THE YALE LAW JOURNAL

COMMENT

Shifting the Burden in Software Licensing Agreements

Consumer information is exchanged more frequently with each passing day. Indeed, the number of electronic payments in the United States in 2009 totaled 84.5 billion, representing a 31% increase since 2006.[1] Whether consumers purchase clothing online or swipe their Visa cards after dinner, personal information moves constantly through the electronic channels of commerce. As consumers expect to purchase goods more easily in this electronic economy, they also rely increasingly on businesses to protect their personal information.[2]

Businesses protect consumer information by installing encryption and data security software. Recently, one state even mandated that businesses take specific and complex preventive measures to help ensure that security breaches do not occur.[3] As many companies are now required to use data security

1. *See* FED. RESERVE SYS., THE 2010 FEDERAL RESERVE PAYMENTS STUDY: NONCASH PAYMENT TRENDS IN THE UNITED STATES: 2006-2009, at 22 tbl.4.2 (2011), *available at* http://www.frbservices.org/files/communications/pdf/press/2010_payments_study.pdf.

2. *See* FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY-DECEMBER 2009, at 3 (2010), *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf (noting that the Consumer Sentinel Network "received over 1.3 million complaints during calendar year 2009: 54% fraud complaints; 21% identity theft complaints; and 25% other types of complaints").

3. *See* Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00 (2011) [hereinafter Massachusetts Privacy Regulation]. The Massachusetts regulation requires all companies that "own or license personal information about a resident" to provide "security and confidentiality" for this information. *Id.* at 17.01. Specifically, the new Massachusetts regulation requires companies to implement a "written, comprehensive information security program" and encrypt all personal information stored on portable devices and all personal information that is transmitted wirelessly or over public networks. *Id.* at 17.04.

software, software vendors find themselves in increasingly strong bargaining positions when negotiating software licensing agreements.[4] Further, the highly specialized nature of this software and the consolidation within the software security industry mean that fewer vendors provide these products, and businesses in need of this software face increasingly asymmetrical negotiations.[5] Certain companies, including smaller businesses, face the most pressure because they have fewer options for recourse if a fair licensing agreement is not reached.[6]

Some critics also argue that this level of industry consolidation has led to a decline in the quality of products offered by some software vendors.[7] Despite the fact that some software companies are arguably providing a lower quality good, the bargaining power created by consolidation in the industry—combined with the fact that many businesses are statutorily required to use

4. *See* Steven P. Mandell & Stephen J. Rosenfeld, *Drafting Software Licenses for Litigation*, *in* UNDERSTANDING THE INTELLECTUAL PROPERTY LICENSE 2009, at 741, 746 (PLI Intellectual Prop. Practice, Course Handbook Ser. No. 19149, 2009).

5. *See, e.g.*, Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 314-15 (2006) (describing the theory that suppliers have little incentive to "add high levels of security because the buyer has no low-cost method for ascertaining quality"); *Security Software Market To Grow 8% in 2009*, HELP NET SECURITY (Sept. 21, 2009), http://www.net-security.org/secworld.php?id=8137 ("The security software market in 2008 was characterised by a high level of consolidation with the examples of Mc Afee [sic] purchasing Secure Computing, Symantec and Sophos acquiring MessageLabs and Ultimaco, respectively. This is a sector where further consolidation is expected in the near future." (quoting Ruggero Contu, Principal Research Analyst, Gartner, Inc.)). The consolidation in this market can be seen by the fact that the top two business security software vendors, Symantec and McAfee, maintain almost half of the market share. *See Higher McAfee Share in Business Security Software*, THESTREET (Aug. 27, 2010, 3:44 PM), http://www.thestreet.com/story/10846552/higher-mcafee-share-in-business-security-software.html (noting that McAfee maintained about 17% market share in business security software as of 2010); Trefis Team, *Sophisticated Cyber Attacks Expand the Addressable Security Software Market*, NASDAQ (Mar. 2, 2011, 10:30 AM), http://community.nasdaq.com/News/2011-03/sophisticated-cyber-attacks-expand-the-addressable-security-software-market.aspx?storyid=60129 (noting that Symantec is the market leader with roughly 29% of the business security software market). Other major business security software vendors, including Trend Micro, IBM, and EMC, maintain substantial market shares as well. *See* Ellen Messmer, *Intel Steps in to Security Software Market with McAfee Deal*, COMPUTERWORLDUK (Aug. 20, 2010), http://www.computerworlduk.com/in-depth/security/3236326/intel-steps-in-to-security-software-market-with-mcafee-deal ("Led by Symantec, McAfee, Trend Micro, IBM and EMC, total industry sales are projected to hit at least $16.5 billion this year . . . .").

