Trade Secrets: How Well Should We Be Allowed to Hide Them? 
The Economic Espionage Act of 1996

Rochelle Cooper Dreyfuss
New York University School of Law
Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996

Cover Page Footnote
"I wish to thank Harry First."
Trade Secrets: How Well Should We Be Allowed To Hide Them? The Economic Espionage Act of 1996

Rochelle Cooper Dreyfuss*

_The secret that I hide..._
_How will they hear?_
_When will they learn?_
_How will they know?**_

INTRODUCTION

Something seems to have gone awry in the intellectual property bargain. Here is my understanding of how this bargain is supposed to work: a creator discloses new information in exchange for which the state grants him protection against free riders for a limited period of time. For the creator, the bargain is advantageous because it allows him to capture a reward sufficiently large to recoup the costs of inventing and earn a substantial profit. From the point of view of the state, the potential for profit creates incentives to innovate. More important, the innovations that this system encourages become contributions to the storehouse of knowledge. To make the bargain meaningful, however, that contribution has to

---

* Professor of Law and Director of the Engelberg Center on Innovation Law and Policy, New York University Law School. I wish to thank Harry First for his close reading and illuminating comments on an earlier draft. A version of this Essay was presented on April 17, 1998, at the Sixth Annual Conference on International Intellectual Property Law and Policy at Fordham University School of Law.

** MADONNA, Live to Tell, on TRUE BLUE (Sire Records 1986).
be "real"—real in the sense that the must not already be a part of the knowledge base. Also real in that the contribution has to be genuinely placed into the knowledge base, that is, disclosed in a manner that allows others to learn from it during the term of exclusivity, and utilize it without restriction when the term of exclusivity expires.

To be sure, not all intellectual property law makes this bargain quite as explicitly as I have done. In trademark law, for example, the "innovation" is mainly goodwill, which not everyone would consider a contribution to the storehouse of knowledge. Nor is it always the case that the bargain is examined every time a claim for protection is made. Thus, there are copyrights that protect works that are not very innovative, and trade secrets are generally enforceable without direct scrutiny of their degree of novelty. Further, the public's interest in free access is not always directly safeguarded. For example, neither trademarks nor trade secrets are subject to a specific term of years. Nonetheless, in all the traditional intellectual property regimes, the basic contours of the bargain are always in place: fair use creates a way for the public to utilize trademarks even while they are protected; the subject matter restrictions of the Copyright Act, coupled with its definition of infringement, keep non-novel material in the public domain; the definition of a trade secret eliminates from the ambit of protection information that is already generally known. And although in some cases, there is no specific time when the rights expire, so far, they have all always eventually ended. For patents and copyrights, the rights end at the expiration of the statutory term, for trademarks, the rights end through abandonment, and for trade secrets, through reverse engineering, independent discovery, or inadvertent disclosure (in today's terms, "leaks").

Now, what has gone wrong? Recent changes (or proposed changes) in the law are making it possible to acquire exclusive rights in information that is not new, and to acquire rights in new information without meaningfully placing that information in the storehouse of knowledge. For example, I have written about ex-

panding trademark rights and rights of publicity. I will not revisit that analysis here, except to repeat that as interpreted, these provisions create nearly perpetual protection for symbolic representations that are not necessarily novel, that have significant expressive impact, and that do not appear to go into the storehouse of knowledge in any real sense. A recent amendment to the Lanham Act protecting famous marks against dilution—a concept much more nebulous than consumer confusion—exacerbates this problem. A new bill to register and protect trade dress goes even further, for it covers a large range of materials, both packaging and product configurations, without the need to demonstrate any informational content whatsoever. Similar changes have occurred, or are proposed, in the copyright industries. Thus, questions have long been directed at the way that copyrights in computer programs are treated, for the Copyright Office’s willingness to register programs without full disclosure has led to a situation where access to unprotectable ideas is denied. The same may soon hold true for

3. See Rochelle Cooper Dreyfuss, We Are Symbols and Inhabit Symbols, So Should We Be Paying Rent? Deconstructing the Lanham Act and Rights of Publicity, 20 COLUM.-VLA J.L. & THE ARTS 123 (1996) (analyzing how images are perceived and interpreted and how to decide when a proprietor’s interest in capturing the value in what has been created ends and the public’s interest in using that creation symbolically begins) [hereinafter Dreyfuss, We are Symbols]; Rochelle Cooper Dreyfuss, Expressive Genericity: Trademarks as Language in the Pepsi Generation, 65 NOTRE DAME L. REV. 397 (1990) (criticizing recent case law for paying insufficient attention to the expressive dimension of trademarks to their powerful role in the vocabulary as metaphors and symbols) [hereinafter Dreyfuss, Expressive Genericity].

4. See id.


7. H.R. 3163, 105th Cong. (1998). As proposed, the bill requires that trade dress be inherently distinctive, but does not require a showing that customers associate the trade dress with any particular message. Admittedly, this definition conforms to current case law, see Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992), but without this legislation, there was some hope that the lower courts would understand Two Pesos to have been overruled sub silentio, see Qualitex Co. v. Jacobson Prod. Co., Inc., 514 U.S. 159 (1995), which requires a showing of secondary meaning in connection with the protection of color.

8. See Patents, Trademarks, and Copyrights, 37 C.F.R. §§ 202.20(c)(2), 202.21 (1997); David A. Rice, Sega And Beyond: A Beacon For Fair Use Analysis... At Least
factual material. Unless carefully drafted, meeting the demand for database protection is likely to withdraw significant amounts of raw material from the storehouse of knowledge.\(^9\)

Despite all of these problems in trademark and copyright law, it is probably fair to say that nothing is as likely to affect the creative environment as much as two recent developments in trade secrecy law. At the state level, there is a proposal to amend Article 2 of the Uniform Commercial Code ("U.C.C.") to cover intellectual property licensing,\(^10\) and at the federal level, there is the 1996 enactment of the Economic Espionage Act (the "EEA").\(^{11}\) These developments have much in common. Both drastically change the bargain between the public and the rights holder. By moving the core divide between what is secret and what is not, they allow for the protection of material that is not new. And by making trade secrets less susceptible to exposure, they both substantially eliminate the possibility that the right holder’s contribution, such as it is, will ever go into the domain of the public.

Significantly, neither proposed Article 2B nor the EEA was primarily the work product of the intellectual property community. Commercial lawyers, like those who wrote Article 2 on the sale of goods, largely drafted Article 2B. Their interest was initially to create a mechanism for contracting in cyberspace. Toward the end of the project, the decision was made to expand Article 2 to cover the licensing of intangibles more generally; thus, it was rather late As Far As It Goes., 19 U. DAYTON L. REV. 1131, 1151 (1994); S. Carran Daughtrey, Reverse Engineering of Software for Interoperability and Analysis, 47 VAND. L. REV. 145, 153-55 (1994).

9. See Jane C. Ginsburg, Creation and Commercial Value: Copyright Protection of Works of Information, 90 COLUM. L. REV. 1865, 1916 (1990). See generally, Jessica Litman, Copyright and Information Policy, 55 LAW & CONTEMP. PROBS. 185 (1992) (arguing for a reversal in the current course of copyright expansion); J.H. Reichman, Electronic Information Tools—The Outer Edge of World Intellectual Property Law, 17 U. DAYTON L. REV. 797 (1992) (suggesting that the tension that arise when information is viewed wither as a "literary work" or as a "tool" confirm the need for a new intellectual property model that is not premised on the classical distinctions between "art" and "inventions").


in the day that intellectual property lawyers, their bar associations, and their clients became heavily involved. By the same token, the EEA is best viewed as an outgrowth of concern over what nations will do with the spies and spying equipment left over from the Cold War. In the Senate, the legislation was considered by the Select Committee on Intelligence and the Judiciary Subcommittee on Terrorism, Technology, and Government Information; in the House, the Subcommittee on Crime of the Judiciary Committee had primary responsibility for the legislation. Although hearings were held, the witnesses were not members of the intellectual property bar, but rather people like Louis J. Freeh, Director of the Federal Bureau of Investigation. In the case of both measures, the drafters focused on protecting the value of existing works, rather than supporting an environment in which creativity and innovation would continue to take place. Indeed, the drafters of these provisions seem to have entirely missed the dynamic quality of invention—the fact that knowledge builds upon itself; that existing works are not only output that can be exploited, but also the input on which innovators of the future depend.

In a companion piece, I analyze proposed Article 2B of the U.C.C. More specifically, I demonstrate in some detail how Article 2B’s policy of transactional autonomy will alter the structure of intellectual property protection. I argue that some of these effects are likely to run afoul of national innovation policy and are problematic from a normative perspective. This Essay analyzes the EEA. Part I describes the Act, its legislative foundation, and reviews the five key features of the statute. Part II explores the Act’s likely impact on innovation. This Essay concludes that if the EEA

is interpreted broadly, it will to stifle innovation by reducing the flow of public domain information.

