Professors' Letter in Opposition to the

"Defend Trade Secrets Act of 2014" (S. 2267) and the

"Trade Secrets Protection Act of 2014" (H.R. 5233)

August 26, 2014

To the sponsors of the above-referenced legislation and other Members of the United States Congress:

The undersigned are 31 professors from throughout the United States who teach and write extensively about intellectual property law, trade secret law, innovation policy and/or information law.[1] We urge Congress to reject the proposed legislation to create a new private cause of action under the Economic Espionage Act of 1996 ("EEA"),[2] known as the "Defend Trade Secrets Act of 2014" ("DTSA") and the "Trade Secrets Protection Act of 2014" ("TSPA," collectively, "the Acts"). As explained in Senator Coons' press release announcing the introduction of the DTSA,

> In today's electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. These losses put U.S. jobs at risk and threaten incentives for continued investment in research and development. Current federal criminal law is insufficient.[3]

While we acknowledge the need to increase protection both domestically and internationally against domestic and foreign cyber-espionage, this is not the way to address those concerns. Instead, as explained below, the Acts will create or exacerbate many existing legal problems but solve none. Accordingly, we oppose their adoption.

---

[1] Many of the signatories to this letter also have extensive intellectual property litigation experience in state and federal courts, including trade secret litigation.

[2] 18 U.S.C. § 1830 *et seq.* (2014).

[3] Press Release, *Senators Coons, Hatch introduce bill to combat theft of trade secrets and protect job*s, Office of Senator Christopher Coons (April 29, 2014), available at http://www.coons.senate.gov/newsroom/releases/release/senators-coons-hatch-introduce-bill-to-combat-theft-of-trade-secrets-and-protect-jobs.

The Acts should be rejected for five primary reasons:

1. <u>Effective and uniform state law already exists.</u>

United States trade secret law was developed and is applied against a backdrop of related state laws and legal principles that reflect the values and interests of individual states, particularly with respect to issues of employee mobility and free competition. There is already a robust and uniform body of state law governing the protection of trade secrets in the United States, the Uniform Trade Secrets Act ("UTSA"), which has been adopted by 47 of 50 states.[4] Built on over 100 years of case law, numerous US companies have used it with success to combat trade secret misappropriation by both employees and non-employees. Similarly, criminal prosecutions under the existing EEA are increasing and are addressing the concerns motivating introduction of the Acts.[5]

This deep body of state law creates its own benefits; as the general principles of US trade secret law are well-established and substantially uniform, there is a high level of predictability by and for US businesses and their attorneys. But because the Acts cannot entirely preempt state trade secret law (for reasons that are explained below), they will result in confusion, as well as less uniformity and predictability. As a result, the business community will suffer from decreased predictability in the law with, as discussed below, no corresponding benefits.

---

[4] North Carolina has adopted a statute that is substantially similar to the UTSA. *See* N.C. Gen. Stat. § 66-152 *et seq*. (2014). New York generally follows the Restatement (Third) of Unfair Competition (which is largely based upon the UTSA). *See Wiener v. Lazard Freres & Co.*, 241 A.D.2d 114, 124, 672 N.Y.S.2d 8, 15 (1st Dep't 1998) (applying Restatement (Third) of Unfair Competition to define a trade secret in New York). Massachusetts trade secret law is based in small part on statutory law and in large part on common law that is consistent with what is expressed in the Restatement (Third) of Unfair Competition. *See* Mass. Gen. Laws Ann. ch. 93, §§ 42 to 42A and Mass. Gen. Laws Ann. ch. 266, § 30(4).

[5] *See* Webinar Press Release, *Combating Trade Secret Theft: What Every Company Should Know about the EEA and CFAA*, Ballard Spahr LLP (April 24, 2014), *available at* http://www.ballardspahr.com/eventsnews/events/2014-04-24-combating-trade-secret-theft.aspx (asserting that "the U.S. government has made combating corporate and state-sponsored trade secret theft a top priority, and both the [Department of Justice] and [Federal Bureau of Investigation] have increased their investigations and prosecutions of it."); *see also* Indictment, *United States v. Wang Dong et al*., Crim. No. 14-118 (W.D. Pa. May 1, 2014) (criminally charging five members of China's People's Liberation Army with economic espionage and computer hacking).