6. *See* Nim Razook, *Legal Issues Facing Corporations*, 36 CREIGHTON L. REV. 643, 655 (2003).

7. Larry Walsh, *Analysis: Security Industry Consolidation*, CSO ONLINE (Nov. 7, 2007), http://www.csoonline.com/article/221303/analysis-security-industry-consolidation ("Longtime customers and partners have complained bitterly about the decline in quality . . . .").

data security software—allows these companies to disclaim practically all liability stemming from a security breach, even where the software fails.[8]

Moreover, as businesses acquire and transmit more consumer information, the potential liabilities associated with a security breach increase. Indeed, several of the worst data security breaches have occurred in recent years.[9] One example involved TJX Companies, a clothing retailer. In 2007, TJX suffered a breach and lost roughly 45.7 million credit card numbers.[10] By 2008, the cost of this security breach was estimated at $216 million, and this figure was expected to climb because of pending litigation, including a class-action lawsuit.[11]

Although the number of people affected and the frequency of security breaches are troubling, this Comment focuses on a company's potential liability after a breach. In doing so, however, it offers a solution that provides software vendors with strong incentives to manufacture more secure products.

When businesses lose information because of a security breach, they face massive costs, as illustrated by the TJX breach. Recently, many states have increased these costs by passing more complex and expensive reporting requirements. These disclosure statutes shift greater costs from consumers to the businesses that hold their information should a breach occur. While these changes affect the relationship between consumers and businesses, software licensing agreements between vendors and businesses remain unchanged. In short, these agreements continue to restrict vendors' liabilities, allowing them to avoid these new burdens. The ability of vendors to avoid these liabilities is

8. *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 427 (2008) ("Yet, software vendors have traditionally refused to take responsibility for the security of their software, and have used various risk allocation provisions of the Uniform Commercial Code (U.C.C.) to shift the risk of insecure software to the licensee.").

9. Mandell & Rosenfeld, *supra* note 4, at 745; *see also* David Hakala, *The Worst IT Security Breaches of 2007*, IT SECURITY (Jan. 22, 2008), http://www.itsecurity.com/features/top-security-breaches-2007-012208 (noting that both private companies, such as TD Ameritrade and Gap, Inc., and public entities, such as the Texas Commission on Law Enforcement Standards and Education and the College of Southern Nevada, have recently suffered data security breaches).

10. *See* Dawn Kawamoto, *TJX Says 45.7 Million Customer Records Were Compromised*, CNET NEWS (Mar. 29, 2007, 9:28 AM), http://news.cnet.com/TJX-says-45.7-million-customer-records-were-compromised/2100-1029_3-6171671.html.

11. *See* Hakala, *supra* note 9.

especially troubling considering that in 2010 more than a quarter of security breaches were due to a system failure.[12]

To address this situation, this Comment argues that courts should adopt a fairer remedy under the Uniform Commercial Code (UCC) by holding unreasonable limitations on liability unenforceable when contractual remedies frustrate the essential purposes of the contract. This remedy will allow businesses to spread costs more efficiently, will give the proper incentives to software vendors,[13] and will allow the UCC to achieve its goal of allowing expectation damages in the case of a breach. This solution is a measured response to the current imbalance in the data security licensing industry because it would only invalidate licensing agreement provisions that frustrate the essential purpose of the contract.

