Secondary Liability for Trade Secret Misappropriation: A Comment

Robert G. Bone

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation

SECONDARY LIABILITY FOR TRADE SECRET MISAPPROPRIATION: A COMMENT

Robert G. Bone†

I. INTRODUCTION

Professor Rustad's article focuses on a problem that has received serious attention in recent years: the involvement of foreign countries in misappropriating trade secrets from American firms.¹ In 1996, Congress adopted the Economic Espionage Act ("EEA") to help address this problem. Professor Rustad reviews the Act's enforcement record and finds it wanting; relatively few cases have been brought and many of these cases have resulted in only mild sanctions.² He identifies several reasons for this poor record, most of which are traceable in one way or another to the statute's exclusive reliance on public enforcement.³ He recommends two reforms: (1) add a private cause of action to the EEA, and (2) extend civil liability to third party software manufacturers and vendors whose negligently

† Professor of Law, Boston University School of Law. I would like to thank the participants in the Santa Clara Conference on Third Party Liability in Intellectual Property Law for many helpful questions and comments. I am especially grateful to Joe Bauer and my colleague Michael Meurer for their suggestions.


³. The EEA uses criminal sanctions as its primary enforcement mechanism, id. §§ 1831, 1832, but it also authorizes the Attorney General to obtain injunctive relief, id. § 1836. According to Professor Rustad's account, there appear to be three chief obstacles to enforcement that stem from the choice of a public rather than private mechanism and the reliance on criminal sanctions. First, affected firms are reluctant to report trade secret thefts, in large part because they worry that the federal government will be less careful about protecting the firm's interests in the resulting litigation than the firms themselves would be. For example, an affected firm with control over the litigation can conduct the lawsuit to limit reputation harms from adverse publicity and better manage the risks of trade secret disclosure. Second, the federal government has limited resources to investigate and prosecute EEA cases, especially since 9/11, when fighting terrorism became a top priority. These resource limitations are especially problematic for criminal prosecutions because of the government's heavy burden of proof and the well-known difficulties in trade secret cases of uncovering evidence and identifying perpetrators. Third, the federal government strongly prefers to bring cases of domestic rather than foreign espionage because of procedural problems and concerns about foreign policy repercussions.
designed software enables trade secret misappropriation.

This Comment focuses critically on these reforms, and especially on the second proposal. Part II briefly examines the basic premise underlying Professor Rustad’s arguments, that foreign theft is a sufficiently serious problem today to warrant bolstering legal protection for trade secrets. I am skeptical of this proposition and Part II explains why. Part III focuses on the specifics of Professor Rustad’s secondary liability proposal. Here too my message is one of restraint. Even if stronger legal protection is a good idea, it is not at all clear that imposing liability on software manufacturers and vendors for negligent enablement is a desirable way to do it given the potentially high social costs and the likely superiority of a contract alternative.

I should state a caveat at the outset. This Comment is not intended to be a complete and rigorous analysis of the many complicated issues involved. Its goal is to raise questions and express doubts that can be the basis of further research and analysis.

II. THE TRADE SECRET THEFT PROBLEM — HOW SERIOUS IS IT?

Professor Rustad makes a number of strong claims about the magnitude and seriousness of the foreign trade secret theft problem, referring at one point to an “astonishing rise in economic espionage and its colossal cost to business” and at another to “overwhelming evidence of widespread state sponsored economic espionage.”4 It is not at all clear, however, that there is enough reliable empirical evidence to support these claims, or that Professor Rustad has a sufficiently articulated normative framework for assessing the seriousness of the problem. Analytical and empirical rigor is particularly important when, as here, conclusions about the severity of the problem are used to support decisions about costly legal enforcement.

I do not question the fact that foreign governments are involved in appropriating trade secrets from American firms.5 However, the

4. Rustad, supra note 1, at 473 (“astonishing rise”), 484 (“overwhelming evidence”). While there is certainly evidence of foreign trade secret theft, I am not aware of “overwhelming evidence,” nor would I necessarily describe the costs as “colossal,” at least not without stronger evidence to support such an extreme characterization. In any event, I would have liked to have seen a more careful review of the relevant empirical literature and a more critical attitude toward the political and media sources cited in the article.

5. Furthermore, it seems likely that this practice is on the rise now that the internet and computer technology make it possible to access secrets from remote locations. See HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING 8-10 (2005). There are numerous
fact that trade secrets are being taken, even with some frequency, is not by itself enough to justify stronger legal protection. Legal intervention through trade secret law can be very costly. We need to know how much trade secret theft is taking place before we can balance the benefits of stronger legal protection against the costs.