2. <u>The Acts will damage trade secret law and jurisprudence by weakening uniformity while simultaneously creating parallel, redundant and/or damaging law.</u>

Generally, the Commerce Clause of the United States Constitution[6] gives Congress power to legislate trade secret law, but Congress' power is limited.[7] To address this limitation, the Acts require a convoluted and untested jurisdictional clause that currently states that the law would only apply to trade secrets that are "related to a product or service used in or intended for use in, interstate or foreign commerce." While the precise meaning of this clause is unclear and unsettled, it obviously does not (and cannot) describe all US trade secret information, as not all trade secrets are necessarily "related to a product or service … used in … commerce," like many customer lists. Accordingly, the Acts will not supplant state law and we expect that the bulk of trade secret claims will still be based upon state law.

Moreover, even under the Acts, ancillary state law will still apply with respect to a number of important issues. Primary among them are ownership of inventions, definitions and obligations of confidential relationships, and enforceability of non-compete agreements. If the concern is preservation of evidence and enforceability of judgments, the US already has a rich body of law and procedure that solves most of these problems, including the diversity jurisdiction of federal courts, multi-district litigation procedures, cross-border discovery procedures, and cross-border enforcement procedures. Additionally, it is worth noting that the Acts cannot and do not address the significant systemic challenges associated with getting jurisdiction over and enforcing judgments against foreign entities, infirmities which, standing alone, should cause Congress to pause.

The Acts' seizure provisions require special attention. The DTSA's provisions that would authorize motions to preserve evidence and seize property are not necessary in light of the broad discretion that federal courts already have under the Federal Rules of Civil Procedure[8] to grant temporary restraining orders *ex parte* and would arguably

[6] U.S. CONST., Art. I, § 8, cl. 3.

[7] *See The Trademark Cases,* 100 U.S. 82 (1879) (Congress has limited powers to legislate under the Commerce Clause).

[8] *See* FRCP 65 (2014).

interfere with the Rules Enabling Act process.[9] Moreover, litigants can already request preliminary relief in trade secret cases and there are severe consequences for the destruction of evidence under existing law and rules of professional conduct.

Similarly, the TSPA's provision, while not as broad as the DTSA's, acknowledges but fails to ameliorate the problems and risks associated with seizure. First, the TSPA specifies that such relief is only available upon a showing that the preliminary relief that is available under FRCP Rule 65(b) is inadequate, a threshold that we believe will be difficult to establish, thereby making the provision superfluous. Second, the required showing is nearly identical to the standards that federal courts currently apply when deciding whether to grant preliminary relief, but with the odd additional requirement that "the applicant has not publicized the requested seizure." The purpose of this requirement and the provision requiring "protection from publicity" is unclear, but we are concerned that the TSPA requires a level of secrecy about court rulings that is unprecedented. The required procedures and findings are also bound to impose great burdens on the federal courts, and like the problems with the jurisdictional clause discussed above, arguably put trade secrets at greater risk. Of even greater concern (for reasons that are explained below), we are concerned about the anti-competitive effects of the seizure remedy.

Therefore, the Acts will exacerbate rather than solve the perceived problem of a lack of uniform state law, with no corresponding benefits and several significant drawbacks.