I. THE EEA

It will probably take some time before the precise contours of the EEA are well understood. Not only are its legislative origins atypical, but its intent is, in some ways, obscure. The legislative history is clear enough. Congress was concerned that there was insufficient protection against the unauthorized appropriation of intellectual products. At the federal level, copyright and patent laws protect only a small part of the "proprietary information" that is valuable to American industry. The rest is secret information.15 To be sure, there are relevant criminal statutes—most obviously, the Interstate (National) Transportation of Stolen Property Act 16 and the statutes that criminalize mail fraud 17 and wire fraud.18 However, Congress believed these enactments to be of limited value. The former requires a "physical taking of the subject goods;" 19 the latter cannot reach appropriations that do not involve the use of the mail or wires.20 At the state level, protection for trade secrets also

15. See S. Rep. 104-359, at 17 (1996) ("proprietary information, in contrast with copyrighted material and patented inventions, is secret. The value of the information is almost entirely dependent on its being a closely held secret.").
20. One can question Congress' judgment. Courts have been very lenient when determining the role that the use of mail or wire must play in the fraud alleged in the indictment. However, these statutes may have other limitations. Past mail and wire fraud cases involving secret information have all concerned breaches of fiduciary duty. See, e.g., Carpenter v. United States, 484 U.S. 19, 28 (1987) (holding that the conspiracy to trade on employer's confidential information is within the reach of the mail and wire fraud statutes). Not all misappropriations involve breaching such obligations. In addition, the enactment of special legislation sends a message to prosecutors that this is an area where Congress wants resources placed.

There are a few other federal criminal statutes that can be used to protect proprietary information, but they too have significant limitations. For example, the Trade Secrets Act, 18 U.S.C.A. § 1905 (West 1998), penalizes only governmental employees who disclose information in government control. The Racketeer Influenced and Corrupt Organizations Act (RICO), Pub. L. 91-452, 84 Sta. 941 (codified as amended in 18 U.S.C.A. §§ 1961-1968 (West 1998)), only enhances the punishment imposed for acts unlawful under
exists, but Congress did not consider these regimes to be adequate either. It found that companies often fail to avail themselves of their civil remedies due to the cost of pursuing legal action and the possibility that the defendant will be found judgment proof. Further, Congress noted that "[e]ven if a company does bring suit, the civil penalties often are absorbed by the offender as a cost of doing business and the stolen information retained for continued use."21 Congress also spoke of a need for legislation that is comprehensive, meaning protection that transcends state and national borders.22

The question, however, is how Congress accomplished its goals. It could have created an analogue to patent and copyright law, but these laws do not have an extraterritorial reach.23 Moreover, they share with state civil law the problems of the resource-deficient plaintiff and the judgment-indifferent defendant. Further, any such legislation might run afoul of the Supreme Court's decision in Feist Publications, Inc. v. Rural Telephone Service Co.,24 which read the Copyright and Patent Clause of the Constitution25 as disabling Congress from recognizing rights in the subcopyrightable and subpatentable materials that constitute the bulk of "proprietary information."26

One alternative available to Congress was to use its Commerce Clause authority to criminalize violations of state civil law: that is, to create criminal liability for committing the tort of misappropriation as defined by state law. Perhaps that is what the EEA was intended to do, but that conclusion is by no means clear. On the one hand, the EEA appears to track the subject matter definitions of state law, and to prohibit "unauthorized appropriation"—a term not

22. See id. at 4 (speaking of information "in interstate and foreign commerce").
23. For a suggestion to this effect, see Christopher Rebel J. Pace, The Case for a Federal Trade Secrets Act, 8 HARV. J.L. & TECH. 427 (1995), which includes a detailed state-by-state analysis of state laws.
too different from the familiar "misappropriation" of state law. At the same time, however, the statute departs from state trade secrecy law in several important respects. Its definition of unauthorized appropriation is different from that found in the states. The statute also includes state-of-mind elements, including the intent to benefit another entity and to deprive the "owner" of the secret's value, which are unknown to state causes of action—as, indeed, is the concept of owner, as opposed to rights holder.27 Finally, the statute creates rights against interceptions that occur outside the United States, which state laws could probably never reach, and—given its criminal nature—also departs from state legislation by substituting punishment for remedial action.28

The result is something of a mongrel. The EEA's many novel provisions will provide courts with difficult questions to resolve, but since the Act is not based on federal intellectual property law, federal criminal law, or state intellectual property law, it is difficult to predict what case law and traditions courts will draw upon in resolving them. This Part describes the five key features of the statute: subject matter, unauthorized appropriation, state of mind, extraterritoriality, and punishment. It points out some of the questions that EEA prosecutions are likely to raise, but it can do no more than suggest what courts should consider when interpreting the statute.

27. See 18 U.S.C.A. § 1832 (West 1998). The term "owner" is defined in section 1839(4) of the EEA, as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed." 18 U.S.C.A. § 1839(4) (West 1998). The difference between the criminal and civil emphasis may be attributable to the fact that there is more concern in civil litigation about the number of potential lawsuits arising from a single breach of a license. Accordingly, standing in the licensing situation is carefully circumscribed. Since only the government can bring a criminal prosecution, the definition of the victim can be more expansive here. Including the licensor as owner may, however, raise other questions. See infra notes 87-89 and accompanying text.

A. Subject Matter

Despite the legislative talk of "proprietary information," the EEA as codified is framed in terms of "trade secrets." These are defined as follows:

[A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and
(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public...

The thrust of this definition appears to be very similar to the analogous sections in the two principal sources of state trade secrecy law, the Uniform Trade Secrets Act ("UTSA"), which is the basis of state trade secrecy statutes and the Restatement (Third) of Unfair Competition ("Restatement"), which summarizes state common law of trade secrecy. All three protect information that requires an investment to create and that is valuable by reason of the fact that it is not publicly known. The holder of the right—or the owner under the EEA—must take reasonable measures to keep the information secret.

The first part of the provision, the types of information that qualify for protection, is not likely to raise many questions. The EEA's list is much longer than the comparable sections of the UTSA and the Restatement, which should lead courts to interpret the provision broadly—to include such "information" as marketing strategy and customer lists, which have sometimes raised questions in state cases. The two provisos, that the information be secret and reasonable measures be employed to keep it secret, are much more likely to prove problematic, for neither the statute nor its legislative history define what is considered secret or explains what measures owners must reasonably take quickly for this protection.

One way that courts could handle the problem would be by deferring to state law, taking the position that the EEA was basically meant as a criminal adjunct to state regimes and should be interpreted as such. The structural commonality between this provision and state laws lends support to the above proposition. Moreover, adopting it would have the advantage of allowing federal courts entertaining EEA cases to rely on the elaboration of these terms in the case law of the state in which the violation took place. For example, if information was appropriated in Utah, then the court would look to Utah decisions determining what is considered secret and what actions were reasonable.

A number of problems can, however, be anticipated with this approach. First, cases that cross state lines would raise choice of law issues. For example, if the information taken in Utah were used in California, would Utah or California trade secrecy law apply? Even more difficult would be the choice of law questions

32. Compare supra note 30 and accompanying text, with Restatement (Third) of Unfair Competition § 39 (1995) (providing that the information be "sufficiently valuable and secret to afford an actual or potential economic advantage over others"; no specific examples of subject matter are provided, except in commentary), and Uniform Trade Secrets Act, § 1(4), 14 U.L.A. 433, 438 (1985) (using language similar to subsections (A) and (B), and providing as examples "a formula, pattern, compilation, program, device, method, technique, or process").

33. See H.R. Rep. No. 104-788, at 7 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4026 ("While it will be up to the court in each case to determine whether the owners efforts to protect the information in question were reasonable under the circumstances, it is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.").

34. See, e.g., Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp., 139
arising from foreign activities. Second, the statute was, as noted above, meant to be comprehensive. That goal might be regarded as precluding outcomes that depend on the vagaries of particular state legal regimes. Third, the many other provisions of the Act that differ from state law demonstrate that the statute was meant to do more than merely criminalize state torts.

The other approach would be to interpret these provisions from first principles. One way to think of the secrecy requirement in trade secrets law is as a substitute for the quality dimension of other laws—the novelty and nonobvious requirements of patent law, 35 and the authorship and originality requirements of copyright law. 36 Under this view, the real issue regarding subject matter is whether the information is new—new to the world or new to the industry that is using it. 37 Secrecy is a proxy for that determination because information that is known is perforce not secret. The same could be said about reasonable efforts to maintain secrecy. Here, the notion is that the owner's actions regarding the information is probative of its novelty. The owner can be assumed to know his own field. Unless the information were novel, meaning it had value by reason of being secret, he would not bother to protect it. To the extent this is true, courts facing difficult questions about whether information qualifies as a secret or was subject to reasonable efforts to maintain secrecy could supplement their consideration of the defendant's activities with a look at the novelty of the information at issue.

Three other considerations can also be brought to bear on the question of interpreting which actions an owner must reasonably take to qualify for protection. One is that the reasonableness requirement can operate as a replacement for requiring the trade secrecy holder to give notice of the intent to assert proprietary rights. Prior to joining the Berne Convention, virtually all American intellectual property laws required notice. 38 The justification was

---

F.3d 1396, 1410 (11th Cir. 1998) (applying Massachusetts law on unfair trade claim and Georgia law on trade secrets claim).

