

Prepared Statement of David M. Simon
Senior Vice President for Intellectual Property
salesforce.com, Inc.

Before the

United States House of Representatives
Committee on the Judiciary,
Hearing of the Subcommittee on Courts, Intellectual Property
and the Internet

On

Trade Secrets: Promoting and Protecting American Innovation,
Competitiveness and Market Access in Foreign Markets

Mr. Chairman, Ranking Member Nadler and members of the House Judiciary Committee, I want to thank you for the opportunity to discuss the need for a federal trade secret law on behalf of salesforce.com. This subcommittee's jurisdiction over both intellectual property and the Internet provides the best forum for balancing the need for robust protection of trade secrets and the privacy of millions of users whose business and lives have come to depend upon the Internet from an overbroad trade secret seizure remedy.

I also believe that my company salesforce.com is well suited to testify about that balance. As Forbes magazine's most innovative company in the world for each of the last three years, trade secrets play a vital role in securing our intellectual property. Offsetting our needs for robust trade secret protection is the even more compelling need to protect the data of our hundred thousand plus business customers and 22,000 charities and educational customers. These customers range from the giants of industry and large multinational charities to small businesses and charities.

To be clear, we believe that federal protection of our trade secrets would be helpful and we support the Congressional efforts to strengthen those protections. Nonetheless, in seeking that protection, we cannot violate our customers' and their users' trust. That trust is core to our business. Our customers, both large and small, trust us to protect their data. They trust us to ensure that we will protect the sanctity and availability of their data. They trust us to ensure that they can reap the benefits that the Internet offers without having their businesses interrupted while protecting their trade secrets. And they trust us to protect their users' privacy. The trust and faith of our customers and their users leads me to be here today to express our concerns with the seizure remedies that we have seen in some of the trade secret proposals. These remedies fail to take into account Internet business models that have emerged over the past decade. Not limiting those remedies could result in the loss of this trust that is so vital to our success by leading to the interruption of our customers' businesses and by comprising the secrecy of their data.

The Importance of Trade Secrets to salesforce.com and the Need for Legislation

While we have concerns about remedies in current proposals, trade secrets are among the most important ways we protect our intellectual property. By the very nature of our offerings, which are almost exclusively software as a service (SAAS), virtually all of the actual software sits on our servers and never leaves our secure environment. Generally speaking, our customers' data sits on those servers too. However, since the vast majority of our code is kept under wraps, the knowledge that the law protects the secrecy of our fifteen year, multibillion dollar investment in our code and computing environment is critical to maintaining the trust of our customers and investors. This code and this environment are

protectable as trade secrets as they are not generally known or readily accessible, have economic value as shown by our multi-year thirty percent year on year growth to a \$ 4 billion per year company and are rigorously kept secret.

And we are not the only company that relies upon trade secret protection. Almost all of our 100,000 plus business customers and 22,000 charitable and educational customers require us to keep their information and data that they entrust to us secret. If the law did not aid us in preserving our customers' secrets, our efforts to gain and keep our customers' trust would be for naught. We know this not only from the probing questions that our customers ask to assure themselves about our security but also from research that shows trade secrets are considered by far the most important form of intellectual property protection.¹

However, the current legal environment for trade secrets has several shortcomings. As many others have noted, US trade secret law is far from consistent. Substantive trade secret law is largely controlled by state laws and in some instances purely by state courts that may still rely on outdated common law doctrines. Even though most states have adopted the Uniform Trade Secret Act, others have not. Further, even the states that have adopted the UTSA have many inconsistencies; the actual individual state statutory texts differ and state court interpretations about even identical versions of the UTSA are far from consistent.² As an another example, the definition of trade secrets in the Economic Espionage Act differs from the definition for the same term in the Uniform Trade Secrets Act.³

While some of these differences are subtle, the absence of a uniform federal trade secret law is manifest with respect to international protection. While TRIPs provides an international regime for trade secret law, the protection that is mandated is unfortunately vague. The heart of the relevant clause in TRIPs is vague; it asks whether the trade secret has been acquired or used "in a manner contrary to

¹ According to the National Science Foundation, almost two times the number of managers considers trade secrets the most important form of intellectual property

² D. Almeling, Four Reasons to Enact a Federal Trade Secrets Act 19 *Fordham Int. Property & Media Law Review* 769, 774 (2009); see also *Firetrace USA LLC v. Jesclard*, 800 F.Supp.2d 1042 (D. Ariz. 2011)(noting substantial diversity among state court interpretations about whether the Uniform Trade Secrets Act preempts common law remedies).