3. <u>The Acts are imbalanced and could be used for anti-competitive purposes.</u>

A hallmark of all US intellectual property laws, including trade secret law, is that they include limiting doctrines that are designed to achieve the appropriate balance between the protection of intellectual property rights and the preservation of free competition. While the Acts appropriately define "improper means" not to include the acts of reverse engineering and independent derivation, other limits on the scope of trade secret protection are missing. In particular, we note that the Acts do not explicitly limit the length of injunctive relief to the period of lead-time advantage, a critical limit on potentially interminable injunctions that can prevent fair competition, employee mobility and new innovation. Additionally, the seizure provisions of both Acts, but

[9] *See* 28 U.S.C. § 2072 (2014).

particularly of the DTSA, introduce a new form of preliminary relief that is fraught with potential misuse due to the fact that such relief could be granted *ex parte,* without either notice to or an opportunity to be heard by the defendant(s). Both of these failures could render the Acts a weapon of anti-competition and societal damage with, again, no corresponding benefits.

4. The Acts increase the risk of accidental disclosure of trade secrets.

Because of the jurisdictional issue discussed in Point Two, there will likely be many motions to dismiss for lack of subject matter jurisdiction that, as a practical matter, will require the plaintiff to identify and disclose its trade secrets early in the litigation. But under all existing US trade secret law, the understandable common plaintiff strategy is to delay the identification and disclosure of trade secrets until the latest possible moment due to the heightened disclosure risk that comes from even the confidential sharing of information. Thus, if the existence and nature of the alleged trade secrets are necessary to establish jurisdiction under the Acts, defendants in trade secret cases will be justified in demanding earlier disclosure of the alleged trade secrets. This will result in a greater risk of accidental disclosure of the trade secrets and slow down the litigation process, with, again, no corresponding benefits.

5. The Acts have potential ancillary negative impacts on access to information, collaboration among businesses and mobility of labor.

While the Acts appear to be ineffective and/or unnecessary in combatting actual cyber-espionage and other misappropriation, they may have more impact on the negative side of the equation, namely, as an additional weapon to prevent public and regulatory access to information, collaboration amongst businesses, and mobility of labor. Although not often linked, there is a direct relationship between availability of trade secret misappropriation claims and regulatory access to information. Labeling information as a trade secret has become a common way to prevent public and even regulatory access to important information ranging from the composition of hydraulic fracturing fluids to the code inside of voting machines, all of which have compelling (but not uncontroversial) reasons for public access in a democracy. These access to information issues – which do not necessarily correlate with support for or opposition to the subject activities or industries – are exacerbated even by otherwise ineffective trade secret law.

The threat of a trade secret misappropriation action can and does have a chilling effect on collaborative innovation efforts between businesses and can be used by those who would rather compete in a courtroom than the marketplace to quell legitimate competition. Adding a new remedy that allows companies to seek preliminary relief to seize wide swaths of property (including computer networks and servers) would only heighten the risk that trade secret litigation will be used as an anti-competitive tool.[10]

Lastly, the importance of employee mobility to the strength and growth of our economy cannot be overstated. Reducing mobility of labor impacts not only those employees who are directly affected, but their new employers and the families of the affected employees. It also has an adverse impact on society by reducing the diffusion of skills and knowledge and stifling the innovation that flows from the sharing of ideas and information. State law currently protects employee mobility; the Acts do not.

If Congress is going to further strengthen arguments against access to information and simultaneously further limit mobility of labor and potential innovative collaboration, as adding yet another potential (even if ineffectual) trade secret misappropriation cause of action to the books would do, it should be because the benefits of such a cause of action outweigh the costs. Here, as previously discussed, the benefits are nonexistent. Therefore, the ancillary costs are not nearly outweighed; in fact, the scale leans decidedly to one side.