37. See GOLDSTEIN, supra note 30, at 125.
that a notice requirement maximizes the usage of those intellectual products that are freely available. Notice also prevents recipients of non-free information from unwisely investing in it by building upon it or commercializing it. Courts could make the EEA conform to this tradition by holding that owners who do not extract promises of confidentiality from those who are privy to their secrets have not taken reasonable efforts to maintain secrecy.39

The next consideration is commercial morality. Many state intellectual property laws grew and are explained in part by the notion that unauthorized appropriation is immoral.40 To the extent that this theme is still in play, decisions on what is reasonable under the EEA should be informed by norms of appropriate behavior. The focus would be on the behavior of would-be copyists and on what activities owners need to guard against. Owners should not be required to anticipate actions that deviate appreciably from social norms, but they should reasonably safeguard their valuable information from behavior that complies with general commercial standards.

The last consideration is, as discussed below, somewhat more controversial. It conceptualizes the law as aimed at saving holders of trade secrets from engaging in activities that represent pure social losses, losses that do not contribute to innovation, yet substantially increase the cost of bringing new technology to market.41


39. Arguably, there may be times when secrecy is best maintained by not highlighting the value of particular information. If so, then there should be a rebuttable presumption that the absence of a confidentiality agreement means that reasonable efforts have not been taken.

40. See, e.g., International News Serv. v. Associated Press, 248 U.S. 215 (1918) (holding that the doctrine of unclean hands does not attach to the taking of published news items as tips to be investigated); Metropolitan Opera Ass'n v. Wagner-Nichols Recorder Corp., 101 N.Y.S.2d 483 (Sup. Ct. 1950) (holding that the allegation of an unauthorized recording of a performance was sufficiently alleged cause of action for unfair competition), aff'd, 107 N.Y.S.2d 795 (App. Div. 1951).

Under this approach, the reasonableness of a measure depends on the cost of instituting it. Things that are relatively inexpensive to do are "reasonable" and therefore required. Examples of such include disclosing information to employees only on a need-to-know basis, or procuring nondisclosure agreements from those who are privy to secret information. Expensive measures, such as building elaborate fortresses, sweeping the workplace for listening devices, and the like, are not "reasonable" and are thus not required.42

B. Unauthorized Appropriation

In many ways, the definition of the "bad act" is the most problematic feature of the EEA. The statute reaches the conduct of anyone who:

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice or deception obtains a trade secret;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in any of the paragraphs (1) through (3).43

Interpreting these provisions will be tricky because they prohibit activity that is not mentioned in the corresponding sections of the Restatement or the UTSA. The Restatement's definition includes "theft, fraud, unauthorized interception of communications, inducement of or knowing participation in a breach of confi-

42. See, e.g., E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970) (holding that aerial photography of plant construction would be an "improper means" of obtaining another's trade secret); James H.A. Pooley et al., Understanding the Economic Espionage Act of 1996, 5 TEX. INTELL. PROP. L.J. 177, 217-18 (1997) (identifying guidelines that have emerged from case law for the protection of trade secrets).
The UTSA covers "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."45

One problem is derived from the interpretation of "reasonable means." The proposition that trade secrecy laws are intended to require holders to undertake only inexpensive measures to maintain secrecy draws support from the kinds of activities that the states have regarded as misappropriation, namely, activities that would be expensive to guard against. In contrast, the EEA covers rather mundane activities. If these are the sorts of things that are now considered bad acts, then it is difficult to imagine what sorts of activities should reasonably be undertaken to prevent them.

A second problem with these provisions is that they appear to encompass activity that states have traditionally considered lawful. For example, is memorizing information a form of unauthorized appropriation? The EEA does not mention memorization, but it includes "communication" and "conveyance," implying that unlawful takings can include takings that are not embodied in any physical product. In contrast, some state courts do not regard memorizing as improper activity because they do not want trade secrecy law to destroy the ability of employees to benefit from the skills they learn on their jobs.46 Other states do not make this distinction, choosing to protect employee mobility in other ways.47

44. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995). That section also includes a broader category of "means either wrongful in themselves or wrongful under the circumstances of the case." Id.

45. UNIF. TRADE SECRETS ACT § 1(2), 14 U.L.A. 433, 438 (1985). Other parts of section 1 cover disclosure to others and uses following disclosure by others.

46. See, e.g., Inflight Newspapers, Inc. v. Magazines In-Flight, LLC, 990 F. Supp. 119, 126 (E.D.N.Y. 1997) (stating that the defendant "should be allowed to use the skills and knowledge he acquired in his overall experience at Inflight"); Reed, Roberts Assoc., Inc. v. Strauman, 353 N.E.2d 590, 594 (N.Y. 1976) (holding that where former employee’s knowledge did not qualify for protection as a trade secret, there was no commercial piracy of the customer list); Ivy Mar Co., Inc. v. C.R. Seasons Ltd., 907 F. Supp. 547, 558 (E.D.N.Y. 1995) (stating that no trade secret protection exists for customer lists that are recalled, unless the information was memorized intentionally); Abraham Zion Corp. v. Libo, 593 F. Supp. 551, 569 (S.D.N.Y. 1984) (stating mere recollection of customer information is not actionable); Darby Drug Co., Inc. v. Zlotnick, 573 F. Supp. 661, 663 (E.D.N.Y. 1983) (stating that “had Zlotnick simply memorized the names of customers, it could hardly be said that he thereby acted tortiously.”).

47. See, e.g., American Republic Ins. Co. v. Union Fidelity Life Ins. Co., 295 F.
Courts addressing the question will be forced to decide whether to follow the law of a state, which raises the choice of law question, or to interpret the provisions of the EEA as a matter of federal law. In the latter case, they will need to be sensitive to the employee mobility issue, which I discuss in more detail in Part II.\footnote{48}

Another interpretive question is more serious. Some commentators have argued that by prohibiting activities like copying, duplicating, sketching, drawing, photographing, downloading, and photocopying, the EEA means to outlaw reverse engineering.\footnote{49} Although that interpretation strikes most observers as rather unlikely, it is not difficult to see how commentators come to that conclusion. The secrecy of information is a relative matter. On one end of the spectrum is information that is obvious upon inspection, the color of an orange is an example. At the other end is information that cannot be learned from just looking at the products that the information produces. For instance, a process for ridding orange groves of weeds cannot be learned by examining the oranges grown in the grove. In the middle is information that can be learned only through careful scrutiny. By prohibiting specific methods of scrutiny, the EEA can be read to imply that anything that requires that kind of examination is a trade secret within the meaning of the Act. That would, for example, include the kind of activity challenged in \textit{Sega Enterprises, Ltd. v. Accolade, Inc.}\footnote{50}—downloading a program, decompiling it, copying it, and then using interface information to create rival products. Yet these are all actions that were considered lawful by the \textit{Sega} court, by the \textit{Restatement}, and by the UTSA.\footnote{51} They are also the activities that

\footnote{48. The difference in state approaches could also raise the question of whether the defendant received constitutionally adequate notice of the crime. See infra note 102 and accompanying text.}

\footnote{49. See Pooley et al., supra note 42, at 195.}

\footnote{50. 977 F.2d 1510 (9th Cir. 1993).}

\footnote{51. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995) (specifically providing that the "analysis of publicly available products or information are not improper means of acquisition"); UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 433, 438 (1985).}
permit the development of a competitive marketplace for computer
games.

Of course, in deciding whether the EEA means to outlaw re-
verse engineering, courts should clearly not consider themselves
bound by state law because the language of the statute is unique.
Furthermore, the EEA is not limited by the same constitutional
constraints under which state law operates. Thus, while the Su-
preme Court decided in Bonito Boats, Inc. v. Thunder Craft Boats,
Inc.\textsuperscript{52} that states cannot prohibit reverse engineering, the case does
not directly impose such a limit on Congress. Congress is, how-
ever, bound by constitutional limitations of its own. Furthermore,
even if the legislators drafting the EEA were not overly concerned
with innovation policy, courts should construe ambiguous lan-
guage in the legislation to make the statute consistent with other
intellectual property initiatives. From that perspective, it is clearly
wrong to interpret the EEA as suggested. Reverse engineering is
one of the most important ways in which trade secrets expire. If
reverse engineering were prohibited, trade secrets would endure
until they were rediscovered—which could be for long enough to
violate the limited-times provision of the Copyright Clause.\textsuperscript{53}
Longer protection for trade secrets would also enhance their value
relative to patents, which expire twenty years after the applications
on which they are based are filed. Since trade secrets are cheaper
to acquire than patents, this interpretation might lead inventors of
patentable inventions to forego patenting in favor of keeping trade
secrets. That would be socially undesirable. Patents disclose in-
formation for use during the patent term and enable the public to
freely use the protected technology after expiration. Trade secrets
do neither. In Bonito Boats and in an earlier case, Kewanee Oil
Co. v. Bicron Corp.,\textsuperscript{54} the Supreme Court warned that states should
not structure their trade secrecy laws in a way that encourages their

\textsuperscript{52} 489 U.S. 141 (1989).
\textsuperscript{53} To be sure, Congress did not enact the EEA under its copyright authority, but it
is unlikely that the Supreme Court would allow it to avoid this constitutional limitation
by utilizing the Commerce Clause. Cf Railway Executors Assn. v Gibbons, 455 U.S.
457 (1982) (holding that non-uniform bankruptcy laws cannot be enacted pursuant to the
commerce power as a way to avoid limitations in the Bankruptcy Clause).
\textsuperscript{54} 416 U.S. 470 (1974).
Although the federal government is, again, not strictly bound by these cases, the Supreme Court's insight surely has broader application: Congress should also be wary of structuring law that encourages innovators to disregard the patent system. To put this another way, criminalizing reverse engineering would upset the basic bargain of intellectual property law. It would take material that was formerly considered public, such as the material that Sega considered public, into the domain of the private. And, as one commentator has noted, it is not even so clear that the drafters of the EEA intended that reverse engineering be considered unlawful.