³ The Uniform Trade Secret Act defines a trade secret as "Trade secret" means information . . . [d]erives independent economic value . . . from not being generally known to . . . other persons who can obtain economic value from its disclosure or use. California Civil Code § 3426.1(d). The EEA defines a trade secret as to information that "derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839(3).

honest commercial practices.”⁴ As a result, in Europe alone, trade secret law, which to date is not yet controlled by a European Union Directive, is a patchwork of different forms of protection. What is contrary to honest commercial practices in one country may be considered acceptable in other countries. Thus, in some states trade secret is viewed largely as a creature of contract while in other states, the scope of protection varies with the type of secret at issue.⁵

Far more serious, however, is many countries’ failure to recognize trade secrets as a form of property.⁶ That refusal to recognize trade secrets as a species of property can have major consequences with enforcement authorities. For example, some European authorities have disclosed companies’ trade secrets under the logic that the harm in disclosing a trade secret involves purely commercial interests and is not irreparable.⁷ It may not be a coincidence that in denigrating trade secrets as a form of intellectual property, at least some countries’ regulators seem to adversely impact foreign companies from the United States and elsewhere.

While my understanding is that the United States Trade Representative historically has favored stronger trade secret protection, the representative’s staff have felt hamstrung by the inconsistent protections offered for trade secrets at the state and federal level. The lack of consistent protection means that in negotiations the USTR in trying to improve foreign trade secret protection in bilateral and multilateral talks can only seek the lowest common denominator of those state and federal laws. That lowest common denominator approach arises according to my discussions with prior USTR staffs from their need not to advocate for treaty provisions that are inconsistent with domestic U.S. law.⁸ Since we have almost fifty different versions of trade secret law, the only approach that the USTR can take is to advocate for the lowest common denominator instead of advocating for strong trade secret protection.⁹ The lack of consistent protection means that the USTR is

⁴ Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994).

⁵ See, e.g., Report of the European Commission Conference of 29 June 2012, “Trade Secrets: Supporting Innovation, Protecting Know-How” 9 (available at ec.europa.eu/internal_market/iprenforcement/docs/conference20120629/ts_summary_consolidatedfinal20120913_en.pdf).

⁶ *Id.* at 15.

⁷ Case T-201/04 R Microsoft v. Commission [2004] ECR II-4463.

⁸ See generally Testimony of Ambassador Marantis, Hearing before the Subcommittee on Trade of the Committee on Ways and Means, U.S. House of Representatives, 120th Congress, First Session, December 14, 2011 Serial No. 112-TR4 (2012).

⁹ To be clear, within the constraint of a lack of a national trade secret policy, the USTR is an excellent resource. For example, the USTR reports regularly highlight inadequacies in trade secret protection with a focus on the adequacy of remedies

restricted in bilateral and multilateral negotiations from trying to improve foreign trade secret protection. Thus, we believe that providing a robust national trade secret policy embodied in a national law will aid the USTR in the development of a robust international trade secret regime without local biases or discrimination that result in inadequate protection.

While we firmly believe that providing a robust federal trade law will aid all businesses, we also believe that the remedies of such a law must recognize that commercial processes have changed since the Uniform Trade Secret Act was drafted in the pre-Internet era. For the reasons that we will now point out, the remedies provisions need to be updated to take into account new commercial realities.

Background on salesforce.com and its Customers in the Internet Age

To understand why the remedies drafted in a pre-Internet era are inadequate today, one needs to understand how software as a service, whether provided by salesforce.com or our competitors, works for hundreds of millions of users here in the US and around the world. salesforce.com relies on the Internet to provide a variety of software as a service. To process and retrieve that data in our service, our customers such as Wells Fargo and the American Red Cross log into their accounts over the Internet and submit their queries to access their data stored on our servers and receive processed information back. They are able to use all of our offerings to run their business without the complexity of running the software themselves.