Professor Rustad does cite several studies which purport to quantify the magnitude of the problem, and there are also other existing studies. Most of these studies use survey methodology and ask firms to report the total number of trade secret loss incidents and the economic value of those losses. While these surveys provide some useful information, they also suffer from serious methodological limitations that undermine their reliability as measures of trade secret misappropriation. The following account briefly describes some of these limitations. While the factors discussed here tend to push the survey results higher than the true loss level, other factors tend to push in the opposite direction. All of these factors compound the uncertainty of the results.

I should state at the outset that I have not read every existing survey, so I do not know for sure whether all of them have serious methodological limitations. However, some of the defects identified documented cases of foreign country involvement. Indeed, in a statement delivered to the Senate during the 1996 hearings on the EEA, Louis Freeh, then Director of the FBI, reported that "at least twenty-three foreign governments actively target the intellectual property of U.S. corporations." Id. at 8.

6. See id. at 60. Also, there is a good deal of reliance on anecdotal evidence. Id. The problems with anecdotal evidence are well known — there is no assurance that anecdotes are representative or even accurate descriptions of what actually occurs.

7. For example, a firm might under-report its true losses because it fails to detect an instance of trade secret theft. Or a firm might decide not to report a known loss out of fear of potential reputation harms from an accidental public disclosure, despite promises of confidentiality. However, some studies make an effort to adjust the total estimates to take account of under-reporting. See, e.g., ASIS INTERNATIONAL, PRICEWATERHOUSECOOPERS & U.S. CHAMBER OF COMMERCE, TRENDS IN PROPRIETARY INFORMATION LOSS: SURVEY REPORT 11 (2002) [hereinafter 2002 ASIS Survey Report], available at http://www.asisonline.org/newsroom/surveys/spi2.pdf.

8. As Professor Nasheri explains: "Quantifying the risks is difficult because we simply do not have the data...[and] what statistics we have are difficult to generalize." NASHERI, supra note 5, at 60. While Professor Nasheri stresses under-reporting, data uncertainties actually cut in both directions, as I explain in the text. Even Professor Rustad admits at one point that "no reliable data exists on basic facts," such as the amount of financial loss due to misappropriation. Rustad, supra note 1, at 524.

9. I read three surveys in preparing this Comment: (1) the most recent ASIS Survey, see 2002 ASIS Survey Report, supra note 7; (2) the 1995 ASIS Survey Report, see RICHARD J. HEFFERNAN & DAN T. SMARTWOOD, TRENDS IN INTELLECTUAL PROPERTY LOSS SURVEY (American Society for Industrial Security, Int'l 1995) [hereinafter 1995 ASIS Survey Report]; and (3) the 2005 CSI/FBI Computer Crime Survey, see LAWRENCE A. GORDON ET AL., CSI/FBI
below would be very difficult, if not practically impossible, to eliminate. In any event, one thing is clear: when citing survey evidence, one should be aware of its potential limitations, and should take those limitations into account when making claims based on the results.

One problem with trade secret surveys is the difficulty of verifying that a loss is indeed due to trade secret theft. Trade secrets, like all forms of information, exhibit the public-good characteristics of nonexcludability and nonrivalry. This means that a trade secret can be appropriated without depriving the owner of the information. As a result, a firm might suspect that its trade secret has been taken, but have very little evidence to support the suspicion and no evidence to identify the responsible party. The suspicion alone might be enough for the firm to report the loss, especially if the firm is asked to report suspected as well as known losses. But if the suspicion turns out to be unfounded, the report will erroneously inflate survey results.

Another related problem is that not all methods of acquiring trade secrets are illegal. It is perfectly lawful, for example, to reverse-engineer a trade secret or to discover it by searching publicly available records. Those who complain about economic espionage are not always careful to distinguish between lawful and unlawful methods. Indeed, it is not clear how a survey could be designed to


10. In addition, some surveys cover much more than trade secret loss. The CSI/FBI Computer Crime Survey, for example, collects data on many different kinds of computer security breach, including virus damage, denial of service losses, laptop theft, and the like. See 2005 CSI/FBI Survey, supra note 9, at 15.

11. See WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 13-14 (2003). The fact that information is infinitely replicable at little marginal cost has two important consequences: (1) it means that it is difficult to exclude others after information is made public (nonexcludability), and (2) it means that everyone can possess the information without anyone having any less of it (nonrivalry).