Part I provides a brief background on how Article II of the UCC affects software licensing agreements. Part II then introduces the recent state statutory developments in data security and demonstrates why these new reporting requirements justify shifting additional liability back to software vendors. Part III builds on Part II and argues that courts should stop enforcing a licensor's limitations on liability when they frustrate the agreement's essential purpose, except in cases where the fault causing the breach lies with the software user.[14]

I. SOFTWARE LICENSING AGREEMENTS AND THE UCC

A. Applying Article II to Data Security Licensing Agreements

Whether Article II even applied to the sale of software was a hotly debated issue just fifteen years ago.[15] This initial question is critical because Article II covers only transactions that involve a sale of goods.[16] "Goods" are defined as

12. PONEMON INST., 2010 ANNUAL STUDY: U.S. COST OF A DATA BREACH 25 (2011), *available at* http://www.cenzic.com/downloads/Ponemon_DataBreach_201103.pdf (finding "system failures" account for 27% of all breaches).

13. By placing potential liability on software vendors when their products fail and cause a breach, this remedy can be expected to protect consumers' information more effectively by giving vendors strong economic incentives to make more secure products.

14. This Comment does not advocate shifting liability should the breach occur because of user error. This shifting should only apply when there is a software failure caused by the software vendor's error.

15. *See* Amelia H. Boss & William J. Woodward, *Scope of the Uniform Commercial Code; Survey of Computer Contracting Cases*, 43 BUS. LAW. 1513, 1514-15 (1988).

16. U.C.C. § 2-102 (2003) ("Unless the context otherwise requires, this Article applies to transactions in goods . . . .").

"all things [including specially manufactured goods] that are movable at the time of identification to a contract for sale."[17] This definition distinguishes goods from services that lie beyond Article II's scope.[18]

Software is a hybrid good because it involves certain services that accompany the tangible product.[19] To determine whether software qualifies as a good or service, most courts evaluate the contract's "predominant purpose."[20] This test asks which part of the contract is paramount—the goods sold or the services rendered.[21] The second test, used by a minority of courts, is known as the "gravamen of the action" test.[22] Under the "gravamen" test, courts determine whether the source of the complaint regards the goods or the services section of the contract.[23] Even with these two tests, determining the contract's "predominant purpose" or the "gravamen of the action" can be complex because of these interrelated features. Despite this complexity, courts generally view software licensing agreements as contracts for "goods" and review their terms under Article II.[24]

B. Limiting Liability and Remedies Under Article II

Software licensors attempt to limit their liability by using provisions of the UCC, such as warranty disclaimers, limitations of liability, and limitations on

---

17. *Id.* § 2-103(1)(k).

18. Whether Article II applies to software transactions has been discussed widely. *See, e.g.*, David A. Owen, *The Application of Article 2 of the Uniform Commercial Code to Computer Contracts*, 14 N. KY. L. REV. 277, 278 & n.9 (1987).

19. *See id.* at 277-82.

20. *See, e.g.*, Bonebrake v. Cox, 499 F.2d 951, 960 (8th Cir. 1974) (articulating the predominant purpose test).

21. *See* Nat'l Historic Shrines Found., Inc. v. Dali, 4 U.C.C. Rep. Serv. (West) 71 (N.Y. Sup. Ct. 1967).

22. LYNN M. LOPUCKI ET AL., COMMERCIAL TRANSACTIONS: A SYSTEMS APPROACH 12 (4th ed. 2009).

23. *Id.* Under the gravamen of the action test, "[i]f the problem lies with the services, then Article 2 does not apply to the dispute even if the predominant purpose of the transaction is goods rather than services." *Id.*

24. *See, e.g.*, Dealer Mgmt. Sys., Inc. v. Design Auto. Grp., Inc., 822 N.E.2d 556, 560 (Ill. App. Ct. 2005) ("A sampling of decisions from various jurisdictions shows that courts have generally recognized that computer software qualifies as a 'good' for purposes of the UCC.").

remedies.[25] Licensors can disclaim these liabilities and warranties under the UCC because Article II allows parties to depart from the Code's default rules if they agree.[26] Simply put, the UCC promotes freedom of contract, and only a few provisions cannot be altered by agreement.[27]