Our customers' data and our software are stored in large storage arrays that we call pods. While there are always exceptions, few customers have dedicated storage for their information in our system. Rather, systems such as ours scatter the customer data among a host of storage devices. As a result, the data is sometimes in geographically different locations. Individual customer data at the physical level is intermixed with data of other customers according to complex algorithms that take into account workloads, access speed and security. While an individual customer's data may be arrayed across dozens or hundreds of storage devices intermixed with others' data, no customer has the ability to access the other customer's data without that customer's permission. Any one physical drive at any moment in time could have fragments of hundreds of customers' data. In the blink of the eye, our systems that monitor work loads and security may move some or all of those fragments to different systems with different customers' data in our quest for flawless performance. Notwithstanding this intermixing of data, we have a reputation of providing a secure and robust environment for our customers to store and access the data that drive their billion dollar businesses.

and prevention of discriminatory rules. See US Trade Representative, 2014 Special Report 301 Report 16 (available at ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf).

There are a couple of points to draw from this structure, which is not atypical of businesses that host other people's data and provide software as a service over the Internet. Physically removing or seizing any one physical drive unit will generally remove only a fraction of a typical customer's data. Worse, physically removing that drive may also remove data for dozens, if not hundreds, of other customers' data on that unit. And removing that data could interrupt our customers' business, costing them millions of dollars each and in some instances involving medical customers could even jeopardizing people's lives. It is the current proposals' seizure provisions' failure to take into account how information is handled in the information age that concern us.

Seizures in the Salesforce.com Environment

We understand the need for the seizure authority in trade secret law. In a prior job, I was involved with a criminal investigation and subsequent prosecution of economic espionage. Without the FBI's ability to seize thousands of pages of electronic documents that had been stolen, I am not sure that the case could have been brought.

The problem with the seizure provisions included in many proposals we have seen for a federal trade secret law is they do not take into account this new and increasingly common way of doing business over the Internet. Rather, all of the proposals are based off of normal seizure rules in trademark counterfeiting statutes¹⁰ and copyright statutes¹¹ and in Federal Rule of Civil Procedure 65.¹² These rules and statutes were originally drafted before there was an Internet and, in some instances, were first drafted when computer disk drives had not even been invented.¹³

Consideration of how these rules operate in normal trademark and copyright seizure cases demonstrates a need to change the model for the law. First, ex parte seizures are usually authorized in a sealed courtroom with only the plaintiff and counsel present. Based on the facts presented solely by the plaintiff's counsel, the judge makes a determination of whether the goods are a counterfeit. Ordinarily,

¹⁰ The Lanham Act provides for seizure of counterfeit trademark goods. 15 USC § 1116(d).

¹¹ The Copyright Act incorporates by reference certain subsections of §1116(d). See 17 USC § 503(a)(3).

¹² While on its face, Federal Rule of Civil Procedure 65 does not refer to seizures, courts have approved the appropriateness of using Rule 65 to authorize ex parte seizure orders. See, e.g., *First Technology Safety Systems, Inc. v. Depinet*, 11 F.3d 641 (6th Cir. 1993)(finding § 503(a)(3) inapt and analyzing the appropriateness of a seizure under Rule 65).

¹³ Federal Rule of Civil Procedure 65 was first adopted in 1937. Section 1116(d) was added in 1984 by Pub. L. 98-473, 88 Stat. 1949 (1984).

that requires no technical expertise. In a trade secret case, however, what is a trade secret requires a technical analysis—an analysis that few judges are able to make on their own.¹⁴

These technical determinations go far beyond what is or is not a trade secret. Often trade secret plaintiffs want to seize hard drives to see whether forensics can establish what the alleged wrongdoer may have erased.¹⁵ An expert may submit a truthful declaration about forensics about what information can be gathered from a disk drive taken from a personal computer. The typical trial judge with a degree in history or political science may well be swayed by such “evidence” along with having heard war stories over the years regarding what can be discovered from a disk drive. Yet, the non-party hosting the data will not be present and will be unable to tutor the judge that a PC environment is totally irrelevant to a cloud-based storage warehouse with data being replicated and shifted constantly, irrespective of what the data owner is doing. Nor will the party who hosts the data be able to explain to the judge that this forensic analysis could expose otherwise legally protected third party data, such as health records. Grave harm could be done in the face of such overly zealous or poorly informed private litigants.