A closer question on reverse engineering may, however, soon reach the courts in the form of an investigation of whether Reuters Holdings P.L.C. misappropriated information from Bloomberg L.P. One reported version of the facts states that Reuters acquired the information at issue through a consultant who subscribed to Bloomberg's service and then used the materials in violation of a contractual prohibition against reverse engineering. There is, again, some controversy as to whether the EEA was meant to ban the use of expertise to dissect publicly distributed product.

56. See Darren S. Tucker, Comment, The Federal Government's War on Espionage, 18 U. Pa. J. Int'l Econ. L. 1109, 1143 (1997). Tucker relies on the following statement by Senator Kohl: “If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent or [the EEA], then that form of 'reverse engineering' should be fine.” 142 Cong. Rec. S12212-13 (daily ed. Oct. 2 1996) (statement of Sen. Kohl), cited in 18 U. Pa. J. Int'l Econ. L. at 1143. It is not clear how much weight this statement should be given. First, not all courts feel bound by remarks appearing in the Record. More importantly, since the issue here is what violates the EEA, the remark says nothing. See also 142 Cong. Rec. S12212 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl) (stating in effect, that the Act is meant to reach "flagrant and egregious cases of information theft"). The House Report also mentions the problem: "[I]nformation which is generally known to the public, or which the public can readily ascertain through proper means, does not satisfy the definition of a trade secret under this section.” H.R. Rep. No. 104-788, at 31 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4032. Furthermore, the statutory defining of a trade secret also incorporates the notion of "not being readily ascertainable through proper means.” 18 U.S.C.A. § 1839(3)(B) (West 1998). However, since the issue is what is proper, these statements beg the question.
58. See id. at 6 (quoting 142 Cong. Rec. S12212 (daily ed. Oct. 2, 1996) (Man-
is also a question whether such a restriction would survive a pre-emption challenge. *Bonito Boats* would seem to say that enforcement of the restriction would be preempted, but strong arguments have been made by, among others, the drafters of Article 2B that bargained-for obligations are analytically different from the statutory situation analyzed by the Supreme Court in *Bonito Boats*. The drafters argue that "'[a] contract defines rights between parties to the agreement, while a property right creates rights against all the world. They are not equivalent.'" If an effective bar on reverse engineering can be imposed contractually, it is difficult to see why a breach of such an obligation should not be treated like any other breach—as an improper way in which to acquire a trade secret. The activities involved certainly match the description in the EEA.

Another worrisome aspect of the EEA's definition of a "bad act" is that it criminalizes attempts. The interpretation of the provision could have a big impact on innovation. Thus, in the "worst-case scenario", the government would be able to prosecute people who engage in one or more of the prohibited activities even when there is no secret information available for them to take. The statute would, under this interpretation, be unique to intellectual property law because it would create the only situation in which a defendant could not defend on the ground that the right itself is invalid. It would build fences around companies like Sega and

ager's Statement that there is no violation "if a person can look at a product and, by using their own general skills and expertise, dissect the necessary attributes of the product.")

59. See, e.g., *Bonito Boats*, 489 U.S. at 160 ("If [the State] may prohibit this particular method of study and recomposition of an unpatented article, we fail to see the principle that would prohibit the State from banning the use of chromatography in the reconstitution of unpatentable chemical compounds, or the use of robotics in the duplication of machinery in the public domain.").

60. U.C.C. § 2B, *supra* note 10, at Preface at 13 (citing ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996)) (emphasis in original). See also Dreyfuss, *Do You Want to Know a Trade Secret?*, *supra* note 14.


62. See 18 U.S.C.A. §§ 1831(4), 1832(4) (West 1998). Similar comments can be made about conspiracies, which are covered by subsection (5) of each of these provisions.

63. Under the Lanham Act, trademarks registered for more than five consecutive years can become incontestable, but only with respect to certain defenses. See 15 U.S.C.A. § 1065 (West 1998). Private control over trademarks does not have the same impact on innovation as does private control over other technologies.
around their products, even if they are not, in fact, particularly innovative. The flow of information between firms would, as a result, be curtailed and the utilization of information that is public and free to all would decrease.

The question, then, is whether this scenario is likely. The interpretation is supported to some extent by one of the few EEA prosecutions reported to date, *United States v. Hsu.* The defendants there were charged with unauthorized conveyance of the formula and processes for manufacturing Taxol and with attempting to misappropriate this secret information from its developer, Bristol-Myers Squibb Company ("Bristol-Myers"). In the course of preparing for trial, the defendants asked to review Taxol technology documents and the government resisted. The statute specifically provides for protective orders to prevent public disclosure of trade secrets during trial; the prosecution wanted that order structured so that the defendants and their lawyers could not learn any Bristol-Myers technology. The government argued that the legal impossibility of committing the crime is not a defense, and if the defendants could not win by proving that the material sought did not qualify as secret, then details about the technology were irrelevant and immaterial. The Third Circuit agreed. After noting that the EEA is an attempt to provide a "comprehensive mechanism for curtailing the escalating threat to corporate espionage," the court stated, "we find it highly unlikely that Congress would have wanted the courts to thwart that solution by permitting defendants to assert the common law defense of legal impossibility." The court concluded that "[i]t naturally flows that the government need not prove that an actual trade secret was used." In addition, the court noted that the defendants' view would lead to a "bizarre" result: the government would have to disclose secrets to the very

64. 155 F.3d 189 (3d Cir. 1998).
67. *Hsu,* 155 F.3d at 201 (emphasis added).
68. Id. at 202.
69. Id. at 203.
people accused of stealing them. But whatever the merits of this position, the decision on impossibility seems to create a situation where taking even public information could serve as the basis for a prosecution.

This is not, however, the only way to interpret Hsu or the EEA. The Hsu prosecution was based on a sting operation: the defendants were trying to take genuine trade secrets, but the government sought to establish the crime by handing out so-called "dummy" technology. Because the EEA was, in part, inspired by sting operations that the government had conducted under other criminal statutes, it was consistent with the legislative history for the judge to interpret the EEA in a way that preserved the viability of this method of apprehending economic espionage agents. There was, however, no real argument in Hsu that the government was relieved of an obligation to prove that Bristol-Myers possessed secret technology. Thus, the case need not stand for the position that the government can prosecute even in situations where a target has nothing worth taking.

70. See id. at 202.
71. See Hsu, 982 F. Supp. at 1023. There is, apparently, some question whether the documents passed were real or fake. See Hsu, 155 F.3d at 192-93 (noting that the indictment alleged that the documents contained trade secrets). But see id. at 202 (assuming government would not pass genuine information).
73. See Hsu, 982 F. Supp. at 1024. See also supra note 71.
74. For further discussion, see infra note 81 and accompanying text. Hsu is troublesome for two other reasons. First, it is probably the tip of the iceberg on difficult discovery issues that the EEA will create. Second, if the court is right, and the government can give allegedly secret documents to suspected misappropriators, how will the requirement that targets take reasonable measures to maintain secrecy be established? It is also worth noting that courts manage to handle the disclosure problem in civil trade secrecy litigation without depriving defendants of a crucial defense. Information can be redacted, shown only to the lawyers, or the defense reviewed by the court alone.
C. State of Mind

Most intellectual property violations do not turn on knowledge or intent, except as an enhancement of relief. According to the state-of-mind provisions of the EEA, the statute will require courts to consider factors they have not been previously required to address in the intellectual property area.

This is where the origins of the statute as a measure to combat the activities of foreign espionage agents can best be detected. Thus, the statute draws a distinction between acts undertaken on behalf of foreign governments and acts undertaken for private gain. In the former case, the government must show that the defendant, "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly" engaged in the acts described in the previous section. For other cases, the statute punishes:

Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that secret, knowingly [engages in the acts described in the previous section].

The interesting question is whether these several state-of-mind elements will impose limits that make up for the broad interpretation to which the rest of the EEA is susceptible. It seems unlikely.

75. See, e.g., De Acosta v. Brown, 146 F.2d 408 (2d Cir. 1944) (holding that an infringement action lies even if defendant did not know that the work copied was copyrighted). As noted in the text, courts can increase damages on proof that the infringement was willful. See 35 U.S.C. § 284 (1994 & Supp. I 1996); 15 U.S.C.A. § 504 (West 1998).

76. To put this more precisely, the EEA will require courts to make distinctions that the Supreme Court has, in some circumstances, declared impossible. See Warner-Jenkinson Co., Inc. v. Hilton Davis Chemical Co., 520 U.S. 17 (1997) ("At a minimum, one wonders how ever to distinguish between the intentional copyist making minor changes to lower the risk of legal action, and the incremental innovator designing around the claims, yet seeking to capture as much as is permissible of the patented advance.").


