Secrets Act and applied it there. There was an objection, mainly from the California delegation, principally Senator Feinstein, based on the concern that they had about the inevitable disclosure doctrine. But basically, when I worked with the staff on putting together language that would meet this objection—and with some help from Professor Lemley at Stanford—we suggested language that would refocus the issue away from this so-called inevitable disclosure doctrine and onto the question of what constitutes threatened misappropriation, and what public policy issues should inform a court's decision on what you can do about an employee who has left and is going to work for a competitor, thereby essentially impairing the security of the information that they know. And all that formulation that was agreed on was that courts can do this. You can't stop a person from taking a job, but you can put conditions on it but only if the evidence shows that they have acted in such a way that the conclusion can reasonably be drawn that they can't be trusted. You can't get an injunction solely based on how much that somebody knows.

The third provision that I wanted to talk about tonight is extraterritoriality. It's not a provision in the codified statute, but accompanying the statute as passed you will find very strong statements by Congress of their concern on the impact on U.S. companies and U.S. jobs from the misappropriation that happens

26. *Id.* § 1833(b)(3)(D).

27. *Id.* § 1836.

28. *Compare id.* § 1836(b)(3) ("In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may . . . grant an injunction . . . to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable . . . ."), *with* UNIF. TRADE SECRETS ACT § 2(a) (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1985) ("Actual or threatened misappropriation may be enjoined.").

outside the United States.[29] So there is an expression of, "We believe that this has an effect." Right? And there's also an expression found in a direction that the director of the Patent Office is supposed to report back regularly on the state of foreign-based misappropriation of U.S. trade secret assets.[30]

So, let me quickly go through a couple of issues or details related to the whistleblower provision. We've had our first, and so far as I know, the only published decision—*Unum Group v. Loftus*[31]—in which the plaintiff had sued the departing employee and attached to the complaint all of the correspondence that they had had with the employee's lawyer who said, "Yeah the guy did take a bunch of stuff, but he gave it to me so that I could make an analysis for purposes of this whistleblower protection, which we have. So, you can't sue us."[32]

Well they did. They asked the court for an injunction and the defendant moved to dismiss.[33] The court granted the injunction and denied the motion to dismiss.[34] And the issue is, as it was presented by the court, yes I know this is an immunity, but the facts predicate to establish the immunity are not clear—have not been established yet. Whether or not he took this information solely for the purpose of reporting it as a whistleblower or had some other purpose—we haven't been able to determine yet.

Professor Menell, who had written the article that led to this provision being in the DTSA, quickly posted a blog that called *Misconstruing Whistleblower Immunity Under the DTSA* and pointing out that what Congress had done here was to establish an immunity,

29. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376, 383–84 (codified as amended at 18 U.S.C. § 1836 (Supp. IV 2017)) ("It is the sense of Congress that—(1)trade secret theft occurs in the United States and around the world; (2) trade secret theft, wherever it occurs, harms the companies that own the trade secrets and the employees of the companies . . . .").

30. *Id.* at 383 (requiring that the Director of the United States Patent and Trademark Office, in conjunction with the Attorney General and IP Enforcement Coordinator, provide a report on global trade secret theft that describes enforcement in foreign jurisdictions, recommendations, and actions taken by U.S. agencies).

31. Unum Grp. v. Loftus, 220 F. Supp. 3d 143 (D. Mass. 2016) (treating the whistleblower provision as an affirmative defense); Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, CLS BLUE SKY BLOG (Jan. 3, 2017), http://clsbluesky.law.columbia.edu/2017/01/03/misconstruing-whistleblower-immunity-under-the-defend-trade-secrets-act/ (stating that *Unum Grp.* is the first reported decision regarding the whistleblower provision).

32. *See Unum Grp.*, 220 F. Supp. at 146.

33. *Id.* at 145.

34. *Id.*

and under Supreme Court precedent defining what an immunity is.[35] What the judge should have done here would be to protect the defendant from having to answer the lawsuit at all because that's what immunity is. It's not an affirmative defense.[36] And so, we're left with the question of how do you follow the instructions of the Supreme Court that says that an immunity has to be determined at the earliest possible time[37] while dealing with an immunity like this, which unlike most immunities, doesn't exist on the basis of status—who the person is, i.e. they're a government employee, et cetera. It has to do with a fact that may or may not be true. We don't know where this will go, but it will definitely be interesting. Perhaps this will get to be treated like personal jurisdiction, where there might be a limited amount of litigation allowed at the beginning with limited discovery to establish the predicate facts.

Now, inevitable disclosure. Some of you probably are very familiar with this. The inevitable disclosure doctrine was created from a 1995 case where dictum was extracted to suggest that a court could stop somebody from taking a job because they knew too much—in effect.[38] This was not the holding in this case, where the employee had lied about what he was going to do and where he was going to go after he left,[39] and where the judge had said, "Look you really can't be trusted and the information that you have is so sensitive that we're going to force you not to work, at least not work in that particular job,

35. Menell, *supra* note 31 (stating that Saucier v. Katz, 533 U.S. 194 (2001) provides the definition of immunity and that "Congress chose to insulate whistleblowers from exposure to trade secret liability through an express grant of immunity").

36. *See, e.g.*, *id.* ("Immunity is not a 'mere defense' to liability but an 'immunity from suit'" (quoting *Saucier*, 533 U.S. at 200).); Mitchell v. Forsyth, 472 U.S. 511, 526 (1985) ("[I]mmunity is 'an entitlement not to stand trial or face the other burdens of litigation.'").

37. *Saucier*, 533 U.S. at 201 ("[W]e repeatedly have stressed the importance of resolving immunity questions at the earliest possible stage of litigation.") (quoting Hunter v. Bryant, 502 U.S. 224, 227 (1991) (per curiam)).

38. PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995) ("The ITSA, *Terradyne*, and *AMP* lead to the same conclusion: a plaintiff may prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets . . . The defendants are incorrect that Illinois law does not allow a court to enjoin the 'inevitable' disclosure of trade secrets."); *cf.* Ryan M. Wiesner, *A State-By-State Analysis of Inevitable Disclosure: A Need for Uniformity and a Workable Standard*, 16 MARQ. INTELL. PROP. L. REV. 211, 214 (2012) (stating that the *PepsiCo* decision led to the inevitable disclosure doctrine gaining popularity).