12. It should be noted that Professor Rustad is aware of the difficulties with detecting trade secret theft and identifying the perpetrator. His article mentions the problem repeatedly. See generally Rustad, supra note 1.

13. For example, the 2002 ASIS Survey Report lumps “suspected losses” together with “known losses.” See 2002 ASIS Survey Report, supra note 7, § 3.2 at 9.

14. For example, Professor Rustad quotes a source that defines “economic espionage” as “the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies.” Rustad, supra note 1, at 464. Notably, this definition includes both “clandestine” and “unlawful” methods, even though trade secret law reaches only the latter. As another example, Professor Nasheri, in her recent book on economic espionage and the EEA, condemns eleven methods of acquiring
reliably screen out losses due to lawful activity. For example, if Firm A discovers that Firm B is using information which A keeps as its trade secret, it would be natural for A to assume wrongdoing and report the loss in response to a survey question even if B actually obtained the information in a perfectly lawful way.15

A third defect is perhaps the most serious of all.16 The law protects trade secrets only if the trade secret owner first implements reasonable security precautions on its own.17 The idea is to force firms to use less costly forms of self-help to prevent misappropriation before allowing them access to costly litigation after a misappropriation occurs. This means, however, that any survey used to support more expansive trade secret protection must be limited to firms that already have reasonable security measures in place. The problem is that some of the most frequently cited surveys are not limited in this way. For example, the 2002 ASIS Survey, while it asks respondents about their security precautions, makes no effort to exclude firms with inadequate precautions from the reported loss totals.18 This omission is particularly salient since there is reason to believe that many firms neglect their security needs and could easily avoid some of their information losses if they installed reasonable security measures.19

15. The 1995 ASIS Survey Report asks respondents to identify the method by which the loss occurred. However, some of the categories, such as copyright, patent, or trademark violation, do not involve trade secret appropriation at all, and some are described in such vague language that they give firms an opportunity to report losses of unknown cause — something even the ASIS Report itself concedes. 1995 ASIS Survey Report, supra note 9, at 12-13. In any case, given the difficulties of detecting and investigating trade secret theft, identification of the method of acquisition is bound to involve a lot of guesswork.

16. There are other defects as well. For instance, many of the most frequently cited surveys are sponsored by groups with an obvious self-interest in the results, such as the American Society for Industrial Security (which is an association of security professionals) and PricewaterhouseCooper Cybercrime Prevention and Response (CPR) Group (which advises companies on their security needs). See, e.g., 2002 ASIS Survey Report, supra note 7, at 3.


18. In fairness, I should make clear that the ASIS survey was not designed specifically with an eye to advocating for broader legal protection. In fact, one of its major goals is to encourage firms to adopt stronger security measures on their own. See 2002 ASIS Survey Report, supra note 7, at 28.

19. Indeed, the 2002 ASIS Survey Report itself found widespread neglect of security needs among firms reporting losses. It also found a strong negative correlation between the
My point is simple: we do not have enough reliable empirical evidence to be sufficiently confident of the magnitude of the misappropriation problem to advocate strongly for legal reform. It bears repeating that it is not enough simply that stronger trade secret protection would prevent more trade secret thefts. Trade secret law generates substantial costs of its own so the benefits of stronger protection must be substantial as well.

Like many advocates of broader trade secret protection, Professor Rustad argues at times as if he believes that an ideal legal system would prevent all trade secret appropriation. His use of the word "theft" is suggestive in this regard. It trades on strong moral intuitions and conjures up images of criminals stealing tangible property. An intangible trade secret, however, is very different from tangible property, and the differences make enforcing trade secret rights much more costly than enforcing other types of property rights.

Two features of trade secrets are particularly salient in this regard: their quality as information and their quality as secrets. Because information can be taken without leaving a trace behind, it can be extremely difficult to establish that a trade secret has been misappropriated, and equally difficult to identify the perpetrator. As a result, detection and investigation can be very costly and civil suits and criminal proceedings expensive to litigate.\textsuperscript{20} Moreover, these costs tend to escalate as trade secret appropriators respond to greater investments in detection and investigation by adopting more sophisticated and difficult to detect appropriation techniques. Indeed, this dynamic can turn into a costly arms race if trade secret owners respond to more sophisticated appropriation techniques by adopting more sophisticated detection and investigation counter-measures, thereby triggering yet another round of response and counter-response.