On the government-entity side, there are ostensibly only two state-of-mind requirements: that the defendant intend or know that the offense will benefit a foreign entity, and that the defendant know she is engaged in one of the named activities. As discussed above, the named activities are so mundane; showing that the defendant intended to engage in them will pose no real bar to prosecution. The “benefit” provision is also not likely to constrain the EEA very much. This section does not modify the term “benefit” by the word “economic,” as does the private-entity provision. According to the legislative history, Congress intended to include rather amorphous benefits, such as reputational, strategic, and tactical advantages. That means almost anything could qualify as a benefit. It is, however, arguable that the proviso “intending or knowing that the offense will benefit” foreign entities interposes a third element—that the government show that the defendant had intended to commit an offense because the defendant targeted a genuine trade secret for taking. If that interpretation is adopted, then the EEA may have some limits. The language is, however, rather ambiguous on this point.

On the private-entity side, the government needs to establish several elements, but here too, the limits they interpose may be somewhat illusory. The government must demonstrate that the defendant intended to convert a trade secret and intended to benefit someone other than the owner, had intent or knowledge that the information will injure an owner of the trade secret, and knew that she was engaged in a denominated act. As with the government-entity provision, it is unlikely that the prosecution will have trouble proving that the defendant knew she was committing one of the specified acts. The better interpretation of Hsu is that the government must show that the activity at issue was intentionally targeted at a genuine trade secret as defined by the EEA, even in cases

---


80. The question of whether they are sufficient is discussed infra at Part II.

81. Arguably, the government must also show that the defendant knew that the trade secret was in a product in interstate or foreign commerce. Although the legislative history recites this requirement, the description of the state-of-mind elements omits it, making it appear that this language is there for jurisdictional purposes only. See H.R. Rep. No. 104-788, at 10-11 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4029-30.
where the actual information with which the defendant dealt was dummy technology. The statute does not, however, require that reading. A defendant can intend to take a trade secret even if she is mistaken about whether the technology in question is secret.

Even more worrisome is the possibility that the government will try to prosecute a defendant who believed she was learning material that exists in the public domain. That interpretation of the statute comes from a passage in its legislative history, which indicates that even a defendant who was erroneous in her belief about the status of the material taken can, in some instances, be considered to possess the requisite state of mind.82

Admittedly, that passage comes from the Senate Report on a bill that was modified before it became the EEA; as enacted, the EEA talks of the "intent to convert a trade secret."83 The draft bill did not. Moreover, it is probable that the Senate simply failed to consider how difficult it can be for an actor to determine whether a technology is, in fact, a trade secret—to consider, for example, that the adequacy of the target's efforts to maintain secrecy is uniquely within the knowledge of the target. One hopes that courts will not utilize this passage to water down the intent elements of the statute, and that instead the prosecution will be required to show that the defendant's intent actually was to take a material "secret" within the meaning of the statute.

82. The Senate Report states:
A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one's conduct, and (2) an awareness of or a firm belief in or knowledge to a substantial certainty of the existence of a relevant circumstance, such as whether the information is proprietary economic information as defined by the statute. The statute does not require proof that the actor knew that his conduct violated Federal law. The Committee intends that the knowing state of mind requirement may be satisfied by proof that the actor was aware of a high probability of the existence of the circumstance, although a defense should succeed if it is proven that the actor actually and reasonably believed that the circumstance did not exist. . . . This approach deals with the situation that has been called willful blindness, the case of the actor who is aware of the probable existence of a material fact - for example, that he has no authority, or that the information is proprietary - but does not satisfy himself that it does not in fact exist.


Next, there is the question of interpreting the requirement that the prosecution demonstrate an intention to benefit someone other than the owner and an intent or knowledge of injury. Here, the statute does appear to limit benefits and injury to economic repercussions. But even so, there is substantial room to maneuver. The common conception of a trade secret is a positive technology, for example, the process for manufacturing Taxol, which, when utilized, will create a profitable product for the acquirer’s beneficiary and undermine the market position of the technology’s developer. In some instances, however, much less of a transfer has been considered to raise competitive concerns. Thus, courts have recognized that there are economic benefits in learning no more than that a research path is fruitless. Since the cost of research is built into the price of goods sold, courts that see “negative know-how” as conferring a benefit should also see its acquisition as inflicting an injury. Similarly, a firm can benefit just by hiring an employee who knows its competitor’s strategies. The firm may not choose to duplicate the strategy, but it is somewhat inevitable that the employee will help direct the firm’s activities in a way that undermines the competitor’s planned tactics. Again, courts that recognize “inevitable disclosure” as a benefit should also see it as creating injury. Both interpretations, if adopted for the EEA, will substantially increase its scope.

The other potential issue on the private side is the question of why the statute defines “owners” to include not only trade secrecy holders but also licensors. Some commentators have suggested that Congress included the term “licensor” so that the government could use the statute to prosecute breaches of licensing agreements. If that is the way courts read the EEA, prosecutions could

---

85. See, e.g., Pepsico, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995) (holding that former employer was entitled to a preliminary injunctive relief under the Illinois Trade Secret Act because disclosure to competitor was inevitable if former employee accepted employment with competitor).
86. See Joseph F. Savage, Jr., The New Economic Espionage Act can be Risky Business, 12 CRIM. JUST. 12, 15 (Fall 1997).
88. See Mossinghoff et al., supra note 13, at 198.
produce some surprising results. Consider, for example, a contractor who produces sweaters on knitting machines programmed to make a novel pattern. The license requires the production of five thousand garments, but the licensee produces ten percent extra in anticipation that some of the garments will be rejected. What happens if some of these extras work their way on to the market: should selling the overrun to recover the cost of production be considered a crime? Significantly, prior law has taken a rather benign view of this activity. Although the licensee would be breaching the contract, contract law does not usually impose punitive remedies. Even the Trademark Counterfeiting Act of 1984 excludes overruns from criminal coverage. Nonetheless, the argument that the EEA does penalize this conduct cannot be ignored. The United States has been extremely active in protecting trademark holders from this sort of infringement, particularly in foreign countries. Given the statute’s unique extraterritorial reach, courts may have a hard time resisting this interpretation.

The final question concerns how the EEA will be applied to employers. Both the government and private-entity provisions impose high penalties on organizations committing the described offenses. The statute does not specify the circumstances in which this can occur. One can surmise, however, that, as in other situations where corporations face criminal prosecution, a firm will be criminally liable for the acts of its agents that are conducted within the scope of their authority and for the benefit of the firm. Avoiding this liability may not be easy. Employees in high-tech firms are under a great deal of pressure to produce. There have been instances where an employee has taken information learned

91. See, e.g., New York Cent. & Hudson River R.R. Co. v. U.S., 212 U.S. 481 (1909) (holding that an agent acting under the authority delegated to him may be controlled by imputing the actions to the employer and subsequently imposing penalties upon the corporation).
on one job and used it in another employer’s project. Although
this may have been done without specific direction from that em-
ployer, it was nonetheless for the new employer’s benefit and to
the detriment of the earlier employer.92 If this sort of activity is
now regarded as criminal, employers may need to institute cross-
examination procedures whenever a new employee makes what
appears to be a breakthrough, just to make sure that the work is in
no way dependent on information learned on a previous job—and
even to ensure that the employee did not rely on prior experience
to avoid blind alleys. In fact, commentators are recommending in-
termediate compliance plans, including elaborate exit and entry inter-
views and rigid insulation of new employees from those working
in areas where the new employee was previously engaged.93 These
activities may be costly. They may lead a firm to reject an appli-
cant with expertise that would improve that firm’s research efforts.
information walls will certainly disrupt the flow of information
within firms. It is hard to see how any of this will improve the
creative environment or enhance innovation.