39. *PepsiCo, Inc.*, 54 F.3d at 1264 (stating that after receiving a written offer from Quaker and accepting it to be the Vice President-Field Operations for Gatorade, defendant told plaintiff he received an offer to be the COO of Quaker's Gatorade and Snapple company, but had yet to take it).

for a few months until the information becomes sufficiently stale."[40] And like I said, this comes from, or at least is based on the issue of, threatened misappropriation. Now, not every court was enthusiastic about this doctrine—that you could issue an injunction against a departing employee because what they knew when going to a new job where they would be directly competing presented itself as a threat. That was certainly the reaction in California, by both the commentators and ultimately by the first court that got this, because California is a place that is very solicitous of the rights of employees and where we value the free mobility of labor.[41] In *Whyte v. Schlage*, a 2002 case, the court said basically we reject this doctrine of inevitable disclosure and it cannot be asserted as it was in that case as an alternative to proving threatened misappropriation.[42] That is an interesting idea, that there was distinction made between the two, but there we are. The conclusion since then has been that California is one of the places where inevitable disclosure doesn't work—it works in other places.[43] In fact, if you actually review all of the cases, there are very, very few cases anywhere else in the country where courts have prohibited someone from taking a job without evidence of some improper behavior and so the doctrine really hasn't been applied in the way that those who feared the whole thing thought that it was or might be.[44] In any event, with the DTSA, what we have tried to do is come

40. *Id.* at 1272 (affirming the district court's injunction enjoining defendant from taking new position through May 1995, in part because he "could not be trusted" with sensitive information).

41. *See, e.g.*, CAL. BUS. & PROF. CODE § 16600 (West 2017) ("[E]very contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."); Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d 277, 281 (Ct. App. 2002) ("We hold this doctrine is contrary to California law and policy because it creates an after-the-fact covenant not to compete restricting employee mobility."); Catherine H. Helm, *Unholy Covenants: Not Only Are Most Covenants Not to Compete Unenforceable in California, They Can Also Open the Employer to Expensive Liability Claims*, L.A. LAW., Oct. 2000, at 40, 44 (arguing that the inevitable disclosure doctrine, if adopted in California, could "drive a large hole through" the state's statutory protection of worker mobility); John H. Matheson, *Employee Beware: The Irreparable Damage of the Inevitable Disclosure Doctrine*, 10 LOY. CONSUMER L. REV. 145, 162 (1998) (arguing that if the inevitable disclosure doctrine was accepted in California, statutorily void non-competition agreements could be upheld "under the guise of protecting trade secrets").

42. *Whyte*, 125 Cal. Rptr. 2d at 281 (stating the court "reject[s] the inevitable disclosure doctrine").

43. *See, e.g.*, *id.* at 291 (stating that the court's survey of other jurisdictions shows the majority adopting some form of the inevitable disclosure doctrine); Cypress Semiconductor Corp. v. Maxim Integrated Prods., Inc., 186 Cal. Rptr. 3d 486, 504 (Ct. App. 2015) (reaffirming that the inevitable disclosure doctrine has been "flatly rejected" in California).

44. *See, e.g.*, Padco Advisors, Inc. v. Omdahl, 179 F. Supp. 2d 600, 611 (D. Md. 2002) (declining to find inevitable disclosure because no tangible trade secrets were taken);

up with a solution to that problem that we hope will overcome the differences between the states who appear to have embraced the doctrine and those who haven't by again directing attention back to the fundamental issue of "What does it take to prove threatened misappropriation—what is the proper balance in terms of public policy between the interests of the employee and the interests of the employer?" That balance, which is essential in trade secret law, has been with us since courts were first struggling with what should be protectable as between an employee's skill and general knowledge on one hand, and the employer's trade secrets on the other. We're constantly dealing with these sorts of things, and this is one of the areas where we think a better focus on that balance could be made. So, my prediction here is that if we get cases where you have facts similar to *PepsiCo*,[45] you could get a federal court in California issuing an injunction limiting what the departing employee could do notwithstanding Business & Professions Code 16600 because it does not violate the policy of that section.[46]

Finally, extraterritoriality. We all know that laws in the U.S. are not to be applied externally to this country, unless congressional intent is very clear that they should.[47] The National Espionage Act has a section in it that is the Act as it existed before the DTSA, Section 1837,[48] that limits extraterritoriality to an act in furtherance of the offense or where the offender is a U.S. citizen. So the question is: will Section 1837 be seen as a limitation on the broad exercise of jurisdiction or not? And again there is a decent argument that it should not be a limit. And speaking of limits, I am at the end of my time.

CALO: Thank you very much, Jim. In a moment, we will get Elizabeth up here to give a critical assessment of what is going on in this phase.

I wanted to clarify something. So, the idea is that there are federal trade secrets. There's a federal trade secret act, there are other federal

Bridgestone/Firestone, Inc. v. Lockhart, 5 F. Supp. 2d 667, 682 (S.D. Ind. 1998) (finding no inevitable disclosure because the employee did not take documents or other confidential information); Nw. Bec-Corp v. Home Living Serv., 41 P.3d 263, 268 (Idaho 2002) (requiring a showing of misappropriation of trade secrets, not just a potential for future disclosure).

45. *PepsiCo, Inc.*, 54 F.3d at 1264–65.

46. CAL. BUS. & PROF. CODE § 16600 (West 2017).

47. *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 265 (2010) (holding that the "presumption against extraterritoriality" is absolute unless the text of a statute explicitly says otherwise).

48. 18 U.S.C. § 1837 (2012).

laws. Then there are the state laws, almost all of which peg the uniform trade secret law. What's different here? So what I got out of it was the fact that, number one, there's a private cause of action and that differs from the federal law before, correct?

Number two, there's the whistleblower protection, which is preemptive, and I want to come back to preemption in a minute when I get a chance to ask questions. There is this idea that you can seize things that was not in the federal law before. Was that in state law already or not in state law?

POOLEY: Some states.

CALO: Some states, not others. Okay, one question I did have was, isn't there a specific law that goes after folks who are from foreign countries who try to steal trade secrets as well? That has extraterritoriality by definition, right?

POOLEY: In the criminal statute, that's Section 1831.[49]

CALO: Got it. Okay, fascinating. So, I was thinking about how important all this is and to think about. Just recently, the head of Google cars who does the driverless car stuff, Chris Urmson, he gets paid all this money by Google. He gets paid so much money that he decides with one of his friends, I'm going to do my own driverless car start-up.[50] And so he leaves Google, right?[51] And he's going to have his own start-up using all of the technology that they developed at Google. He has to be thinking really hard about these issues, and whether or not he makes the decision to go out on his own and maybe do something innovative is going to turn, in part, on these kinds of questions. Okay, well thank you very much again, Jim. I would like to invite Elizabeth up to make her remarks.

ELIZABETH ROWE: Thank you all very much. I appreciate the opportunity to be here to speak with you all today about the DTSA. The DTSA is, as you've heard, is indeed a very important piece of legislation and the goals were quite admirable. However, as with all legislation arrived at by compromise, the language in certain provisions is not entirely clear or could be read more broadly than what Congress might have intended. These unintended consequences

49. *Id.* § 1831 (2012).