Even more serious are the potential costs to technological

---

priority a company placed on information security and the amount of loss the company reported. See 2002 ASIS Survey Report, supra note 7, §§ 3.9-3.11, § 4, at 18-25, 27 (concluding that "[r]esearch data about attitudes and best practices reveals that many companies do not follow important basic information protection policies"); see also 1995 ASIS Survey Report, supra note 9, at 19-29 (detailing widespread failure to implement basic security precautions and urging firms to develop systematic and comprehensive Safeguarding Proprietary Information (SPI) Programs); NASHERI, supra note 5, at 65 (noting that a "lax attitude and insensitivity to secrets is common in the business world.")

Innovation. By rewarding secrecy, trade secret law encourages firms to keep secrets, and secrecy impedes the diffusion of information. When one firm's stronger trade secrecy prevents other firms from building on the information, the pace of innovation is likely to slow with negative effects on economic productivity.\(^\text{21}\)

In sum, while it is natural for a trade secret owner to want to safeguard its secrets from all forms of appropriation and thus to push for ever broader legal protection, these incentives are not necessarily optimal for society at large because of the externalities that trade secret law creates. These externalities include expensive litigation, wasteful arms races over detection, and impediments to innovation. The fact is that firms currently have access to state trade secret remedies and may sue both foreign and domestic misappropriators when jurisdictional and other procedural requirements are satisfied.\(^\text{22}\)

Given the empirical uncertainty and the potentially serious costs, I am skeptical about the wisdom of adding to these remedies by strengthening the EEA.

### III. SECONDARY LIABILITY FOR TRADE SECRET MISAPPROPRIATION

In this section, I assume, for purposes of argument, that there is a serious trade secret theft problem warranting legal reform, and I focus on whether secondary liability makes sense as a solution. First, I

---

21. *Id.* at 266-67. This is especially problematic when a firm chooses trade secrecy rather than patent to protect its patentable invention, since doing so frustrates the Patent Act's strong policy in favor of public disclosure. *See id.* at 269. The adverse impact of secrecy on innovation is illustrated by well-known studies of Silicon Valley and Route 128, which highlight the benefits of porous secrecy protection in facilitating information diffusion through employee mobility. *See, e.g., Annalee Saxenian, Regional Advantage: Culture and Competition in Silicon Valley and Route 128 (1994); Ronald J. Gilson, The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete, 74 N.Y.U. L. REV. 575 (1999) (focusing on the California rule prohibiting enforcement of covenants not to compete). Indeed, trade secret owners could end up in a Prisoners' Dilemma, in which they take advantage of strong trade secret protection when it is offered even though they would be better off if they all could credibly commit themselves to refrain.

22. Professor Rustad also argues that the current system of state remedies ought to be replaced by a federal statute in order to achieve uniformity and to tap the expertise of federal courts. *See Rustad, supra* note 1, at 514. I am not convinced, however, that much would be gained by federalizing trade secret law. The core features of state law are fairly uniform already (although there are some variations, as Professor Rustad notes), and the expertise of federal judges is not readily transferable from copyright and patent to trade secret because of the distinctive liability theories underlying these different forms of protection. In any event, even if the arguments for a federal claim are persuasive, adding a private claim to the EEA is not the best way to do it. Rather than gerrym a statute that was never designed for private enforcement, it would be better if Congress considered the matter anew and constructed an appropriate federal statute from scratch.
review secondary liability doctrine generally in the trade secret field and speculate on some reasons for its relative scarcity. Then I examine software defects and Professor Rustad's proposal.

A. Secondary Liability Generally in the Trade Secret Field

Secondary liability is liability imposed on a third party who actively induces, materially contributes to, fails to control, or in some other significant way facilitates the infringing acts of others. The key feature of the doctrine is that it holds a party liable for the underlying infringement even though that party does not itself do the infringing act.

Although the secondary liability doctrines of contributory infringement, vicarious liability, and active inducement play an important role in other areas of intellectual property law, especially copyright and patent, they do not play a significant role in trade secret law. The principal trade secret doctrine imposing liability on third parties is in fact based on a form of primary rather than secondary liability. This doctrine holds that a third party is liable when the third party acquires a trade secret from another and then discloses or uses the secret under circumstances where he knows or should have known that the trade secret was wrongfully acquired. The third party is liable for his own use or disclosure, and the knowledge requirement assures some degree of individual culpability.