Courts generally enforce the restrictive language inserted by software vendors in an effort to limit virtually all of their potential liabilities.[28] For example, in disclaiming the various warranties provided for in the UCC, many provisions inserted by vendors include disclaimers for: (1) "all implied warranties (e.g., merchantability and fitness for a particular purpose)"; (2) "any express warranties except as otherwise stated in the agreement"; and (3) "in those states that have adopted the Uniform Computer Information Transactions Act (UCITA), the warranties implied through UCITA."[29] Further, in limiting liabilities and remedies, vendors insist on including provisions that specify the licensee's remedies (if any)—including time frame and mechanism for providing notice of election of remedies—and that state that the remedies in the contract provide the "sole and exclusive" means of

25. *See* U.C.C. § 2-312(1)(a) (2003) (implied warranty of title); *id.* § 2-313 (express warranties); *id.* § 2-314 (implied warranty of merchantability); *id.* § 2-315 (implied warranty of fitness for a particular purpose).

26. *See* U.C.C. § 1-301(a) (2001); *see also* Thomas J. McCarthy, *An Introduction: The Commercial Irrelevancy of the "Battle of the Forms,"* 49 BUS. LAW. 1019, 1022 (1994) (discussing how gap-filler provisions only apply in the absence of contract disclaimers and terms negotiated by the parties).

27. *See* U.C.C. § 1-302(b) ("The obligations of good faith, diligence, reasonableness, and care . . . may not be disclaimed by agreement.").

28. *See, e.g.*, U.S. Achievement Acad., LLC v. Pitney Bowes, Inc., 458 F. Supp. 2d 389, 400 (E.D. Ky. 2006) (finding no unconscionability between "seasoned business entity" and software supplier); Bray Int'l, Inc. v. Computer Assoc. Int'l, Inc., No. CIV H-02-0098, 2005 WL 3371875, at *3 (S.D. Tex. Dec. 12, 2005) (finding that Texas law provided no bad faith exception to enforcement of limitation of liability clause); Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., 85 F. Supp. 2d 519, 529 (W.D. Pa. 2000) (noting that the license agreement limited duration of any warranty to ninety days and stating that "[t]here is nothing legally objectionable about such a temporal limitation"); Markborough Cal., Inc. v. Superior Ct., 227 Cal. App. 3d 705, 714-15 (1991) (holding that contractual limitation of liability clauses have long been recognized as valid).

29. *See* Mandell & Rosenfeld, *supra* note 4, at 751; *see also* AES Tech. Sys., Inc. v. Coherent Radiation, 583 F.2d 933, 939 (7th Cir. 1978) ("By limiting the warranties available and the remedies under the warranties, parties are able to provide a consensual allocation of risk in accordance with sound business practices.").

redress.[30] Vendors also sometimes require that businesses send back the defective software before receiving a refund.[31]

While vendors employ the UCC to disclaim many of these warranties and to limit their liabilities and remedies, businesses have attempted to recover some of the losses stemming from software vendors after security breaches.[32] Various theories used in these cases include unconscionability,[33] tort doctrines such as negligent misrepresentation or fraudulent inducement,[34] and the failure of essential purpose doctrine.[35] These theories usually do not prevail, except for the failure of essential purpose doctrine, which a few courts have adopted.[36] This doctrine renders liability limitations unenforceable if the remedy provisions frustrate the contract's essential purpose.[37]

Despite the limited acceptance of the failure of essential purpose doctrine, most courts continue to enforce these warranty and liability limitations in a manner that forces virtually all security breach costs and liabilities onto the businesses that use the software to protect consumers. Over the past few years, this asymmetrical situation has become more uneven as state legislatures have placed more complex notification and disclosure requirements on businesses should a breach occur. These added costs provide another justification for courts to use the failure of essential purpose doctrine to shift some potential liabilities back onto software vendors. Before Part III argues for that solution, Part II introduces the new requirements and costs recently placed on businesses by various state statutes.

---

30. Mandell & Rosenfeld, *supra* note 4, at 751.

31. *Id.* at 755.

32. *See, e.g.*, U.S. Fibres, Inc. v. Proctor & Schwartz, Inc., 509 F.2d 1043, 1048 (6th Cir. 1975) (concerning an unsuccessful claim by a business to recover on the basis of the contract's unconscionability).

33. *See, e.g.*, Hunter v. Tex. Instruments, Inc., 798 F.2d 299, 303-04 (8th Cir. 1986) (holding that a seller's ability to limit liability for breach of express warranties to repair or replace was not unconscionable).