50. Kara Swisher & Johana Bhuiyan, *Google's Former Car Guru Chris Urmson Is Working on His Own Self-Driving Company*, RECODE (Dec. 10, 2016, 1:07 PM), https://www.recode.net/2016/12/10/13905292/google-car-chris-urmson-new-company.

51. *Id.*

might ultimately serve to the disadvantage of the very parties that were meant to be protected by the Act; ultimately time will tell as the courts address these issues in the coming years. So today, I want to highlight a few of the provisions that appear to raise questions as I've studied them.

The first is the applicability. I draw your attention to this language: "An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in or intended for use in interstate or foreign commerce."[52] It's the particular language: "related to a product or service used in or intended for use in interstate commerce" that appears that it could be quite restricted because there are indeed trade secrets that will not fit into that category. Now this language is the same as that which was added to the EEA, the Economic Espionage Act, in response to the *Aleynikov*[53] case from a few years ago, but it's still ambiguous. So for instance, what about trade secrets that are for internal business use only, such as customer list pricing information, source codes, and programs? These types of trade secrets are involved in a large number, if not a majority, of cases that are filed in federal and state courts in the U.S.[54] Are these types of cases then not covered by a strict reading under this language? There's no question that they are in fact covered in the UTSA, the Uniform Trade Secrets Act,[55] and state laws based on it.[56] We've already had one DTSA case where a complaint was dismissed based on this ambiguous provision and this

52. 18 U.S.C. § 1836(b)(1) (Supp. IV 2017).

53. United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012); *see* United States v. Agrawal, 726 F.3d 235 n.3 (2d Cir. 2013) ("Following *Aleynikov*, but prior to Agrawal's conviction, Congress amended Section 1832(a) of Title 18, United States Code, to reverse our reading of the EEA.").

54. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 72–73 (2011).

55. *See* UNIF. TRADE SECRET ACT § 1 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1985) ("The definition includes information that had commercial value from a negative viewpoint, for example the results of a lengthy and expensive research which proves that a certain process will *not* work could be of great value to a competitor"); *see generally* 1 ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS, § 1.01 (2017) (identifying the development of the UTSA, the definition of "information," and its enactment by the states).

56. *See* Joseph W. Hammell, PROTECTION OF EMPLOYERS' TRADE SECRETS AND CONFIDENTIAL INFORMATION, Practical Law Practice Note 5-501-1473 (stating that trade secret protection has been recognized in a various states for marketing plans, commercial drawings, recipes, sales date, manufacturing processes, chemical formulae, and detailed information about customers); *see also* Beck Reed Riden LLP, *Trade Secret Laws and the UTSA: 50 State and Federal Law Survey* (Jan. 24, 2017), http://www.beckreedriden.com/trade-secrets-laws-and-the-utsa-a-50-state-and-federal-law-survey-chart/ (identifying that every state but Massachusetts and New York have adopted the UTSA in one form or another).

language: a district of Delaware case that involved allegations of misappropriation of some confidential recordings.[57] And the court ruled that because the recordings were not related to a product or service in commerce, the count had to be dismissed.[58]

But, the provision that received the most attention, as Jim mentioned earlier, and to which critics have voiced the most opposition has been the seizure provision. My own sense is that the provision will not be as problematic as critics feared. This is particularly because it says, the court may upon ex parte application, but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.[59] So, it's very clear that only in rare circumstances, only in extraordinary circumstances, should a court grant such an order. There are also several additional limiting provisions in the DTSA, such as the requirement of a showing that a Rule 65 order (such as a temporary restraining order or a preliminary injunction) [60] would not be sufficient under the circumstances and that the party might avoid, evade, or not comply with such an order. There is specific language saying that, where there is a showing that the person against whom the seizure would be ordered or persons acting in concert with such person would destroy, move, or hide, or otherwise make such matters inaccessible to the court, then in those types of extraordinary circumstances, a judge should consider issuing such an order.[61] In addition, there could also be damages against the party who seeks the order for wrongful reason or where there is an excessive seizure or attempted wrongful seizure.[62] This could also serve as a disincentive for plaintiffs who wish to seek such an order unnecessarily.

Nonetheless, there is at least one part of the provision that does seem to raise a question for me, and it is this language: "the court may upon ex parte application, but only in extraordinary circumstances, issue an order providing for the seizure of property, necessary to prevent the propagation or dissemination of the trade secret that is the

57. Hydrogen Master Rights, Ltd. v. Weston, 228 F. Supp. 3d 320, 337 (D. Del. 2017).
58. *Id.* at 338.
59. 18 U.S.C. § 1836(b)(2)(A)(i) (Supp. IV 2017).
60. *Id.* § 1836(b)(2)(A)(ii)(I).
61. *Id.* § 1836(b)(2)(A)(ii)(VII).
62. *Id.* § 1836(b)(2)(B)(vi).

subject of the action."[63] This word "property" could be interpreted very broadly. For instance, would it allow seizure of a person's computer or all of a person's computers if the alleged trade secret is in electronic form? And today, most trade secrets are, in fact, in electronic form. You could imagine the potential for a very far-reaching and invasive sweep if a court were to read the term "property" broadly.

A procedural question that I have about this provision is whether a state court judge can grant a seizure order. The jurisdiction language under the DTSA says that the district courts of the United States shall have original jurisdiction of civil actions brought under this section.[64] Since federal courts don't have exclusive jurisdiction, only original jurisdiction to apply the DTSA, then arguably a state court judge could be granting, could be hearing the request and could be granting the seizure order if a DTSA count is filed in state court because we know that there are already existing provisions to file simultaneously a state court action and a federal court action under the DTSA under the same set of facts. So, assume a plaintiff were to file in state court originally, and file a DTSA count, and at the same time request a seizure order, what should happen? It would be up to the defendant to seek removal to the federal courts. But these ex parte seizure hearings would occur before the defendant even knew that there was a lawsuit, which would provide even more opportunity for a state court judge to rule on this issue. So, I wonder what scenarios might appear down the road with state courts ruling on seizure orders.

Now I would like to talk a little bit about the non-competition agreements and the inevitable disclosure doctrine. The DTSA provides that a court may grant an injunction, provided that it does not 1) prevent a person from entering an employment relationship and that conditions based on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows,[65] or 2) otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business.[66] So, this seems to me that you can't enforce non-competes or otherwise enjoin an employee from working because that would

63. *Id.* § 1836(b)(2)(A)(i).
64. *Id.* § 1836(c).
65. *Id.* § 1836(b)(3)(A)(i)(I).
66. *Id.* § 1836(b)(3)(A)(i)(II).

"prevent the person from entering into an employment relationship." Although query, what does entering into an employment relationship mean? Does it mean you can't seek, accept, and start a new job? Or if you've already accepted the offer, but haven't actually started work yet, does it mean you cannot report to work? Or if you've already been on the job a few days or just a few weeks? Could DTSA force a brief interruption that makes you sit out for a period of time, if a court were to grant an injunction? In other words, would an injunction that prevents you from continuing on the job, be in compliance with this language?