The one genuine example of secondary liability in trade secret law is the respondeat superior liability of employers for trade secret misappropriation by their employees. Yet even here the case law is quite thin and the opinions relatively recent. Notably, those judges

23. I base this conclusion on a search of the indices of the major trade secret treatises, which, with one exception covered in the text of this Comment, do not list "secondary liability," "contributory infringement," "vicarious liability," or "respondeat superior." Moreover, the Third Restatement of Unfair Competition does not include a secondary liability theory; it confines the liability of third parties to the principles discussed here. Finally, a search for federal and state cases in LEXIS, using combinations of "trade secret" and one of the aforementioned phrases, revealed only the few employer respondeat superior cases discussed in this Comment.

24. See, e.g., UNIFORM TRADE SECRETS ACT § 1(2)(ii), 14 U.L.A. 433 (1985); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40(b)(3) & cmt. d (1995). Conversely, a third party who acquires a trade secret from another without actual or constructive knowledge that the trade secret was wrongfully acquired is not liable for use or disclosure of the trade secret, at least not until the third party learns about the misappropriation.

who make an effort to analyze the issue struggle to square respondeat superior liability with traditional trade secret principles. These justificatory difficulties are instructive, for they suggest that there is no strong tradition of secondary liability in trade secret law. The question is why.

One possible answer is that trade secret law has less need for secondary liability than does copyright and patent law. In copyright, for example, a major reason for secondary liability is to solve certain enforcement problems and encourage less costly methods of preventing infringement. For instance, when there are many potential infringers under the control of a third party with the ability to reduce or eliminate the infringements, holding the third party liable on a contributory infringement or vicarious liability theory saves transaction costs and can prevent the infringements more efficiently than suing all the direct infringers individually. The obvious litigation cost advantages give copyright owners a reason to push for recognition of secondary liability, and the efficiency benefits give judges a reason to respond favorably. Similarly, when the direct infringers are judgment proof (as might be the case for young musicians and artists living on a shoe string), copyright owners have an incentive to seek secondary liability doctrines that make it possible to reach third parties with deeper pockets.

Cases like these—involving multiple direct infringers under the control of a third party or infringers who are judgment proof—are much less likely to arise in the trade secret field. As a result, there are probably fewer occasions for plaintiffs to seek secondary liability and fewer opportunities for judges to consider it. For instance, trade secret cases do not normally involve multiple misappropriations by separate individuals under the common control of a third party. Misappropriation is usually a single, discrete act performed by one or a small number of persons, all of whom can be easily sued in the same lawsuit. Furthermore, many trade secret cases involve employees who take their former employer’s trade secrets to their

26. Most of these cases deal with the issue in the context of state statutes modeled on the Uniform Trade Secrets Act. One of the difficulties involves reconciling respondeat superior liability with the traditional rule, codified in the UTSA, that a third party without knowledge cannot be held liable. See, e.g., Newport News Indus. supra note 25, at 752-54; see also Infinity Prods. v. Quandt, 810 N.E.2d 1028, 1033-34 (Ind. 2004) (rejecting respondeat superior liability under the Indiana trade secret statute because the statute requires actual or constructive knowledge on the employer’s part).

new employment. The problem of the judgment-proof defendant will not arise in these cases if the new employer has sufficient assets to pay the judgment, since the new employer itself can be held liable on grounds of actual or constructive knowledge or on a theory of respondeat superior.

Another possible reason for the relative scarcity of secondary liability doctrine in trade secret law has to do with doctrinal differences between trade secret and other intellectual property theories. Copyright and patent create forms of strict liability for well-defined acts, and the class of direct infringers is limited to those who do one of those acts. No one else can be a direct infringer, no matter how involved they are in the infringing activity. For example, the Copyright Act imposes liability on anyone who "publicly performs" a copyrighted work without permission, and the Act defines "to perform a work" as to "recite, render, play, dance, or act it." Therefore, a concert promoter who profits from promoting a singer while knowing that the singer performs copyrighted songs illegally does nothing that directly infringes copyright, despite his obvious culpability. One needs a secondary liability doctrine—in this case, contributory infringement—to hold the promoter liable.

Trade secret law is not based on strict liability. The acquisition, use, or disclosure of a trade secret must involve a breach of confidence or some other type of wrongful conduct. This requirement narrows the scope of liability as compared with copyright and patent. But it also makes it easier to catch culpable third parties in the direct liability net. For example, a person who encourages or entices another to misappropriate a trade secret, and then profits from the use, can easily be seen as a primary wrongdoer directly liable for the unlawful use. There is no need in such a case to struggle over refined distinctions between primary and secondary liability.

28. See 1 MILGRIM, supra note 17, § 5.01 ("[T]he great majority of reported trade secret cases arise in the context of the employer-employee relationship.").

29. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION, supra note 24, § 40, cmt. d, illus. 2 (actual or constructive knowledge of the misappropriation); see also supra text accompanying notes 25-26 (discussing respondeat superior).


31. See 2 MILGRIM, supra note 17, § 7.02 [a] (explaining the rules for holding parties liable for inducing or conspiring in trade secret misappropriation).
B. Secondary Liability for Computer Software and Professor Rustad's Proposal

The fact that secondary liability has not historically been terribly important to trade secret law does not mean that the doctrine should not be applied to computer software manufacturers and vendors in the way Professor Rustad recommends. However, whether it is a good idea to do so depends on the costs and benefits.

The first thing to note is that Professor Rustad's proposal differs from the typical secondary liability case. In cases like Sony Corp. of America v. Universal City Studios, Inc.,32 A & M Records, Inc. v. Napster, Inc.,33 and Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.,34 the product in question was used directly by the infringers to carry out their infringements. In the scenario Professor Rustad contemplates, the product (computer software) is used by the trade secret owner to protect its trade secrets. It is a software defect that renders those secrets vulnerable to misappropriation.

In the following discussion, I will first consider the secondary liability question in its more conventional form, and then address it in the context of Professor Rustad's proposal.

1. Conventional Secondary Liability for Distribution of Computer Software

In the conventional secondary liability case paralleling Sony, Napster, and Grokster, a vendor sells software to consumers, some of whom use the software to penetrate a firm's security and misappropriate its trade secrets. In this situation, liability has nothing to do with defects in the software. It has to do instead with how the software is used.

Secondary liability makes sense for software programs designed and marketed with the intent that they be used as tools of misappropriation, such as a hacking program created and distributed by a proud hacker. This scenario falls squarely under the inducement theory articulated by the Supreme Court in the Grokster case. However, the scenario is not likely to involve legitimate software companies.

Beyond this obvious and extreme case, it is highly doubtful that the benefits of secondary liability justify the costs. It is possible, in

33. 239 F.3d 1004 (9th Cir. 2001).
34. 125 S. Ct. 2764 (2005).
theory at least, to imagine a software program marketed for legal purposes that is frequently used or adapted to misappropriate trade secrets. In such a case, it might be more effective to enjoin the software vendor than to pursue each of the many misappropriators individually. But there are at least three serious problems with this secondary liability approach.

First, as cases in the copyright and patent fields make clear, it is important to confine secondary liability based on selling a lawful article of commerce to situations where the illegal use of the article is sufficiently pervasive. This requirement creates problems for the trade secret case because proving that a software program is being used pervasively for misappropriation is bound to be extremely difficult. By contrast, proof of illegal use is relatively easy in copyright cases like Sony and Napster because of the nature of the technology and the relative simplicity of the illegal act.

Second, trade secret thieves have a variety of tools to achieve their illegal objectives. Enjoining the software vendor deprives them of only one such tool, and they are likely to respond by switching to another. As a result, it is not clear that secondary liability will significantly reduce the rate of serious trade secret theft. To be sure, the alternative methods might be more costly, but if the value of the trade secret is substantial enough, the additional cost should be no impediment. At the limit, the misappropriator will just bribe current employees or place its own agents inside the company.

Third, imposing secondary liability on software vendors is likely to chill software innovation. A software company interested in developing a new software product would have to take into account the possibility that its product would be used or adapted for illegal purposes and that its sale may be enjoined by a court. Limiting relief to reasonable damages can reduce this chilling effect, but it is not clear how to formulate a damage remedy to fit a large aggregate of trade secret violations. In a secondary liability copyright case like Sony or Napster, it is possible to use statistical sampling techniques to get a rough idea of the frequency of unauthorized copying, and then apply the statutory damage provisions to arrive at an aggregate

35. Otherwise, the risk of liability will chill innovation and give the copyright or patent owner—and here the trade secret owner—excessive control over promising technology.

36. Employee-based strategies for appropriating trade secrets are a very common technique. Indeed, Professor Rustad finds in his examination of EEA cases that "employees, ex-employees, and insiders were the primary wrongdoers in seventy-three percent of the EEA prosecutions." Rustad, supra note 1, at 492.
damage award. However, statutory damages are not available in trade secret cases. Instead, monetary relief is usually measured by a plaintiff’s actual loss or a defendant’s illegal gain, and there is no obvious statistical way to calculate these amounts on an aggregate basis without identifying individual victims and individual losses.