D. Extraterritoriality

Unlike intellectual property laws, which are territorially lim-
ited, the EEA applies to conduct occurring outside the United
States whenever:

(1) the offender is a natural person who is a citizen or per-
manent resident alien of the United States, or an organiza-
tion organized under the laws of the United States or a
State or political subdivision thereof; or
(2) an act in furtherance of the offense was committed in

93. See, e.g., Savage, supra note 86, at 17 (suggesting strategies for dealing with
clients seeking protection from the EEA); Pooley et al., supra note 42, at 224 (same);
Mossinghoff et al., supra note 13, at 205 (same). Compliance schemes also are advanta-
geous because their existence can reduce penalties under the federal sentencing guide-
lines. See Thomas M. Kerr, “Trade Secrets.” I.E., Confidential Business Information or
Business Intelligence, 145 PITTSGURGH LEGAL J. 27 (Dec. 1997); Ronald Abramson,
Economic Espionage Act of 1996; Theft of Trade Secrets Addressed, N.Y.L.J., Apr. 28,
1997, at S1 (“These and other possibilities for institutional violations suggest the possible
need to include compliance efforts in this area in an ‘effective program to prevent and
the United States.\textsuperscript{94}

The general debate on how far one nation can regulate conduct in another jurisdiction is well beyond the scope of this Essay.\textsuperscript{95} But it is worth noting that attempts to criminalize commercial activity occurring elsewhere have, from time to time, led to significant political repercussions for the United States and to the institution of countermeasures by foreign governments.\textsuperscript{96} In the context of intellectual property rights, extraterritorial applications are particularly problematic. First, intellectual works have cultural implications. Not every country takes the same view on whether it is moral to create proprietary rights in intellectual efforts. Moreover, some nations reject the idea of applying the theory of competitive advantage to cultural matters when the result could be the domination of their cultures by countries with more developed innovation industries.\textsuperscript{97} In addition, the export of U.S.-style intellectual property law could intellectually handicap less developed countries, re-

\begin{footnotes}
\footnote{94. 18 U.S.C.A. § 1837 (West 1998).}
\end{footnotes}
quiring these nations to pay supracompetitive prices in order to come up to world intellectual standards. This is something that currently developed countries were not always forced to do.\textsuperscript{98}

Furthermore, foreign enforcement of the EEA may lead to accusations that the United States is trying to end-run the 1994 Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPs Agreement").\textsuperscript{99} The TRIPs Agreement requires every member of the General Agreement on Tariffs and Trade ("GATT") to protect undisclosed information.\textsuperscript{100} However, it also includes special transition arrangements that give developing nations time in which to conform their law and legal practice.\textsuperscript{101} These provisions were very carefully negotiated; if the United States can, for example, prosecute the knitting contractor discussed in the previous section under the EEA when it could not bring an action against the country in which the contractor is operating under TRIPs, then these negotiations will have provided developing countries with very little of the temporal benefits they thought they had bargained for.

The extraterritorial application of the EEA will also give rise to some difficult procedural questions. As noted above, there is a degree of fluidity in the way that the elements of an EEA case are defined. If courts decide to defer to local law on some of these matters, then difficult choice of law questions will arise, especially in countries that have not yet conformed their law to the TRIPs Agreement and in nations that are not participants in GATT. Even if deference is put to one side, there will be hard conflicts of laws issues. Could, for example, someone be prosecuted under the EEA for activity that is not considered unlawful in the country in which it is committed? What about activity that is expressly privileged under the intellectual property laws of the nation in which it oc-

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{98} See, e.g., Rochelle Cooper Dreyfuss & Andreas F. Lowenfeld, Two Achievements of the Uruguay Round: Putting TRIPs and Dispute Settlement Together, 37 Va. J. INT'L L. 275 (1997) (using a series of hypothetical cases to examine the "Understanding on Dispute Settlement").
\item \textsuperscript{100} See TRIPs Agreement art. 39, 33 I.L.M. at 1212-13.
\item \textsuperscript{101} See id. arts. 65-66, 33 I.L.M. at 1222.
\end{itemize}
\end{footnotesize}
curred? If nothing else, it seems hard to believe that a defendant who committed an act (such as reverse engineering) in a country where that act (copying) is privileged would have constitutionally adequate notice that she was committing a crime.\(^\text{102}\)

Finally, there will be issues of proof. Trade secrets are almost by definition used in secret. Without a right to discovery abroad, the government may have difficulty proving its case. More significantly, defendants may have trouble mounting their defenses. For instance, it may be difficult to acquire the evidence necessary to show that the alleged target's information was not a trade secret or that the target had failed to take reasonable measures to keep its technology secret.\(^\text{103}\)

E. Punishment

The EEA imposes four types of punishment. First, individuals can be fined up to $500,000, imprisoned for up to fifteen years, or both for activities that benefit a foreign government; there is also a maximum fine and ten years imprisonment for activities benefiting private entities.\(^\text{104}\) Second, organizations can be fined up to $10,000,000 and $5,000,000, respectively, for these crimes.\(^\text{105}\) Third, a court can order forfeiture property if it meets certain requirements.\(^\text{106}\) Finally, the government can institute federal civil

---

102. See, e.g., Colautti v. Franklin, 439 U.S. 379, 390 (1979) (declaring that a criminal statute that fails to give a person of ordinary intelligence fair notice that the contemplated conduct is forbidden is void for vagueness); Savage, supra note 86, at 14 (commenting that the EEA explicitly prohibits the improper "use" of information).

103. But cf. In re Bayer AG, 146 F.3d 188 (3d Cir. 1998) (upholding discovery of foreign documents under 28 U.S.C. § 1782(a) for use in foreign litigation whenever the substance of discovery is not objectionable under comity principles). Bayer's emphasis on "providing equitable and efficacious discovery" in international contexts may be token increased cooperation among jurisdictions in discovery matters. Id. at 195.

104. See 18 U.S.C.A. §§ 1831(a), 1832(a) (West 1998).

105. 18 U.S.C.A. §§ 1831(b), 1832(b) (West 1998).

106. See 18 U.S.C.A. § 1834 (West 1998). The statute provides that a court can order forfeiture of:

1. any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of [a] violation; and
2. any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of [a] violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.
actions for injunctions against violations of the EEA. The problems with giving courts the amount of discretion the EEA contemplates are obvious, notwithstanding the federal sentencing guidelines. Equally problematic are the numerous issues that arise in connection with forfeiture statutes. These issues are especially complicated in light of the EEA's extraterritorial application. It is hard to see what an American court can do to enjoin acts occurring abroad or to seize assets that are located abroad without risking serious international consequences.

Forfeiture of property derived from the receipt of a trade secrets is especially troubling. The scope of infringement is not as clear in trade secrecy law as it is in patent cases (and even there, it remains controversial.) More important, a trade secret can constitute a very small part of a much larger invention. Confiscating the invention or the profits derived from that invention could be grossly disproportionate to the technological contribution of the trade secret, yet the proportionality language of the statute applies only to forfeiture of property used to commit the offense, not to forfeiture of the benefits of the violation. In a case where a firm

has a technology whose provenance is questionable, this provision will make it risky to incorporate it into a larger product. Despite the social disutility of reinventing something that already exists, the firm might choose that course to avoid the possible forfeiture of the benefits deriving from the larger work.

II. THE EEA AND FEDERAL INNOVATION POLICY

While the courts busy themselves sorting out the difficulties involved in applying the EEA, it behooves the scholarly community to consider the effects of this legislation on national policy. Hopefully, our deliberations will influence how courts construe the statute.

The most worrisome possibility is that the law will be interpreted in a manner that makes it actionable to learn and utilize public information. That could happen if the definition of "secret" is made too broad, if certain activities that constitute reverse engineering are classified as unauthorized appropriation, if attempts include situations where the defendant is mistaken in his belief that the target possesses trade secrets, or if employers become reluctant to hire knowledgeable employees. If these interpretations are adopted, the statute will have a substantial impact on prices, quality, and consumer choice. It was, after all, the ability to discover and utilize the interfaces between Sega cassettes and consoles that allowed competitors to enter the computer game market, drive down the price of games, and give consumers a new set of materials to play on their Sega consoles. Insulating firms from competition in non-secret information could also have a detrimental effect on these firms' propensity to invest in innovation. That is, although intellectual property is a method of encouraging creativity, no one has suggested that Joseph Schumpeter's notion of competition—the "engine of creative destruction"—is not an equally powerful mechanism.\(^{112}\)

\(^{112}\) Cf. Frank H. Easterbrook, Treble What?, 55 ANTITRUST L.J. 95 (1986) (warning that antitrust laws are also sometimes misinterpreted in a manner that reduces competition). See also Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 151 (1989) ("The attractiveness of [the patent law] bargain, and its effectiveness in inducing creative effort and disclosure of the results of that effort, depend almost entirely on a backdrop of free competition in the exploitation of unpatented designs and innov-
Even if the EEA is interpreted more narrowly, it could exert significant effects on innovation. To the extent that Congress thought about the creative environment, it apparently assumed that if strong proprietary rights are good, then stronger rights must be better: if trade secrecy protection is currently weak, then adding a new level of deterrence will be an improvement. The problem here is that the logic is wrong—more is not always better.

One factor was alluded to above. Innovators choose where to allocate their efforts and what intellectual property regimes to rely upon when their efforts pan out. Because trade secrets have always been vulnerable to leaks, to independent discovery, and to reverse engineering, patents have had the greater allure despite their cost and relatively short term. With the EEA, the calculus shifts. Because it deters attempts to figure out what competitors are doing, the EEA allows developers to hide their trade secrets more effectively than before. With less vulnerability to leaks and reverse engineering chilled, the trade secrets of the future will only be acquired through independent invention—making them distinctly better than patents.