34. *See, e.g.*, Moses.com Sec., Inc. v. Comprehensive Software Sys., Inc., 406 F.3d 1052, 1065 (8th Cir. 2005) (dismissing claim for negligent misrepresentation against software developer); *see* Scott, *supra* note 8, at 441-42; *see also* U.C.C. § 2-721 (2003) ("Remedies for material misrepresentation or fraud include all remedies available under this Article for non-fraudulent breach.").

35. *See* U.C.C. § 2-719(2).

36. *See, e.g.*, Givan v. Mack Truck, Inc., 569 S.W.2d 243, 247-48 (Mo. Ct. App. 1978).

37. *See, e.g.*, R.W. Murray, Co. v. Shatterproof Glass Corp., 758 F.2d 266 (8th Cir. 1985); Goddard v. Gen. Motors Corp., 396 N.E.2d 761 (Ohio 1979).

II. NEW AND EVOLVING STATUTORY FRAMEWORKS INCREASE LIABILITIES AND COSTS FOR BUSINESSES

A. Understanding the Myriad of State Reporting Requirements

Currently, forty-six states and the District of Columbia have enacted breach notification statutes.[38] These security breach statutes outline disclosure requirements for companies that lose consumer information during a security breach. After a breach occurs, companies must first decide whether the "breach" triggers the statutory requirements. The vast majority of these statutes define "breach" broadly, so this is a simple determination.[39] For example, Texas and California define "breach" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information."[40]

Once a company determines that a breach has occurred, it must conclude whether "personal information" was lost. The loss of "personal information" is the critical factor that triggers disclosure under the various state statutes, but states define "personal information" differently. Generally, "personal information" is defined as (a) a person's first and last name or (b) first initial and last name, in combination with at least one of the following: (i) Social Security number; (ii) driver's license or state ID number; (iii) bank account, credit card, or debit card number, along with security or access codes or passwords;[41] (iv) medical information;[42] (v) health insurance information;[43] or (vi) certain biometric information.[44]

---

38. *See* John B. Kennedy et al., *U.S. State and Selected Federal Privacy and Data Security Developments 2011: On the Threshold of a Federal Law?*, *in* TWELFTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW 165, 173 (PLI Privacy & Data Sec. Law Practice, Course Handbook Ser. No. 28713, 2011).

39. John B. Kennedy, *U.S. Information Security Law Update 2009: The Patchwork Quilt of Regulations Continues To Grow*, *in* TENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW 115, 125 (PLI Intellectual Prop. Practice, Course Handbook Ser. No. 19129, 2009).

40. CAL. CIV. CODE § 1798.82 (West 2009); TEX. BUS. & COM. CODE § 521.053 (Vernon 2009).

41. The majority of jurisdictions only include (i), (ii), and (iii) as elements in defining "personal information." *See* Kennedy et al., *supra* note 38, exhibit A, at 235.

42. Arkansas and California include medical information. ARK. CODE ANN. § 4-110-103(7)(D) (Supp. 2011); CAL. CIV. CODE § 1798.29(e)(4).

43. CAL. CIV. CODE § 1798.29(e)(5).

44. Iowa, Nebraska, North Carolina, and Wisconsin include certain biometric data. IOWA CODE ANN. § 715C.1(11)(e) (West Supp. 2011); NEB. REV. STAT. § 87-802(5)(e) (2008); N.C. GEN. STAT. § 75-66(c)(10) (2009); WIS. STAT. ANN. § 134.98(1)(b)(5) (West 2009).

Finally, businesses must determine which state law applies. State legislatures draft security breach statutes to protect their residents. Thus, if a company loses information about consumers from twenty different states, the required level of disclosure differs based on where those individuals are domiciled. Because it can be prohibitively expensive to determine each individual's domicile, companies may have to comply with the most stringent disclosure laws to avoid liability.[45]

Recently, Massachusetts imposed even greater costs on businesses in an effort to prevent breaches.[46] These new regulations require every company "that owns or licenses personal information about a resident" to provide reasonable security for this information.[47] Specifically, the new Massachusetts regulation requires such companies to implement a "written, comprehensive information security program" and to encrypt all personal information stored on portable devices and all personal information that is transmitted wirelessly or over public networks.[48] These regulations took effect in 2010.[49] As most companies store at least a few Massachusetts residents' personal information, these regulations likely will become the norm.[50] Because companies face these greater burdens in the event of a software breach, they ought to be able to shift some liability back to software vendors.