With respect to the inevitable disclosure doctrine, the DTSA provides that court-imposed conditions of employment have to be based on evidence of threatened misappropriation, not just what is in a person's head, what a person knows.[67] This seems quite reasonable and could still work for some of the jurisdictions that have, in fact, adopted the doctrine. However, it seems to me, the nail in the coffin for the inevitable disclosure doctrine is actually this language: "prevent a person from entering,"[68] because if entering is interpreted broadly, it strikes at the heart of the inevitable disclosure doctrine, which prevents a person from working for a new employer. The other more troubling part of this, which I imagine, was unintended, is that the injunction can't conflict with state law prohibiting restraints.[69] So, this would work well in California, and it should, because as you've heard, the California lobby fought for this language, and it reflects California's public policy.[70] However, what if you are in Florida, Texas, or the vast majority of states that do not prohibit employment restraints, such as non-compete agreements? Since it is impliedly okay to conflict with their laws not prohibiting restraints, then it seems to me you can't enforce a non-compete or otherwise restrain an employment relationship, even in states that otherwise enforce such restraints, when according to the legislative history, I think the intent

67. *Id.* § 1836(b)(3)(A)(i)(I).

68. *Id.*

69. *Id.* § 1836 (b)(3)(A)(i)(II).

70. *See* Viva R. Moffat, *Making Non-Competes Unenforceable*, 54 ARIZ. L. REV. 939, 944 (2012) ("The California rule against the enforceability of non-competes is codified in section 16600 of the Business & Professions Code, which states that 'every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void.'"); 70 M. KIRBY WILCOX, CALIFORNIA EMPLOYMENT LAW, § 70.09 (2017) ("[C]ourts in California have consistently affirmed that section 16600 evinces a settled legislative policy in favor of employee mobility.").

was probably to not conflict with the public policy of laws such as in California, but to respect the laws of other states that grant such injunctions. But perhaps I misunderstand that; I'm going to talk to Jim about that tonight. If this reading is accurate and a plaintiff wants to enforce a non-competition agreement or make an inevitable disclosure argument, would they need to file in state court their state trade secret action and does that mean they can't file or shouldn't file a DTSA count? This certainly seems to undermine the goal of access to the federal courts to address trade secret claims, which was one of the motivations behind the law.

Another provision I would like to bring to your attention is that involving "improper means." The DTSA says "improper means" does not include reverse engineering, independent derivation, or any other lawful means of acquisition.[71] For the most part, the DTSA language on the definition of what misappropriation means mirrors that of the UTSA.[72] However, they chose this language to make even more explicit what is not considered improper means: reverse engineering and independent derivation. Well, we already knew that, because under the common law and fundamental trade secret principles, trade secret misappropriation can't apply to one who has reverse engineered or independently derived the secret.[73] My issue with this is probably having to do with punctuation, but we'll see. Instead of putting a period after the word "derivation," they added this language: "or any other lawful means of acquisition." Well, it has long been held and accepted that "improper means" does not have to be unlawful in order to constitute misappropriation.[74] Otherwise legal conduct can nonetheless be improper if that conduct violates standards of commercial morality, for instance.[75] So, if this new language is somehow excluding acquisition by any lawful means, it would be a

71. 18 U.S.C. § 1839(6)(B) (Supp. IV 2017).

72. UNIF. TRADE SECRETS ACT § 1 (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1985).

73. 1 MILGRIM, *supra* note 55, § 1.01.

74. *See* Douglas W. Swartz, *Mining Agreements: Contracting for Goods and Services*, 5 2015 ROCKY MTN. MIN. L. FOUND. SPECIAL INSTS. 1, 7 (2015) ("If a trade secret is acquired by improper means (a somewhat wider concept than 'illegal means' but inclusive of such means), the secret is generally deemed to have been misappropriated.").

75. 64 RICHARD E. KAY, CAUSE OF ACTION FOR MISAPPROPRIATION OF TRADE SECRETS § 6 (2017); *see also* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970) ("A complete catalogue of improper means is not possible. In general they are means which fall below the generally accepted standards of commercial morality and reasonable conduct.") (citing RESTATEMENT OF TORTS § 757 cmt. f at 10 (AM. LAW INST. 1934)).

tremendous departure from the current status of the law. In order to avoid that, I think we might want to interpret the language consistent with statutory interpretation principles to read "other lawful means" as being limited by the words that came before it, i.e., "reverse engineering" and "independent derivation," but we'll see.[76] We could have clever defense counsel who try to argue otherwise.

So, this is about all that I have time for, so I will stop here and I thank you for your attention.

CALO: It's just so fascinating: you have this set of political compromises, you have this idea of what needs to be fixed, right, and you have this language and the language has a life of its own and maybe it doesn't do exactly what was intended. That's a pretty common issue in the law. Okay, so last but certainly not least, before we jump into Q&A, we have some remarks from Dave Green, who works for a company that has a lot of intellectual property, Microsoft. Recently, Microsoft has made a kind of a pivot to hosting things in a cloud and doing data analytics and even making devices. At least, that's the way they're playing themselves these days and it seems to be working quite well; Microsoft's doing great. But historically, the very lifeblood of this company, of course, is the ability to protect its secrets and its intellectual property, and not just in the United States, but also abroad. According to what I've heard from folks there, Microsoft gets 51% of its revenue outside of the United States.[77] So now we're going to hear the perspective from a person who actually has to live and breathe and really battle this stuff out. So with that I'd like to invite Dave to make some remarks.

DAVID GREEN: Great, thanks, Ryan. I'm going to strategically avoid—the lectern. It's not because I want to disadvantage myself of the gravitas that the lectern provides, but it's just that when I disconnect my power cord, my screen goes black, and I've got notes here.

Let's pause for a moment and consider that, in the DTSA, Congress passed an intellectual property law with almost unanimous support of the tech industry, the manufacturing industry, and from a number of other industries. In contrast, other areas of intellectual property law, particularly copyrights and patents, cause significant

76. 18 U.S.C. § 1839(6)(B) (Supp. IV 2017).

77. *See Microsoft 2016 Annual Report*, *Note 21*, MICROSOFT (Oct. 18, 2016), https://www.microsoft.com/investor/reports/ar16/index.html.

amounts of dispute, as parties have very different positions on what the law should be. Yet here, in the field of trade secrets, there was almost unilateral agreement that the law was necessary and that the law adopted is a good compromise. Any time Congress passes an intellectual property statute of the scope and breath of the DTSA, it should tell you something about the importance of that area of intellectual property. And you might ask yourself, gosh, what is the DTSA's signal to all of us with respect to the status of trade secrets? What's fundamentally going on with trade secrets that we needed a new law on the books to give us a federal civil cause of action? So I'll just speak from Microsoft's perspective, which I hope in some ways reflects the tech industry's perspective, on what is going on with trade secrets, which as Ryan alluded, is definitely a consequence of what we're seeing in businesses' shift to the cloud.