Further, the plaintiff who is asking for the ex parte relief will ask the judge for a de minimus bond. Judges have broad discretion in setting bonds and the bond amounts are often hastily arrived at with little or no consideration of the real harms. Many judges believe that requiring significant security or bonds will deny plaintiffs the relief they seek and therefore set de minimus amounts for the security.¹⁶ While a party can recover against security ordered by the court, recovery by the injured party exceeding the amount of the security is a rare exception.¹⁷ That is a first problem with current security requirements for injunctions as security is often too low in view of the potential for harm. Further, Federal Rule of Civil Procedure 65 has a major shortcoming as the amount of security posted only covers the harm to parties in the litigation.¹⁸ The result is that if a court grants a seizure order against

¹⁴ While it is noted that in technical patent cases judges often get tutorials from both sides in the litigation and can appoint their own technical experts, in the context of an ex-parte hearing in a sealed courtroom, these aids are not available to the court.

¹⁵ See *Lexis-Nexis v. Beer*, 41 F.Supp.2d 950 (D. Minn. 1999)(forensic analysis of defendants’ hard drive showed erasure of plaintiff’s files).

¹⁶ In *Bragg v. Robertson*, 54 F. Supp. 2d 635 (S.D. W. Va. 1999) where the court granted a \$5000 bond and then the appellate court reversed the granting of the injunction, leaving the plaintiff with no effective remedy. *Bragg v. W. Va. Coal Ass'n*, 248 F.3d 275 (4th Cir. 2001).

¹⁷ *Intl Assn of Machinists v. Eastern Airlines, Inc.*, 925 F.2d 6, 10 (1st Cir. 1991).

¹⁸ Federal Rule of Civil Procedure 65 (c) “The court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained.” See *O. Grosskopf*

an alleged misappropriator that harms innocent third parties such as salesforce.com, or its customers, there is no ability to recover against the security, even if the amount set was adequate. Thus, current security and bond practice for seizures have several shortcomings.

That harm does not stop at the courtroom, however. When the marshal accompanied by plaintiff's representatives arrives at the storage site, the same technical issues that confronted the district court judge also confront the marshal.¹⁹ Assuming the site owner who hosts the alleged misappropriator's data decides not to risk a contempt citation and admits the marshal (and the marshals do have guns and badges after all), the marshal will be confronted with row after row of equipment racks with hundreds of cables. The site owner is then faced with a Hobson's choice. Either it must comply with the court order, if even possible, by removing disk drives and interrupting the business not only for the alleged misappropriator, but also of dozens or hundreds of innocent customers. Alternatively, the owner of the storage site may refuse compliance so that the businesses of thousands of thousands of customers continue to run but risk contempt citations.

Proposed Solutions

Despite highlighting a number of potential problems with trade secret seizures, we do believe in strong trade secret remedies but subject to certain protections. We believe that the remedy needs procedural and substantive safeguards that are not reflected in the copyright and trademark law remedies that antedate the Internet and software as a service. Our belief is that courts should be prescribed from ordering any seizure of third parties hard disk drives absent compelling evidence of wrong doing by the third-party. Absent such evidence, the appropriate remedy for those who host third-party information is to require the third-party hosting entity to deny access to the specified information and create a copy of the relevant information.

If Congress believes that there are truly unique situation where the harm to third parties justifies seizure of media from a business that hosts third party data, then several protections must be provided. First, the law needs to explicitly recognize that ex parte orders for the seizure of property owned by innocent third parties should be ordered in only the rarest of circumstances. Most hosting

& B. Medina, Remedies for Wrongfully-Issued Preliminary Injunctions, 32 Seattle Law Review 903 ,909 (2009).