B. Calculating the Costs of These New and Complex Regulations

The costs of these disclosure requirements vary based on the characteristics of the company, the data lost, and the state statute implicated by the breach.

---

45. Many states include safe harbor provisions in these data security statutes, which provide that a company is deemed in compliance if it follows its own breach notification procedure or adheres to more stringent state or federal regulations, as long as it is consistent with the timing requirements in the statute. *See, e.g.*, DEL. CODE ANN. tit. 6, § 12B-103 (West 2005); KAN. STAT. ANN. § 50-7a02 (2006); *see also* Kennedy et al., *supra* note 38, exhibit A, at 235 (summarizing the safe harbor provisions in the various state statutes).

46. Massachusetts Privacy Regulation, *supra* note 3, at 17.01 (noting that the purpose behind the new Massachusetts regulation is to "insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer").

47. *Id.* at 17.04. Section 17.02 defines "owns or licenses" to mean "receives, stores, maintains, processes, or otherwise has access to personal information." *Id.* at 17.02.

48. *Id.* at 17.04.

49. *Id.* at 17.05.

50. *See* sources cited *supra* note 45.

Despite these variations, reports estimate that these new regulations alone will cost $15 per customer should a breach occur.[51] When a company holds millions of consumer records (and loses between 46 million and 215 million individuals' information, as in the case of TJX Companies[52]), these costs compound quickly. Also, when the total costs associated with a breach are viewed, costs can climb to over $200 per record.[53] Between these direct costs, new disclosure requirements, and general reputational costs, companies face greater expenses than they did just five years ago should a breach occur.[54] Courts, however, continue to enforce extremely restrictive limitations on liabilities and remedies inserted by vendors into software licensing agreements.[55] Part III argues that courts should spread these new costs more fairly across businesses as well as software vendors.

III. TOWARD A FAIRER REMEDY FOR BUSINESSES

As noted above, a few courts refuse to enforce certain licensing agreements when the contractual remedies are so limited that they frustrate the contract's essential purpose.[56] Simply put, if an agreement provides no meaningful possibility of recovery, some courts will look beyond the contract's four corners to provide an adequate remedy under the failure of essential purpose

51. Amy O'Connor, *Security Breach Notification Laws Reinforce Need for Cyber Insurance*, INS. J., Mar. 4, 2010, http://www.insurancejournal.com/news/southeast/2010/03/04/107853.htm.

52. *See* Kawamoto, *supra* note 10.

53. *See* PONEMON INST., *supra* note 12, at 5 ("The average organizational cost of a data breach this year increased to $7.2 million, up 7 percent from $6.8 million in 2009. Total breach costs have grown every year since 2006. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from last year."). The costs associated with security breaches include: lost business, ex-post response, notification, and detection/escalation. *Id.* at 18-19.

54. While the new notification requirements increase the costs associated with a breach, costs also are greater today than they were just a few years ago because companies hold more consumer information due to the increase in electronic transactions. *See supra* note 1.

55. *See, e.g.*, Chatlos Sys., Inc. v. Nat'l Cash Register Corp., 635 F.2d 1081, 1087 (3d Cir. 1980) ("In short, there is nothing in the formation of the contract or the circumstances resulting in failure of performance that makes it unconscionable to enforce the parties' allocation of risk. We conclude, therefore, that the provision of the agreement excluding consequential damages should be enforced, and the district court erred in making an award for such losses."); *see also supra* note 28 (noting other representative cases).