So, there's really two reasons that I think trade secrets, by and large, are starting to rise in terms of their significance and their importance. And just think of this from a company's perspective. A company like Microsoft depends on intellectual property in order to protect our innovation. We've got patents and we've got copyrights for our code and maybe our APIs; we'll have to see how it turns out to be with respect to the *Oracle v. Google* case.[78] And then we've got, obviously, trade secrets. There's two things going on with the cloud. The first is that some interesting things happen when you try to graft a lot of the traditional IP protections that happen in the tech industry—which is primarily copyrights and patents—onto cloud technology. I'll explain that in a moment. The second thing is that there's something fundamental about the cloud that's causing us to treat confidential and proprietary information differently in terms of how we share it, whether we share it broadly and under the circumstances in which we're sort of forced, because of the cloud's infrastructure, to share this information. I'll talk a little about that and give an example.

But first, let me come back to some sort of high-level thoughts. When an owner prefers trade secrecy protection over copyright and patent protections, it's usually because of two reasons. The first is that there's some measurable business advantage that you obtain by controlling access to this innovation, rather than by releasing it in

78. Oracle Am., Inc. v. Google, Inc., 750 F.3d 1339 (Fed. Cir. 2014) (holding that Oracle's API packages were copyrightable).

reliance on enforcement mechanism enabled by intellectual property laws, licenses, or a combination of the two. The second is it may be difficult to detect infringement: practically, it's just difficult to discover when infringement occurs, unless it becomes publicly known. Let's turn to copyright for just a moment and think about the shifting role that copyright protection is playing on the cloud. So you've got cloud architecture, which means no longer are you forced to distribute source or object code. A lot of that code can just sit behind a server, and what the consumer has access to is the functionality of the code or the service provided by the code, not the raw bits. So the code stays in the cloud, and that fact necessarily decreases your reliance on enforcement triggered by reproduction and distribution rights. One practical consequence is that your competitors are much less likely to reverse engineer our processes because they don't have access to the code; they can't decompile, they can't run their various sniffers and analytic tools to determine what's going on or what the secret sauce is. When you remove reproduction and distribution of code in which copyright plays a vital role, that lessens the role that copyright plays on the value chain.

So now let's switch over to patents. There's some fundamental things going on with patents in this day and age that are causing some stress as well. If you've taken in your Patent Law courses or you just follow the news, obviously, you understand that software patents and business method patents generally are under pressure, if not under attack. We have some decisions like *Alice*[79] that are narrowing patent subject matter eligibility. And as a consequence, when you're drafting a patent, in order to overcome possible attacks on eligibility, you will tend to disclose more information; you've got to specify and articulate different methods and systems, which invariably causes you to reveal more about the specific process that protects your innovation. Whereas before, you had more of a generic application and you could keep from disclosure your own specific implementations by generalizing the scope of the patent. So that's an interesting complication. And if you have disclosed an innovative process in a patent, the cloud makes it more difficult to detect infringement of that patent. That's because the means, methods, and systems of operation used by your competitors

79. *See* Alice Corp. Pty. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347 (2014) (holding that software implementation of an escrow arrangement was not patentable on the grounds that generic computer implementation fails to transform an abstract idea into an invention).

are also in a cloud and you just don't have the visibility into the inner mechanisms and process. You see the outputs and functions, but you are guessing at what systems and methods of operation produced those outcomes. In a system where you have to disclose more to obtain a patent, and the detectability of infringement is more difficult in the cloud, you've got a mismatch between the protection realistically available in the cloud and that provided via traditional IP such as patent and copyright regimes.

Now let's turn to the second reason, a tension with our traditional dichotomy for understanding trade secrets. The dichotomy is: the value of disclosure versus this value of secrecy. And people tend to think of that as a binary choice, right? You either disclose and lose, or you withhold and maintain that value. I think what we are finding in a cloud is actually more complicated. We are starting to see hybrid models — I'll give one particular example. The challenge of reliance on a binary model where you don't disclose and you put in the reasonable measures to control access is that those measures introduce friction. And that friction introduces inefficiency in the marketplace in terms of how people access and utilize your material. If you really want to maximize the value of your proprietary information, particularly in a cloud environment, you may have to disclose that information in a much broader way than would be typical if you were a biotech company with a secret biotech formula for a drug, or if you are a manufacturer with a particular processor method of manufacture that you want to keep proprietary. So I'm going to use an example that shows attention to this dichotomy.

Apple has this terrific application called Siri, its personal digital assistant. There may be aspects of Siri that are patentable, but a lot of the proprietary innovation around Siri has been kept behind closed doors: how it works, the algorithms, the information that helps Siri understand how to execute a user's tasks, etc. That approach provided Apple with an initial period of exclusivity, a competitive benefit for this great exclusive feature. They were first to market with it, and it produced some renown. And then very soon you saw competitors come into the field with their own innovations. But they did not just come in with their own competing innovations; they came in with their own competing business models. Siri came to market in 2011 and its main features were things like: searching the Internet, getting directions, calling or texting somebody in an automated fashion. Now

compare that to its competitor, Amazon's Echo. First of all, Amazon came out of nowhere: the AI processes for the Echo just sort of popped almost out of thin air. You have this device and all of a sudden, within about 12–18 months . . . —who here bought one for Christmas?—they are just everywhere. And the functionality that Amazon's Echo enabled was far broader than Siri for a very important reason; Amazon had a strategy of releasing an SDK[80] that actually revealed far more information about the processes and systems of its AI and allowed people to develop independent applications that did things like ordering tulips on 1-800 flowers, calling an Uber, checking your balance on Capital One, or playing NPR—things that couldn't have been done as efficiently or brought as quickly to market in a closed environment and closed model. So you've got this interesting new hybrid model where you release more information than you typically would. You can do so if you utilize the cloud. A lot of the really sensitive information you can keep in the cloud behind closed doors. You can parse out the functions and provide via an SDK, perhaps one with confidentiality provisions and reliance on trade secret protection, some measures that allow a broader disclosure than you typically would and then the information that sort of has less relevance as a trade secret may not have any protections under copyright or patent gets just broadly distributed. So the cloud is doing something fundamental in our industry to elevate the role of trade secrets.