¹⁹ See generally A. Kramer & M. Sommers, Taking an Aggressive Stance Against Counterfeiters: An Overview of Trademark Counterfeiting Litigation under the Lanham Act, IP Litigator, September/October 1999 (last viewed at <http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=d0fb159b-947e-427a-b03a-e6d60cf272f5>).

agencies already have the ability to either deny access to accounts or download all of the information in the account that can then be sequestered in case of subsequent attempts to change the information. salesforce.com regularly accomplishes these tasks when responding to subpoenas or other judicial orders. Once access has been denied and the information has been copied, the court can provide for an evidentiary hearing permitting a third-party hosting entity and others who may be harmed by a seizure order to argue to the court whether a seizure is the appropriate remedy on a full evidentiary record. Simply put, there needs to be a heavy thumb on the scales for when the courts so that ex-parte seizures in such circumstances are truly rare.

Second, to avoid harm to the innocent host and their other customers, the law should compel a plaintiff seeking a seizure has to come forward with clear and convincing evidence that the harm it will suffer grossly outweighs the harm the seizure may impose upon these third parties, including the business disruption they may suffer. That showing should also expressly require the party seeking such extraordinary relief to demonstrate clear and convincing evidence why other less damaging alternatives such as denial of access to the information and storing a copy of the information of concern is inadequate.

Third, the court should ensure the information of the innocent third parties is not placed in jeopardy. In particular, upon seizure, the court should direct that the media be placed in the custody of a trusted third-party who will segregate the alleged misappropriator's information from other information and only the directly relevant information may be provided to the plaintiff's counsel under a suitable attorneys eyes only protective order. Otherwise, we could be allowing the information of innocent customers to be put in jeopardy by the process.

Fourth, current procedural rules permit up to fourteen days before a court is required to permit others' to seek judicial intervention to either expunge or limit a seizure order. That is simply too long of a period. Given the potential disruption to innocent hosts and third-parties, the host and any customer or user should be permitted to seek emergency relief from the order within four hours. Many customers insist on "seven-nine's service (99.99999%) up time." Translated into laymen's terms, that means they expect less than six minutes of interruption in an entire year to their service. Anything longer simply results in too much harm. As a result, the right to seek urgent relief from an ex-parte order is just as important as the right for plaintiffs to be able to obtain prompt ex-parte relief and rules need to reflect this urgency.

Fifth, the security that the court requires to protect against erroneous seizure orders cannot be the limit that is placed upon third-parties inadvertently harmed by the order. Current law only requires bonds for parties but non-parties will need protection if seizures are permitted under this regime. Arbitrary limits from security regimens designed to protect only plaintiffs are demonstrably inadequate. My experience in trademark and copyright cases is that these security amounts are

often an afterthought and bonds rarely exceed \$100,000. Judges even have discretion to set the security at zero.²⁰ Rather, in entering the order, the court should require security commensurate with the number of potentially impacted parties and the magnitude of their businesses along with providing an advisory to the plaintiff that the plaintiff is liable for all harms that the seizure order can ensue. Such financial incentives have long been recognized as a way to avoid over zealous litigants; even the drafters of the Uniform Trade Secret Act included a provision to deal with abusive trade secret plaintiffs.²¹ Simply put, changes in technology during the last twenty years raise the need for adequate protection from such overzealousness where the potential harm to third parties have escalated since the drafting of the UTSA.

Conclusion

While we believe in strong trade secret remedies, we also believe that if we are going to enhance our trade secret protections then the seizure provisions need to also be updated to reflect modern commercial practices. Information stored over the Internet by alleged misappropriators is intertwined with third parties' information and seizure orders places those third parties' businesses and confidential information at risk. Given this committee's special purview over the Internet, we trust that any legislation will provide adequate protections.

²⁰ *District 17, United Mine Workers Assoc. v. A & M Trucking, Inc.*, 991 F.2d 108, 110 n.2(4th Cir.1993)("The court's complete silence as to the bond requirement for the injunction distinguishes the instant case from those in which a court, in its discretion, chooses to set the bond amount at zero.)

²¹ See, e.g., Section 4 of the Uniform Trade Secret Act, providing for attorneys fees for "claims of misappropriation in bad faith."