56. *See* U.C.C. § 2-719 (2003) ("Where circumstances cause an exclusive or limited remedy to fail of its essential purpose, remedy may be had as provided in this Act.").

doctrine.[57] This minority rule—which has been articulated by the Eighth Circuit—allows the failure of essential purpose doctrine to affect limitations of liability as well.[58] A Missouri state court provided a succinct summary of this principle: "Since . . . the limitation of remedy has failed of its essential purpose . . . all other contractual remedies are available . . . . Other remedies available include the buyer's incidental and consequential damages resulting from the breach . . . ."[59]

If courts followed this minority position and gave the failure of essential purpose doctrine more equitable bite in the software security context, they would essentially create a mandatory rule (similar to unconscionability) that software vendors could not frustrate a licensing contract's essential purpose. This kind of mandatory rule appears necessary in this context—as opposed to the current default rule framework—because of the parties' asymmetrical bargaining positions, caused by the recent statutory burdens placed on businesses as well as the small amount of competition in the industry.[60] Further, the fact that consumer privacy is compromised when this type of software fails to function properly provides an additional public policy reason for not allowing vendors to escape liability simply because of their strong bargaining position.[61]

Currently, however, most jurisdictions do not give the failure of essential purpose doctrine this amount of equitable bite. The majority position holds that liability limitation clauses are independent of the limitations on remedies.[62] Under the majority's framework, a limitation of liability clause will survive even if the remedy limitation is unenforceable. The justification behind the majority rule is that "an exclusion of consequential damages stands unless it is unconscionable, and unconscionability is determined by a court as a matter

57. *See, e.g.*, R.W. Murray, Co. v. Shatterproof Glass Corp., 758 F.2d 266 (8th Cir. 1985); Goddard v. Gen. Motors Corp., 396 N.E.2d 761 (Ohio 1979).

58. *R.W. Murray, Co.*, 758 F.2d at 266; *Goddard*, 396 N.E.2d at 761.

59. Givan v. Mack Truck, Inc., 569 S.W.2d 243, 247-48 (Mo. Ct. App. 1978).

60. *See supra* note 5.

61. This type of public policy justification can also be seen in cases where automobiles were defective and put consumers in physical danger. *See, e.g.*, Hibbs v. Jeep Corp., 666 S.W.2d 792 (Mo. Ct. App. 1984); *Goddard*, 396 N.E.2d 761; Ehlers v. Chrysler Motor Corp., 226 N.W.2d 157 (S.D. 1975). For a general discussion of the failure of essential purpose doctrine, see Howard Foss, *When To Apply the Doctrine of Failure of Essential Purpose to an Exclusion of Consequential Damages: An Objective Approach*, 25 DUQ. L. REV. 551 (1987).

62. *See, e.g.*, Chatlos Sys., Inc. v. Nat'l Cash Register Corp., 635 F.2d 1081, 1086 (3d Cir. 1980).

of law."[63] However, as legislatures shift greater liabilities to businesses that hold consumer information in an effort to protect those consumers, courts should refuse to enforce restrictions on limitations of liability when contractual remedies frustrate the essential purpose of software licensing agreements.

Allowing businesses and retailers to shift some costs and liabilities back to vendors under the failure of essential purpose doctrine is desirable for several reasons. First, this solution gives each party the proper incentives. Shifting the possibility of increased liability back to vendors will better incentivize software providers to design products that fail a smaller percentage of the time—providing better protection for consumers.[64] This incentive is especially important because more than one-quarter of security breaches occur because of a software malfunction.[65] And where a breach is caused by a software defect, the software vendor is the least cost avoider. From an economic standpoint, putting some liability and burden on the least cost avoider is only prudent. If the UCC continues to be used as a tool for vendors to disclaim all liabilities and remedies, then software providers have little reason to remain scrupulous in maintaining quality.

Second, shifting some liabilities back to vendors promotes more efficient outcomes. While it is likely that adopting the minority position would cause software vendors to slightly increase the price of their security software to account for the increased potential liabilities, all companies that purchase the software would shoulder this slightly increased price. Instead of a situation where one company faces all liabilities posed by a security breach and has little control over the quality of the security software it uses, this Comment's proposal would force businesses and vendors alike to share in the risk of breach. By sharing in the risk of breach, software vendors also will be incentivized to make more secure products;[66] accordingly, any increased price could be viewed as companies paying for a better product.