In sum, Congress is rightly concerned about cyber-espionage by foreign countries and foreign business interests, but adding to well-established domestic trade secret law to address such concerns is incomplete, ill-advised, and potentially dangerous. The Acts are incomplete solutions because the definition of a trade secret

[10] The Acts' seizure provisions are eerily similar to the problematic provisions in copyright law's failed Stop Online Piracy Act ("SOPA") and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act ("PIPA"). SOPA and PIPA were intended to combat online copyright infringement, but were never passed in large part because of problematic provisions related to removal of allegedly infringing websites from the Internet. *See* Mark Lemley, David S. Levine and David Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (Dec. 19, 2011) ("Websites can be 'completely removed from circulation'—rendered unreachable by, and invisible to, Internet users in the United States and abroad—immediately upon application by the government, without *any* reasonable opportunity for the owner or operator of the website in question to be heard or to present evidence on his or her own behalf. This falls far short of what the Constitution requires before speech can be eliminated from public circulation") (emphasis in original).

under US (and international law) is limited and does not protect all of the information that may be the subject of cyber-espionage, or even all of the information that many businesses believe are trade secrets. The Acts are ill-advised because they focus on trade secret misappropriation instead of the bad acts of cyber-espionage and foreign espionage – *which is where Congress should focus its legislative efforts*.[11] Finally, the Acts are dangerous because the many downsides explained above have no – not one – corresponding upside.

Thus, for all of the above reasons, we oppose the Acts and urge their rejection. Additionally, if not withdrawn, we ask Congress to schedule full hearings so that our views, and all others, can be fleshed out, challenged and discussed in an open forum. The important issues that you are trying to address require and deserve more deliberation and input. While we recognize that there have already been some hearings, the specific language of the Acts, their effectiveness and their ramifications must be discussed and debated in public hearings.

With regard to this letter, you may address any reply or correspondence to its authors and organizers, Professor David S. Levine (dsl2@princeton.edu) and Professor Sharon K. Sandeen (ssandeen@hamline.edu).

Signed,[12]

Professor Brook K. Baker
Northeastern University School of Law

Professor Mario Biagioli
UC Davis School of Law

Professor Barbara B. Bressler
DePaul University College of Law

---

[11] *See, e.g.*, Sharon K. Sandeen, *The Third Party Problem: Assessing the Protection of Information through Tort Law*, in INTELLECTUAL PROPERTY PROTECTION OF FACT-BASED WORKS (Robert F. Brauneis, ed., 2009) (discussing ways to combat bad acts that do not depend on the IP status of the underlying information).

[12] All institutions are listed for identification purposes only and the signatories do not speak for or on behalf of their respective institutions.

Professor Irene Calboli
Marquette University Law School

Professor Michael A. Carrier
Rutgers Law School

Professor Brian W. Carver
University of California, Berkeley
School of Information

Professor Eric R. Claeys
George Mason University School of Law

Professor Thomas F. Cotter
University of Minnesota Law School

Professor Eric Fink
Elon University School of Law

Professor Shubha Ghosh
University of Wisconsin, Madison, School of Law

Professor Eric Goldman
Santa Clara University School of Law

Professor Robert A. Heverly
Albany Law School of Union University

Camilla Hrdy
Fellow
Center for Technology, Innovation and Competition
University of Pennsylvania Law School

Professor Peter Jaszi
American University Law School

Professor Lawrence Lessig
Harvard Law School

Professor David S. Levine
Elon University School of Law
Visiting Research Collaborator
Center for Information Technology Policy
Princeton University

Professor Yvette Joy Liebesman
Saint Louis University School of Law

Professor Brian J. Love
Santa Clara University School of Law

Professor Joseph Scott Miller
University of Georgia School of Law

William J. Moner
Instructor of Communications and Interactive Media
Elon University School of Communications

Professor Ira Steven Nathenson
St. Thomas University School of Law

Professor Phillip Edward Page
South Texas College of Law

Professor Frank Pasquale
University of Maryland School of Law

Professor Michael Risch
Villanova University School of Law

Professor Elizabeth Rowe
University of Florida Levin College of Law

Professor Pamela Samuelson
University of California, Berkeley School of Law

Professor Sharon K. Sandeen
Hamline University School of Law

Professor Kurt Saunders
California State University, Northridge
David Nazarian College of Business and Economics

Professor Christopher Seaman
Washington and Lee University School of Law

Professor Katherine J. Strandburg
New York University School of Law

Professor Tim Wu
Columbia Law School