The one thing I will leave you with—because most of you are law students and many of you are practitioners—is that you've got to encourage a broad perspective of trade secrets, you need to parse through the DTSA to understand the civil causes of action and the requirements to enjoy the enhanced remedies or the seizure opportunities and you have to bring that information back into your company to fully advantage yourself of the DTSA's opportunities. One of the neat things about the DTSA is that the DTSA has rekindled this discussion of trade secrets. It is really helpful to companies like Microsoft. I will just ask a broad question and I won't ask you to answer it, maybe just answer it to yourself. If our competitors could know five things about Microsoft, if they had access to five critical things, what would those five things be? What are the most important

80. A software development kit (SDK) consists of software development tools to create apps for a specific platform. Grant Glas, *What Is an API and SDK?*, APP PRESS, (Apr. 22, 2015), https://www.app-press.com/blog/what-is-an-api-and-sdk.

five or ten things at Microsoft that really constitute proprietary confidential trade secrets? Now, notice I called them confidential trade secrets. And I did that because I think one of the mistakes companies tend to make today is that they put a broad blanket over all information, calling it confidential. They rely on NDAs, they mark things confidential, etc. But there is a difference between what is confidential and what constitutes a trade secret. And if your employees don't know the difference between the two, if your company cannot make the distinction between the confidential information and the components of that confidential information that comprise critical trade secrets, how on earth are you going to impose the type of reasonable measures and reasonable access controls and other compliance practices in order to take advantage of the DTSA seizure provision[81] (which requires what I think is an enhanced pleading burden)? And how are you going to create a culture around trade secrets that is different than creating a culture around confidentiality?

So one of the neat things that the DTSA has done is that it has caused a lot of companies to look at how to comply with these additional requirements under the DTSA and that prompts a really candid conversation about the role that trade secrets play, and how to maximize trade secrets in terms of protecting their innovation. It's a fun question to be able to go to business executives and ask them what's really important. They will say everything is important: marketing, our products, and the make up of our next version of Surface,[82] the technical spec, the marketing timelines, how much we are committing, etc. When that happens, I say, "Stop! What are the five or ten things that if other companies knew or had access to would cause us significant competitive harm?" And the practices around those, the compliance efforts and practices around those, should necessarily be heightened. The consequence of heightening those protective measures is that then you are allowed to look at the other confidential information, not from a compliance perspective—which is how do I protect it, how do I make sure I advantage myself under trade secrets law—but to look at what's the friction that we introduce by controlling the access and use of this material.

81. 18 U.S.C. § 1836(b) (2) (Supp. IV 2017).

82. Microsoft Surface "is a versatile laptop, powerful tablet, and portable studio in one." *Buy Microsoft Surface Version 2*, MICROSOFT, https://www.microsoft.com/en-us/surface/devices/surface-book-2/overview (last visited Nov. 10, 2017).

One company—I won't name one of our competitors, well not really competitor but more of a partner—did this exercise and what they found was that, because of credential restrictions and all the other access protocols that they had around source code, their coders, instead of going into the company's warehouse and utilizing code that had been vetted and tested, actually started rewriting code again, or went to maybe less protective or less critical open source code. So by removing the friction that was caused by some of these access protocols, for some component of their code they ended up creating efficiency in how they and others are able to repurpose this code. Not all of our source code is of equal importance; not every bit is as important as the other bits—there are probably kernels that are really critical, but there is also code that is important but less sensitive and does not need the same access restrictions. If we reduce those access restrictions, without losing the benefit of confidentiality and hopefully without negating our trade secret protection, we have now taken away friction and we have introduced a level of efficiency. And just as Echo and Amazon did, if you take that practice and expand the scale, all of a sudden you are rethinking the "pallet" of your intellectual property protections, i.e. when you use trade secrets, when you use copyright, when you use patents, and when you use none of them.

CALO: I think Dave's contribution we are going to need a glossary. So SDK is a Software Developer Kit, that is what you give to people that you want to develop on your system. API is a Programmable Interface, what is the A for again? I forget.

GREEN: Application.

CALO: Application Program Interface. Thank you. I love it. I just love talking to technologists, or in this case, technologically savvy lawyers, about what they do. In the interest of tim—because I do want to be able to have time to have a little dialogue—I am just going to offer a couple of provocations and get you all to respond to them or whatever interests you. The first is that my intuition is, as a person who studies emerging technology and law, that this notion of preemption is going to be a big deal. And let me tell you why. So right now, there are all these different states that have these security breach notification laws. And what such a law does is that it says that if you are in a particular state and you have a security breach, and all this data gets out about your consumers—big companies hate it. They hate it because they don't know, from state to state, what the laws are. And

they differ from each other. Who do you have to notify, how fast you have to do it, right? So big companies, including Microsoft, Google, and everybody, have been pushing for a unitary standard, a federal law about data breach notification. They are saying yes, yes, regulate us in that way. Tell us what we need to do in the event of a breach. But let me tell you, such a federal law is definitely going to have preemptive effects against state laws when it comes down the line. It will have preemption because it is good for those powerful companies who are asking for it. So here, with DTSA, we have a situation where there is no preemption. You could say there is a patchwork, and actually there are multiple layers that a company can avail itself of if there is a trade secret problem. And yet, there is this one particular place—concerning whistle blowing—where DTSA is preemptive.[83] In other words, maybe there was an intuition that states should have whistle blower protection and they don't. And that ends up being pro-employee. So I guess one thing I want to throw out is, is it weird that there is not preemption? Were there players in the system, in the ecosystem here, that were pushing for preemption and lost out?

The second thing I wanted to flag was basically, and I just want to remind Elizabeth, and I am sure she remembers this, she had this question for Jim about whether or not seizures apply in state court and whether you could go to a state court and ask them to seize something. And I find that fascinating and I hope Jim could give us his thoughts about that.

The last provocation is around this idea of what it means to do more than just know something. So remember my example about Chris Urmson, and he is leaving Google and he is going to go start his own driverless car.[84] I mean all that guy was doing for a living was doing driverless cars for Google. He comes out of Stanford. He is a brilliant guy. Does all of this driverless car work. Obviously, he knows a lot. He and Sebastian Thrun made driverless cars for Google.[85] He

83. *Cf.* 18 U.S.C. § 1833 (Supp. IV 2017) (providing immunity to those who confidentially disclose trade secrets to the government); *see* Daniel Hurson, *The Whistleblower Protections Of The Defend Trade Secrets Act Could Have A Broad Impact—But Only if Employees are Told About Them*, MONDAQ (Sep. 13, 2016),
http://www.mondaq.com/unitedstates/x/526468/Whistleblowing/The+Whistleblower+Protections+Of+The+Defend+Trade+Secrets+Act+Could+Have+A+Broad+ImpactBut+Only+If+Employees+Are+Told+About+Them.