Third, software vendors are in the best position to internalize the risks that are inherent in potential security breaches. As many businesses and retailers lack sufficient assets to offset the liabilities of a potential breach, they have little incentive to take on additional security measures should a breach occur. Indeed, many of these companies would have to file for bankruptcy if all of the liabilities from a security breach fell on them, and thus, their creditors in

63. Rheem Mfg. Co. v. Phelps Heating & Air Conditioning, Inc., 746 N.E.2d 941, 948 (Ind. 2001).

64. *See supra* note 13.

65. PONEMON INST., *supra* note 12, at 6.

66. *See supra* note 13.

bankruptcy would bear the costs and the risks of breach. By placing some of the potential costs of a breach on the software vendor, which is generally a larger entity than the individual businesses that purchase security software, courts could place some liabilities on the party that is in the best position to internalize these risks and insure against them.[67]

Finally, this Comment's proposal allows courts to effectuate the UCC's broader goals.[68] As the UCC generally provides expectation damages—putting "the aggrieved party . . . in as good a position as if the other party had fully performed"—courts should find severe limitations on liability unenforceable.[69] This aspect of the UCC has been critical in minimizing contractors' costs.[70] While some might advocate amending the UCC, such a change likely would be too broad. Under this Comment's proposal, courts could invalidate limitations only when agreements restricted remedies in a way that frustrated their purpose. Moreover, courts could distinguish between breaches caused by software malfunctions and those caused by other factors, while an amendment to the UCC could not account for these nuances as easily. Finally, as the UCC provides broad rules to govern multiple industries, an amendment that carved out a narrow exception targeted solely at data security software would not be consistent with the UCC's overall framework.

---

67. As software vendors tend to be larger businesses, see *supra* notes 5-7, they are also in a better position to handle this increased risk and in a better position to self-insure against it, especially compared to many smaller businesses affected by these state statutory schemes. It should be noted that this justification for placing additional burdens on software vendors implies also that this Comment's solution may create additional barriers to entry in the software licensing market. As noted above, however, the industry has already faced great consolidation, and high barriers to entry already exist. *See id.* The actual effect, therefore, of placing greater potential liabilities on software vendors vis-à-vis market entry should be minimal. Moreover, shifting some liability to vendors would place a higher cost on incumbent vendors compared to upstart vendors. Whereas larger, established vendors are likely able to pay the liabilities from a security breach at one hundred cents on the dollar, many upstart vendors may be forced into bankruptcy after a breach and thus cannot pay their liabilities at one hundred cents on the dollar. *See, e.g.*, Stefan Topfer, *A Wake Up Call for Small Business Data Security*, NASDAQ (May 12, 2001, 12:21 PM), http://community.nasdaq.com/News/2011-05/a-wake-up-call-for-small-business-data-security.aspx?storyid=75654 ("The statistics show that 93% of businesses that suffer data loss for more than ten days go bankrupt within the next year."). Accordingly, shifting some liability to vendors places a greater burden on larger established vendors compared to smaller upstart vendors.

68. Maureen A. O'Rourke, *Rethinking Remedies at the Intersection of Intellectual Property and Contract: Toward a Unified Body of Law*, 82 IOWA L. REV. 1137, 1155-58 (1997).

69. *Id.* at 1155 (quoting U.C.C. § 1-106 (1996)).

70. *Id.* at 1158.

CONCLUSION

Compared to many other contracts, software licensing agreements greatly favor vendors because businesses that hold consumer information are practically required to implement these technologies. Concerns related to the one-sided nature of these contracts have only recently come to the business community's attention.

As state legislatures have enacted a panoply of statutes to protect consumers, the reporting costs and added liabilities imposed on companies have increased dramatically. The current situation squeezes businesses that hold consumer information because they now experience more regulation, while continuing to face licensing agreements that remove the possibility of meaningful relief.

To address this risk shift, courts should adopt the minority position regarding the failure of essential purpose doctrine when reviewing software licensing agreements. This solution would allow courts to use the doctrine to render limitations of liability unenforceable if the remedy provisions frustrate the contract's essential purpose. This proposal also represents a measured response and would more efficiently allocate the risk of loss, provide greater incentives for vendors to manufacture more secure software, better spread liability in the case of breach, and more completely accomplish the UCC's overarching remedial goals.

STEPHEN S. GILSTRAP