2. Professor Rustad’s Proposal: Liability for Negligent Enablement of Trade Secret Theft

Professor Rustad’s actual proposal could be considered a form of secondary liability insofar as it imposes liability on a software vendor for trade secret misappropriation perpetrated by another person. However, it is better, I believe, to view it as a form of primary liability based on the software vendor’s primary negligence in inadequately designing and testing its software product. The policy behind the proposal—to encourage more careful testing—fits a primary negligence theory, and liability depends on the vendor’s failing to use reasonable care. Viewing the proposal this way, the desired end is to improve the security of software and the recommended means is to include trade secret loss in the remedy for negligence.

Many critics agree with Professor Rustad that software testing procedures are too lax and that companies today sell software products with easily preventable security defects. If this is true, negligence liability for some types of losses might improve testing and encourage the production of more secure software. The question, however, is whether negligence liability should extend to trade secret losses. From a doctrinal perspective, the issue can be treated as one of causation. Should negligently defective software be considered the cause of a trade secret loss when someone else—the trade secret


38. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION, supra note 24, § 45. It might be possible to use a reasonable royalty measure and make the royalty uniform across all cases, but there would still be a problem estimating the frequency of misappropriation.

39. Professor Rustad’s proposal requires two things: (1) negligence on the part of the software vendor, and (2) an unlawful appropriation of a trade secret. This creates a potential problem. A firm must have reasonable secrecy precautions in place before it can bring a trade secret claim. If software testing is considered a reasonable precaution, the trade secret owner would have to test the software itself before it could complain of trade secret misappropriation. But then its testing could eliminate any basis for holding the software vendor liable. To avoid this problem, I shall assume that the EEA under Professor Rustad’s proposal does not require software testing as one of the reasonable precautions necessary to qualify secret information as a trade secret. This assumption would make sense as a policy matter if it is less costly for the software vendor to test once than for all the buyers to test separately.
thief—actually does the dirty deed and could have used other means to accomplish it? From a policy perspective, the issue is one of cost-benefit balancing. What is the optimal balance between the costs of chilling software innovation and the benefits of reducing trade secret loss?40

Let us focus on the policy problem. The chilling effect is easy to understand. Under Professor Rustad’s proposal, a software manufacturer or vendor would have to pay all trade secret losses of all its customers caused by unreasonable defects in its software product. Damages for trade secret loss can be very large when only a single firm is involved, and those damages are certain to compound quickly when multiplied over a large number of firms. Even if, as Professor Rustad suggests, reasonable care standards become clearer over time, there is still a significant risk that a jury will find liability no matter how carefully a company follows the teachings of past cases.41

Combined with a huge potential verdict, even a modest chance of liability could trigger a risk-averse response, especially in smaller software companies, and discourage new entry into particularly risky software markets (such as the market for security software).42 If this occurs, competition would suffer, and with only a few companies in the market, the pace of innovation would suffer too. Moreover, even if companies do enter the market, they would have to charge a very

40. One rough analogy is the negligence liability of gun manufacturers for injuries or deaths caused by the illegal use of handguns. See Aaron Twerski & Anthony J. Sebok, Liability Without Cause? Further Ruminations on Cause-in-Fact as Applied to Handgun Liability, 32 CONN. L. REV. 1379 (2000). This issue also involves uncertain causation and potentially burdensome liability.

41. Indeed, the software field is so dynamic that a plaintiff’s attorney should often be able to point to better testing procedures and argue that the defendant should have known about and used those procedures. The defendant might still prevail in the end, but the availability of these arguments enhances the risks.

42. Professor Rustad refers at times to “known defects” and sometimes describes the software vendor’s duty in terms of using “readily available means” to enhance software security. These references suggest the possibility that Professor Rustad means to confine negligent enablement liability to proof of recklessness—in other words, to situations where the defendant fails to take relatively inexpensive and obvious steps to safeguard against clear risks from known defects. If this is what he has in mind, the chilling effect of his proposal would be significantly reduced, but so too would its effectiveness in creating incentives for more secure software. In most of the article, Professor Rustad describes his theory in ordinary negligence terms-as embracing cases where the defendant not only knew but “should have known” of the risks and where reasonable testing would have revealed the defect. Therefore, I shall assume that Professor Rustad contemplates an ordinary negligence standard tailored, of course, to the specific nature of the risks and costs involved in software design and use. See Rustad, supra note 1.
high price to cover insurance for the additional liability. Thus, an attempt to reduce software defects could end up substantially increasing the price of software and impeding the creation of better software products—or at least significantly delaying their introduction into the market.