84. Swisher & Bhuiyan, *supra* note 50.

85. Chunka Mui, *Chris Urmson Reflects on Challenges, No-Win Scenarios and Timing of Driverless Cars*, FORBES (May 8, 2017, 12:45 PM), https://www.forbes.com/

is going to walk away with that knowledge. And whatever he does next, even if he does not take proprietary code, he knows what he knows. And his experiences at Google are going to inform what he does. And then he does a competitive start-up.[86] Is that enough in terms of its behavior to have a trade secrecy problem? So I am just so curious as to what folks think about what goes into that notion of knowledge plus. Aren't we all informed all the time by our experiences and isn't there no way around that? Anyway, those are three provocations I would like to toss around for each of you to respond to as you wish and then I would like to open it up to questions.

POOLEY: I think it's one of the conceits of trade secret law that judges can distinguish between that kind of information that somebody ought to be able to put into in their tool kit and take with them because it represents developed "skill," and on the other hand, the specific information relevant to, that belongs to, the former employer. And actually, in most cases, it is not that hard, but you can imagine ones like the one that you're talking about, where somebody was engaged at such a high level that it is hard—it is very, very hard to draw that line. But that's why judges get paid so much.

CALO: For example, someone goes to Chris, and says, "Hey we should do this thing where we, you know, we can use the STK and the API—we should do that," and then he's gonna be like, "Nope, that doesn't work. We tried that at Google and it doesn't work." I mean, is that potentially protected?

POOLEY: Potentially, you would have to have more context than that.

CALO: Anyone else have any other responses?

GREEN: So did anyone follow the *Oculus Rift*[87] case? The *Oculus Rift* case is a fascinating case; fascinating just for a human drama associated with it. The claims are a little bit difficult to parse: there's a copyright claim, a trade secret theft claim, a breach of confidentiality

sites/chunkamui/2017/05/08/urmson-on-driverless-cars/#26b3b9a747c9; Tom Simonite, *The Creator of Google's Self-Driving Car Now Competes with It*, MIT TECH. REV. (Oct. 26, 2016), https://www.technologyreview.com/s/602712/the-creator-of-googles-self-driving-car-now-competes-with-it.

86. Danielle Muoio, *Tesla's Former Autopilot Head Is Launching a Self-Driving-Car Company—and It Could Have a Big Advantage*, BUS. INSIDER (May 29, 2017, 10:37 AM), http://www.businessinsider.com/aurora-innovation-self-driving-car-company-rival-tesla-google-2017-5.

87. Zenimax Media, Inc. v. Oculus VR, Inc., 166 F. Supp. 3d 697 (N.D. Tex. 2015).

claim.[88] Oddly enough there's a half a billion-dollar verdict, I think.[89] $500 million dollars including personal liability imposed on some of the founders, but the jury found no trade secret theft.[90] They found breach of confidentiality, and they found some copyright infringement based upon some sloppy practices.[91]

My sense is that the challenge with the example you posed is having someone who is a guru in that area and they start to move around; I think tech companies view laws in these situations as both a sword and a shield: if you insist on strong provisions, if you love the inevitable disclosure doctrine, you're never going to have any movement, right? That is bad because I think the lifeblood of tech companies is the free flow of workers and information. The second is, it is not like trade secret information exists in a vacuum. Typically if a company has had a guru there, it also has a team of lawyers, scribbling very furiously, writing down patent applications and copyrighting different implementations of code; so if that person goes to a different company, it is not like suddenly there is no IP to protect the company's innovation. But it is a challenge and we've had scenarios where one of our engineers left to go to Google under challenging circumstances, let's put it that way. So these things can be difficult to parse, but every time a company is in the position of worrying about one of its best and brightest leaving, another section of the same company is worried about the arrival of such a person, what that person brings with them, and hopefully what they do not bring with them because that taints that company's development and responsible companies develop good practices on these issues. They have entrance and exit interviews with their employees so that it is very clear that when an employee departs, they have a really good

88. *See id.* at 703–05; Lucas Matney, *Jury Awards ZeniMax $500 Million in Oculus VR Lawsuit*, TECHCRUNCH (Feb. 1, 2017), https://techcrunch.com/ 2017/02/01/jury-awards-zenimax-500-million-in-oculus-vr-lawsuit.

89. Matney, *supra* note 88.

90. Ben Gilbert, *Facebook Just Lost a $500 Million Lawsuit—Here's What's Going On*, BUS. INSIDER (February 7, 2017, 9:05 AM), http://www.businessinsider.com/facebook-zenimax-oculus-vr-lawsuit-explained-2017-2/#august-2013-oculus-vr-a-startup-working-on-a-virtual-reality-headset-called-the-rift-hires-doom-creator-john-carmack-of-id-software-as-its-chief-technology-officer-1.

91. *See ZeniMax*, 166 F. Supp. 3d at 705 ("According to Plaintiff, Defendant acquired Oculus for a substantial amount of money despite knowing about the copyright infringement allegations. As the owner of Oculus, Defendant []allegedly financed and supported Oculus's conduct of developing software based on Plaintiffs' copyrighted information. These allegations are sufficient to at least plead a plausible claim of vicarious copyright infringement. . . .").

sense of what the company cares about, what they are concerned about, and how to ensure that there is not a leakage of proprietary information as opposed to someone just taking the body of knowledge that they developed over the course of their career and jumping ship.

ROWE: I think too, that one of the tricky things about trade secret law which makes it so complicated is that, in theory, we can talk about all that it covers and specialized knowledge versus generalized knowledge and all of that,[92] but this is one of those areas of law where a lot happens after the fact: while the lawyers are figuring out what they're going to say in the complaint because the client is upset and the lawyers are working backwards from those particular circumstances. For every one trade secret case where you say, "Oh this seems like a perfectly legitimate claim," for example, where the treasurer of the company was just about to walk out the door with this person, you can find several other cases where you think, "Well, I don't know, this is kind of a stretch, I'm not quite sure it's even a trade secret case to begin with." But the lawyers are tasked with crafting a trade secret claim and they want an injunction, and that is why when you look at the jurisprudence, you have such a wide range of cases. Of course, trade secret law is highly factual but much of the variation comes from the fact that the law has evolved as state law. Every state is different, and the trade secrecy law is based upon and supported by the public policy of the relevant states. So again, taking California, one of the leaders and I think, probably the most sophisticated states in terms of handling trade secret cases: when you look at the body of law coming out of California, versus the body of law coming out of Texas or Florida or even New York, California law looks quite different. This was, again, part of the reason for wanting greater harmonization with the federal law, particularly, for companies that do business in more than one state, and across the world. So we'll see how that continues, how it evolves.

CALO: So why not preemption?

POOLEY: You can't get it. Congress won't take it. It's a non-starter.

92. *See generally, e.g.*, *In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 879 (7th Cir. 1986) (noting how the doctrine of trade secrets involves balancing competing interests of employers in wanting to protect specialized knowledge, with that of former employees seeking general use of skills); B.C. Ziegler & Co. v. Ehren, 414 N.W.2d 48, 53 (Wis. Ct. App. 1987) (noting the same balance of interests).