And yet, the public interest has always been thought to favor patents and patented technology. For example, *Bonito Boats* emphasized that federal policy is to encourage the kind of inventiveness that yields patents. Thus, in invalidating a Florida statute that prohibited a cheap method of copying unpatentable boat hull technology, the Supreme Court stated that, "given the substantial protection offered by the Florida scheme, we cannot dismiss as hypothetical the possibility that it will become a significant competitor"

---

114. Or, as Ludwig Mies van der Rohe once said, less is more. See Mies van der Rohe, *Back to Basics*, The Economist, Apr. 19, 1997, at 84.
115. See supra note 55 and accompanying text; Dreyfuss, *Do You Want to Know a Trade Secret?*, supra note 14 and accompanying text.
116. Even independent invention might not be enough to avoid prosecution because it can sometimes be difficult to demonstrate. Of course, the government bears the burden of proof, but the chill produced by the difficulties inherent in the case should not be ignored. Cf. Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 720 (2d Cir. 1992). In *Computer Assocs.*, an attempt to redevelop a computer program through use of a clean room procedure was entirely ignored by the court.
THE ECONOMIC ESPIONAGE ACT OF 1996

1998]

The Federal Trade Commission, acting pursuant to the Federal Trade Commission Act, 15 U.S.C. § 41 et seq. (1988), to ensure that the EEA does not pose a substantial threat to federal patent laws, offering investors similar protection without the quid pro quo of substantial creative effort required by the federal statute. 117 The Court continued, offering that, "the prospect of all fifty States establishing similar protections for preferred industries without the rigorous requirements of patentability prescribed by Congress could pose a substantial threat to the patent system's ability to accomplish its mission of promoting progress in the useful arts."

Further, the Supreme Court in Kewanee warned that federal policy would be undermined if people who did invent patentable subject matter chose to hide their discoveries as trade secrets. In the course of holding that state trade secrecy law is not preempted by federal law, the Court stated: "If a State, through a system of protection, were to cause a substantial risk that holders of patentable inventions would not seek patents, but rather would rely on the state protection, we would be compelled to hold that such a system could not constitutionally continue to exist." 118

Again, Congress is not directly bound by Bonito Boats or by Kewanee. 120 However, the rationales of these cases should be taken seriously. If the EEA increases the risk that holders will not seek patents, it may make state trade secrecy laws vulnerable to preemption. More importantly, the public interest will be damaged. Patents permit the public to monitor the use of new technologies, to learn from the insights of others, and to avoid wasting resources re-inventing something that others have invented before. 121 Trade secrets do none of that.

The last observation points to what is really the fundamental issue here: the weaknesses that Congress saw in trade secrecy are not flaws in the trade secrecy system; they are there for a purpose. Indeed, neither copyright law nor patent law creates a regime that is especially strong; both are porous and "leak" material into a do-

118. Id. This is not to say that I agree with the Court's reasoning: I like gadgets.
120. See supra notes 52-53 and accompanying text.
main where the public can access it for free. That structure is not an accident. In fact, the economics of innovation requires it.

One reason to design a leaky regime is that giving innovators more complete control would create what can be called an "offsets quandary." Since progress depends on innovators building upon the work of those who came before, innovator A's output is innovator B's input. If A enjoys plenary rights over his innovation, then he will be able to extract large rewards. But the encouragement that this reward gives to A will be offset by the higher cost, and obstruction, it produces for B. To avoid the offset problem, patents and copyrights are purposefully weak. Patents are of relatively short duration (twenty years) and patentees are encouraged to surrender their rights through the maintenance-fee system.\footnote{122} In addition, there is a well-developed misuse defense that can prevent patentees from using their rights to block further developments.\footnote{123} Copyrights last much longer, but the statute recognizes a fair use defense and creates several compulsory licenses, all of which have the effect of allowing the Bs of the world to make productive and socially important uses of protected works during the time they are federally protected.\footnote{124}

Two other reasons for according innovators less than plenary rights are the spillover and deadweight social loss problems. These are interrelated in the following way. The social benefits of innovation often derive from applications far outside the initial innovator's own field.\footnote{125} Since A may not appreciate all of the ways

\begin{footnotes}
\item[125] See Zvi Griliches, \textit{R&D and Productivity: Econometric Results and Measurement Issues}, in \textit{Handbook of the Economics of Innovation and Technological}
\end{footnotes}
in which his innovation can be utilized, it is important that people like B, with an expertise that is different from A's, have access to A's insights. Of course, B could pay for this access. Unfortunately, B may have a difficult time evaluating it to ascertain whether it is worth what A is charging. Even if B can make the evaluation, it is possible that the supracompetitive rate that A can set will be more than the access is worth to B—and this could be true even when B, and those who would benefit from B's utilization, would be willing to pay a competitive price to use A's work.

To encourage spillover uses and reduce deadweight loss, copyright law relies once again on fair use and patent law recognizes a limited experimental use defense.\textsuperscript{126} Additionally, both regimes make sure that the ideas underlying protected works are available for study and use even during the time that applications of the ideas are protected. The Copyright Act requires Americans to deposit copies of their work in the Library of Congress.\textsuperscript{127} The cost of private copies is reduced through the first sale doctrine, and the idea/expression dichotomy ensures that the ideas are immediately made a part of the public domain.\textsuperscript{128} Similarly, patent law has a specification requirement to disclose underlying principles. The first sale doctrine reduces the cost of copies, and the principles revealed are considered public, not private.\textsuperscript{129}

\begin{footnotes}


\textsuperscript{129} See 35 U.S.C. § 112 (1994 & Supp. 1996) (specification); Adams v. Burke, 84 U.S. 453 (1873) (holding that there can be no restriction on the use of machines or implements which are limited to one use when once they are lawfully made and sold); Gottschalk v. Benson, 409 U.S. 63 (1972) (principles/embodiment dichotomy). Both regimes also make sure that only works of true intellectual value enjoy any degree of ex-
Because it is largely a creature of the common law, trade secrecy law is less systematic than the federal statutory regimes. However, what Congress saw as weakness is, in part, simply its analogously porous texture. Traditional trade secrecy law protects against misappropriation, but misappropriation is carefully defined to exclude reverse engineering or learning the invention through familiarity with its embodiment. Like copyright law, trade secrecy law does not protect creators against independent inventors. Moreover, it does not create rights against good faith purchasers. As the right to use a trade secret is transferred to licensees, sublicensees, and end-users, as embodiments of the secret change hands, and as employees leave one job and go to another, there are many opportunities for leakage. The traditional structure provides innovators with a period of time in which to earn a return on their investment, but the period of return is relatively short. Leakage built into the system gives others the opportunity to find new uses for the secret, to learn the principles that underlie it, and to deploy those principles in new ways.

Eventually, it is true, the information becomes generally known and it loses its status as a trade secret. But this is not an event that should only be counted only as a business loss, as some in Congress have viewed it. It also represents a business gain because the information becomes freely available for further development. To put this another way, in enacting the EEA, Congress deplored the fact that "civil penalties often are absorbed by the offender as a cost of doing business and the stolen information retained for exclusivity. It is relatively easy to lose patentable subject matter to the public domain and although both regimes create presumptions of validity, in neither does a right ever become incontestable. See 35 U.S.C. §§ 102(b),(c), (d) (1994 & Supp. 1996) (statutory bars on patentability); 17 U.S.C.A. § 410(c) (West Supp. 1999) (presumption of copyright validity for works registered within five years of publication); 35 U.S.C. § 282 (1994 & Supp. I 1996) (presumption of patent validity). For comparison, see 15 U.S.C.A. § 1065 (West 1998) (providing for trademark incontestability).


131. See, e.g., H.R. REP. No. 104-788, at 6 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4024 (estimating the potential losses at $63 million annually, but not mentioning any gains that could come from using the "lost" information as the basis for new inventions).
tinued use." But in some circumstances, that may be exactly what businesses are supposed to do. If a technology that the holder refuses to license is valuable enough and necessary enough to competition, competitors should be allowed to pay for it, either through royalties or civil penalties, and then enjoy the right to use it freely.

This is not to say that every taking of a trade secret is appropriate. Some valuable information products are not patentable or copyrightable. Trade secrecy law is an important adjunct to the federal system precisely because it provides a way to encourage their development. As the technologies of appropriation become more effective, it is not unreasonable to "beef up" trade secrecy law to meet new threats. Courts that apply the new law must, however, be aware that there are important public interests that lie on the side of keeping the "beef" within bounds. The rhetoric accompanying the EEA obscured the interest in these limits. Courts must not only make sure that the EEA does not wind up protecting public information, but they must also be sensitive to interpretations that will chill activity that should be lawful.

The clearest problem is the effect that the statute could have on employment. The EEA was quite definitely targeted at employees. The legislative history is replete with references to such matters as theft by "disgruntled individuals or employees who hope to harm their former company," to "theft by insiders," to "the former

---

133. Cf. Fogerty v. Fantasy, Inc., 510 U.S. 517 (1994). The Supreme Court stated that:

[T]he policies served by the Copyright Act are more complex, more measured, than simply maximizing the number of meritorious suits for copyright infringement. The Constitution grants to Congress the power "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." . . . We have often recognized the monopoly privileges that Congress has authorized, while 'intended to motivate the creative activity of authors and inventors by the provision of a special reward,' are limited in nature and must ultimately serve the public good.

Id. at 526 (quoting Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984)) (internal citation omitted).

employee of two major computer companies," and to "employees who leave their employment and use their knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer." The structure of the statute is consistent with this purpose. It covers all the common methods of transferring information from one employer to another, including memorization and possibly even inevitable disclosure. The statute clearly includes positive technologies and also admits of an interpretation that encompasses negative know-how. It applies not only to individuals, but also to organizations. The penalties can be very high.