This risk might be worth taking if the deterrence benefits were great enough, but this is not likely to be the case. As noted above, there are many different ways to misappropriate trade secrets other than penetrating a firm’s software. If software is more secure, someone bent on acquiring the firm’s trade secret will probably just switch to another method, such as bribing employees or placing an agent in the company—or maybe even figuring out new ways to penetrate the firm’s software shield.\textsuperscript{43} Thus, Professor Rustad’s negligent enablement liability could impose an onerous burden on software companies without doing much to prevent the most serious trade secret losses.

There is another reason to question Professor Rustad’s proposal: contract law might be a better way than tort law to control the risks of trade secret loss. It is true, as Professor Rustad points out, that contract law works poorly for mass-marketed software because manufacturers use shrinkwrap or clickwrap licenses to disclaim liability. But firms with valuable trade secrets have an option other than buying the mass-marketed product. They should be able to contract individually with the manufacturer or vendor for software that has been more extensively tested and meets the firm’s particular security needs (and perhaps also includes warranties against loss).

There are advantages to the contract approach. One advantage is that the software product can be tested and customized to fit the overall software needs of the contracting firm. Another advantage is that it can facilitate efficient price discrimination. Since ordinary consumers do not face the same risks as trade secret owners, it seems reasonable to suppose that they would prefer a less carefully tested product if they could buy it at a lower price. The contract solution allows for this market segmentation. Ordinary consumers can pay the mass-market price while trade secret owners pay a higher price for a more secure product.

\textsuperscript{43} Experience with encryption teaches that there are plenty of clever programmers who enjoy the challenge of figuring out ways to circumvent novel security measures. In fact, in a footnote discussing the problem of multiple causation, Professor Rustad assumes that there can be more than one way to access trade secret information, but he fails to recognize how the availability of alternatives threatens the deterrence benefits of his proposal. \textit{See} Rustad, \textit{supra} note 1, at 502 n.200.
There are potential problems with the contract solution, but I do not think they are disqualifying. For example, a firm might be reluctant to pay for additional software testing if it believes that the company will just sell the better tested product to everyone, including the firm's competitors. Under these circumstances, each firm would have an incentive to free-ride on the others. However, the software manufacturer could apportion the additional testing costs among all its corporate customers if coordination is not too difficult.44

In sum, before holding software manufacturers or vendors liable for trade secret loss on a negligent enablement theory, one should first be confident that the social costs of chilling software innovation and increasing the price of software products do not outweigh the marginal benefit of reducing trade secret theft. I am not at all confident that this is the case, and therefore counsel restraint in implementing Professor Rustad's proposal. Restraint is all the more important because there is a potentially superior alternative to negligent enablement, namely, relying on contract to allocate the risk of loss.

IV. CONCLUSION

Professor Rustad's proposal is intriguing. However, much more empirical and normative work is necessary before its merits can be fully evaluated. Secondary liability has never been a prominent feature of trade secret law, and there are strong reasons to exercise

44. The contract solution works better when the software market is more competitive, since in a competitive market new entrants would supply the better-tested product if the original manufacturer refused to do so (and it was profitable). As one participant at the conference pointed out, the market for some types of software, such as operating systems, is not terribly competitive due to the lock-in effect of network externalities and the availability of exclusive intellectual property rights. However, I do not believe that this concern warrants rejection of the contract approach. Just because the software manufacturer has market power does not mean that there will be no contracts. It just means that the contract price will be higher. Even if a monopolist insists for some reason on selling only the mass-marketed version, trade secret owners could simply purchase that version and test for and correct any defects on their own. Admittedly, this alternative is not socially optimal. The manufacturer should be a more efficient tester since it knows its own product, and each purchasing firm testing on its own creates wasteful duplication of effort. However, assuming no antitrust obstacles, trade secret owners could form a coalition to negotiate collectively with the software manufacturer, or pool their resources to do the testing and modifying only once. It is possible that testing and modifying the software might run into copyright problems, especially if the code has to be reproduced in the testing process. But the resulting copyright infringements should be treated as fair use. Cf. Sega Enter. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) (holding that disassembly of a copyrighted computer program is a fair use when the disassembly is the "only way to gain access to the ideas and functional elements" in the program and "there is a legitimate reason for seeking such access").
restraint in extending it to software manufacturers and vendors. Professor Rustad’s proposal, in particular, is highly problematic, whether it is treated as a form of secondary liability for trade secret theft or a form of primary liability for negligence. In the end, I am deeply skeptical that its likely benefits justify its inevitable costs.