CALO: But why is it so successful with other stuff? For example, Food and Drug Administration rules. You know what I mean, it happens.

POOLEY: I wish I knew, but this is one of the secrets of the political process. In this field, maybe we could just conclude that there was not enough of a sense that we needed to replace state laws as opposed to layer on top of them; there was not a compelling enough need to get over the resistance to preemption. They just don't like it. Preemption is the federal government telling the states what to do.

GREEN: You see that with rights of publicity too. If you ever follow the development and the legislative efforts around rights of publicity, they're going nowhere and it is primarily because they just can't agree on a uniform standard that will overcome some of the concerns. It'd be interesting to see if we can ever have a national right of publicity or even a federal right of publicity that doesn't preempt state rights.

CALO: Fascinating. Okay, questions from our audience?

AUDIENCE: For the ex parte seizure provisions, I want each of you to describe the nightmare scenario, what possibly could go wrong? To anticipate this for district court judges, what should they watch out for, and Dave, particularly for you, if you could characterize a heightened pleading standard. What should it be? What suggestions should we give the courts?

POOLEY: We should probably involve the Federal Judicial Center in this conversation because they have been tasked by the Congress with coming up with a set of best practices for handling these sorts of things, but I'll answer your question. In the terms that were described to me by several federal judges, their nightmare scenario is that the property that has to be seized is bigger than a bread box—a lot bigger than a bread box—and is complicated, and sensitive, and they have to find a place to put it because the statute requires that the property be held by the court.[93] They're worried about that. They can handle paper, but they don't know what might be coming.

ROWE: I think one nightmare provision aside from that has to do with consequences. So, assume you have an innocent victim—assuming that status still exists somewhere—and again, if the word "property" is interpreted very broadly, that they say the person has left

93. 18 U.S.C. § 1836(b)(2)(D)(i) (Supp. IV 2016).

a former employer and has started a competing operation, so the authorities come in and they seize everything that is necessary for the start-up—all the computers, all the information behind the new operation—take it away to be stored. Well in the meantime, what happens? I've seen this happen in state court on a smaller scale where companies actually have to go out of business or they suffer significant financial losses during a period of time when the business simply can't operate because they have been deprived of information. And I think there was a time too—seizure provisions remind me of a time—I don't know if any of you are familiar with the Church of Scientology cases out of California during the late 1990s, where the church moved for preliminary injunctions and temporary restraining orders against former church members who had allegedly taken trade secrets.[94] The California courts—many of them—granted seizure orders[95] and so people entered and removed computers and everything else. And ultimately, most of those orders ended up being reversed,[96] but in the interim, those people were deprived of their property. So I think we could think of those kinds of situations. I think that was what was driving those who were opposed to the seizure provision from the beginning, thinking about the innocent victims that might get caught up in this remedy.

CALO: Maybe you two could connect about the audience question about what would be necessary regarding higher pleadings, and maybe we could take one more question.

AUDIENCE: Hi, I'm a practicing attorney, and one of the areas that wasn't discussed tonight was about contract drafting. There's been a bit of confusion about what language to use in a contract where you're hiring an independent contractor to write a screenplay or to give a record deal versus an actual employee let's say, who actually works at your company on a day-to-day basis. Can you talk a little about that?

94. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1238 (N.D. Cal. 1995) (granting in part and denying in part plaintiff's motion for a preliminary injunction); Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1077–79 (9th Cir. 1986) (reviewing the district court's grant of a preliminary injunction).

95. *See, e.g.*, *Netcom*, 923 F. Supp. at 1240.

96. *See, e.g.*, *Wollersheim*, 796 F.2d at 1091 (reversing the district court's grant of a preliminary injunction); *see also Netcom*, 923 F. Supp. at 1265 (vacating plaintiff's ex parte writ of seizure and ordering return of all articles seized).

GREEN: So we went through that tack ourselves, which is—how can you write in plain English as opposed to the verbosity I guess, the language in the code? What's the right magic words to use?

AUDIENCE: And would you have to?

GREEN: So, you don't have to do anything, right, but you simply don't avail yourselves of the benefits that are afforded under the DTSA. You still have a state secret cause of action, or you may just be limited in terms of the remedies that you can seek. The challenge is that when you want to comply and you try to introduce compliance, you'll find two things: you'll find that fitting that kind of language into the agreement is messy. It was obviously not written by people who draft contracts with artists and entertainers. It raises a lot of questions.

AUDIENCE: Right, it seems to come right out of left field when you put it in there. It's like, "What is this about?"

GREEN: Yeah, and I often see that in settlement agreements. Right, so you've got settlement agreements for release of claims. You've got this language that is unique to California,[97] for example, that sort of pops in there. Look, you don't have to put it in there. I think there are ways in which to parse the language—frankly, just go online and type in the typical query and you'll see different efforts by law firms to try to articulate what a good standard is. I don't necessarily worry so much about that because what most tech companies have done, at least those that I've talked to, is that they actually put their verbatim text, but they just don't put it in the contract. They put a link in the contract to a policy around confidentiality, or they place it in their NDA, where everything in the NDA looks scary and a little bit confusing and so, that's how they get around the practical complications of that language.

POOLEY: One way that a very large client of mine has decided to take care of this, and I think it works fine, is just to say very briefly, the obligations of confidentiality don't apply to any information about wrongdoing that you want to report to the authorities or to a court in confidence in order to use the phrase of the statute that creates the immunity, but it's a single sentence. And what you've done is give them notice that all this doesn't apply, therefore, they have immunity.

97. Bradford P. Anderson, *Please Release Me, Let Me Go! Releases of Unknown Claims in the Penumbra of California Civil Code Section 1542*, 9 U.C. DAVIS BUS. L.J. 1, 2 (2008) ("In any general release with a California nexus, you will likely see a waiver of rights under California Civil Code Section 1542, thereby releasing unknown claims.").

GREEN: Ryan, by the way, I'd like to answer Justin's question very quickly, where you asked about our nightmare scenario. My nightmare scenario is a judge that has, on the one side, an overly sympathetic plaintiff who doesn't understand technology with some loose pleadings in terms of the specificity of what their trade secrets are and the facts suggesting how the secrets were misappropriated. On the other side, there is an unsympathetic defendant, and then in the middle, you've got a cloud services provider who has lots of information, spread across multiple servers, possibly in multiple jurisdictions, and doesn't have an opportunity to educate the court on what seizure in the cloud actually looks like. That's probably the nightmare scenario for a company like Microsoft.

CALO: Me too. When I wake up in the middle of the night, that's usually the first thing I think of: the cloud and what it's going to do. Well, the sign of a great panel is that there are many more things to be asked and said. Please join me in thanking this wonderful panel.