The result is that, unless the statute quickly receives a narrowing interpretation, the high-tech labor market will be rigidified. Although the legislative history makes clear that the EEA is not intended to cover use of "lawfully developed knowledge, skill, or abilities," neither the legislative history nor the Act provides a way to decide what is proprietary knowledge and what is merely a skill. Employees will, therefore, be vulnerable whenever they accept positions that utilize expertise developed with a prior employer. By the same token, a company that needs a particular set of capabilities will be at risk if it hires anyone other than an entry-level candidate. Or, if a firm does hire someone proficient in particular technologies, it will be forced to employ that person outside her area of expertise or build a wall between that person and others at the firm who could utilize what she knows.

None of this can be good for innovation. As intellectual products become more complex, it has become increasingly difficult for firms to cultivate in-house all of the expertise necessary to develop

---

136. Id.
138. S. REP. No. 104-359, at 12 (1996); H.R. REP. No. 104-788, at 18-19 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4026 ("The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed.").
139. See Mossinghoff et al., supra note 13, at 201, 205-6; Pooley et al., supra note 42, at 222.
new technologies. Accordingly, outside consultants and new hires are necessary if innovation is to take place efficiently and expeditiously. Conversely, if technologies are to cross-over from the field where they were developed to all of the places where they can be used, new employees will need to be exposed to the knowledge base of their new firms. Failing to hire, or building walls around new hires, slows the flow of ideas and ultimately hinders development. Ironically, this is actually a problem that Congress once recognized and acted swiftly to counteract. Thus, after a series of decisions where federal courts invalidated patents on the basis of prior research within the firm in which the invention was made, Congress amended the Patent Act to change "a complex body of case law which discourages communications among members of research teams working in corporations." It is a pity that Congress seems to have forgotten the importance of information flows in connection with the EEA.

The cost to employees will, of course, also be high. If employers are unwilling to risk prosecution under the EEA, employees may find themselves suboptimally employed. This will effect compensation. First, money is only one form of compensation in this sector: learning new skills and developing new areas of expertise is another. If these skills become nontransferable, the employment bargain will be undermined. Second, in white collar circles, salary increases are often procured by changing jobs or making credible threats to change. By making these threats less credible, the EEA may hold down wages. And although American business might initially appreciate lower salaries, depressing compensation in the technological sector will be harmful in the long run. It could lead to fewer people entering these fields, which


142. There is also a tinge of possible racism in the discussion of espionage for the benefit of government entities that could translate into job discrimination against ethnics of countries that are suspected of economic espionage. Cf. Tucker, supra note 56, at 1123 (mentioning Japanese and Israelis as possible perpetrators).
would lead to a reduction in the talent available to draw upon.

The EEA could also have a chilling effect on corporate restructuring. Every high-tech employee who starts his own firm, or gets spun off into a new division, will risk prosecution. Yet, as one commentator noted, a place like Silicon Valley “has depended [on this form of employee mobility] for much of its vitality.” Furthermore, partly because the Act incorporates licensors as potential victims, the EEA could also affect mergers and acquisitions, for these create situations where employees hired by one entity work for another, or technology licensed to one entity is exploited by another. The corporate literature has made the benefits of corporate flexibility abundantly clear. All that needs to be added here is to highlight the special benefits that restructuring can bring to the technology sector, where it is sometimes important to segregate risks of nondevelopment or tort liability, and where a lean-and-mean management style can be an important ingredient in product development.

Finally, there is the matter of joint ventures. In the technology sectors, these are important for at least two reasons. First, technologies are often developed in steps—a pioneer invention is made by A, an improvement is made by B, and others may come along later to make further improvements and apply the insight to new fields. Allocating the profits on the products that end-users ultimately enjoy may not be an easy matter: if A receives all of the benefit, there is little incentive to follow on; if B receives all of the benefit, then there will be insufficient encouragement to pioneers. These allocation problems can be partly solved though joint ventures and other methods of pooling rights.

Second, joint ventures are also helpful to the development of complex technologies that require the efforts of researchers with many different areas of expertise. Although sometimes diverse ca-


The plan in both versions of joint venturing is to share in the profits flowing from the intellectual property rights. It may not be easy, however, to predict ex ante what technologies will be invented, or how they will be protected. In some cases, the understanding of participants is rather unclear and it is not unlikely that some method of dispute resolution will be necessary to iron things out at the end. But while the parties may feel that the benefits of developing the technology are worth the risk of civil litigation, they may not feel the same way about criminal prosecution. Thus, we may see fewer of these collaborations as the Act becomes better known. If learning new things puts people at risk of becoming unemployable in the sector for which they have trained, the taste for joining research conglomerations could diminish as well.

There is an interesting footnote to this statute. Apparently, not everyone in the government is certain that American business will be best served by improving the capacity to hide existing technology. In a letter to Senator Orrin Hatch, Chair of the Senate Judiciary Committee, Attorney General Janet Reno indicated that for the first five years after enactment, EEA prosecution will require her personal approval or that of her deputy attorney general, or assistant attorney general for the criminal division. A great deal of selectivity in EEA prosecutions is, of course, one way to make sure that the statute does not overreach. However, it is a limited precaution. Most of the situations that would be criminal under the EEA could have been prosecuted under more general federal statutes. Thus, passage of the EEA cannot but serve as a powerful directive to prosecutors to allocate more of their resources to this area. The courts hearing these cases will, therefore, have to be aggressive in interpreting ambiguous language to make sure that a

145. See Powell, supra note 140, at 197; Rebecca Eisenberg, Intellectual Property at the Public-Private Divide: The Case of Large Scale CDNA Sequencing, 3 U. CHI. L. SCH. ROUNDTABLE 557 (1996).
146. See Savage, supra note 86, at 16.
147. See supra note 20 and accompanying text.
statute designed to protect "the health and competitiveness of critical industries" does not get translated into a provision that undermines their vitality.\(^{148}\)

And while we can hope that the Attorney General and her deputies will make considered judgments on when to use the EEA, the fact of the matter is that the EEA is not the only legislative development with similar problems. For example, a recent amendment to the Copyright Act criminalizes the downloading of commercially valuable information.\(^{149}\) Another new Act criminalizes tampering with encryption devices.\(^{150}\) Given the amount of material now stored in computers, the confluence of these three measures could put much of what is vital to innovation beyond the reach of most innovators.

**CONCLUSION**

The baseline, the Supreme Court has said, is competition. Departures from free competition are "carefully crafted bargain[s]."\(^{151}\) The public foregoes the benefits that flow from competition in order to induce creative endeavors and to assure their adequate disclosure to the public domain. In recent years, our legislators have lost sight of that bargain. After watching steep declines in the manufacturing sector, lawmakers are apparently so relieved that the United States still has something that the rest of the world wants, they have rushed to make sure that those who want what we have are, indeed, forced to purchase it. What they have neglected to notice is that the "something" is not the specific technologies that we have on hand today, but novelty. Novelty does not last long. To be positioned to replace what is novel now with what will be novel in the future, we need to protect the dynamic process that produces innovation. That process requires a robust public domain

---


\(^{150}\) See Digital Millenium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.). The Act creates civil and criminal prohibitions against the use, manufacture, or sale of devices that are primarily designed or produced for the purpose of circumventing copyright protection systems.

from which innovators can draw, an atmosphere where collaboration can occur, and a climate in which ideas can diffuse rapidly.

The high levels of deterrence imposed by criminal law are largely incompatible with these conditions. The EEA’s mongrel nature, which makes it difficult to find sources of interpretation and limitation, exacerbates the problem. It can be interpreted to nudge the line between what is private and what is public toward the private side. It fences in certain information that belongs in the public domain and chills sharing. It will almost certainly slow information flows in the employment context.

On the state and civil front, there is also the interaction of the EEA and proposed Article 2B to worry about. Again, there can be no quarrel about the need to create a mechanism that allows the producers of sub-copyrightable and sub-patentable material to earn a return on their investment. But the combination of these initiatives could alter the basic bargain in unintended ways. First, Article 2B opens the class of material that is protectable. Among other things, it changes the definition of what is public; it may be interpreted to make protectable any information that is subject to a duty of confidentiality, irrespective of whether the information is public or private. Will the EEA be read to criminalize the acquisition of information that is valuable because it is considered secret under Article 2B? How about the use of public information on which a promise of confidentiality has been extracted? Second, Article 2B permits licensors to ask licensees to refrain from particular uses, including uses that might be considered fair under copyright law. Will such restrictions turn the information at issue into trade secrets within the meaning of the EEA? Will ignoring such a restriction be a crime? There is a version of Article 2B that envisions enforcing these restrictions with monitoring devices: will circumventing the monitor violate the EEA? Will it violate the new anti-tampering legislation? Third, Article 2B is very efficient at passing restrictions down the line from developers, to licensees, to end-users. Will the owner/licensor language in the EEA make subsequent purchasers vulnerable to criminal prosecution? How will the “attempts” language of the EEA affect these questions?

The EEA could be interpreted narrowly and become a useful adjunct to other intellectual property legislation. But it has a po-
tentially broad scope. Unless carefully construed, it will allow people to hide secrets in ways that will make it impossible for others to hear, or learn, or know. It could, in the end, breach the careful bargain that intellectual property law has crafted—to the ultimate detriment of the economic sectors that Congress sought to foster.